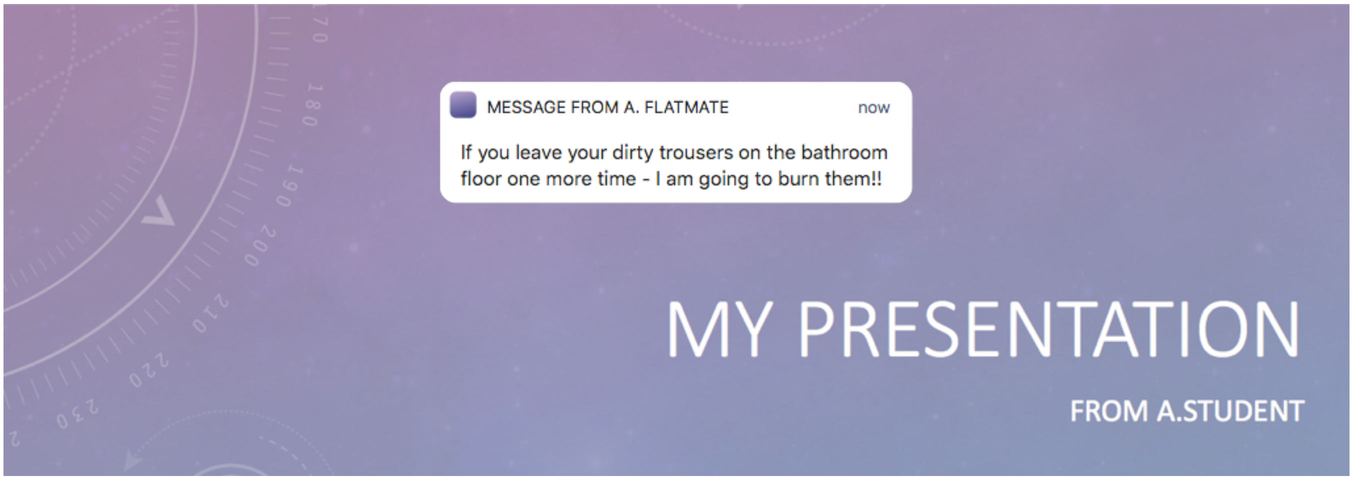
Maguire, J. and Draper, S. (2017) Privacy of Personal Things in Active Learning Spaces Need Individually Evolved Requirements. SafeThings '17, Deflt, Netherlands, 05 Nov 2017. ISBN 9781450355452 (doi:10.1145/3137003.3137009)

Privacy of Personal Things in Active Learning Spaces Need Individually Evolved Requirements

Joseph Maguire
School of Computing Science
University of Glasgow
Glasgow, United Kingdom
joseph.maguire@glasgow.ac.uk

Steve Draper
School of Psychology
University of Glasgow,
Glasgow, United Kingdom
steve.draper@glasgow.ac.uk



MESSAGE FROM A. FLATMATE now

If you leave your dirty trousers on the bathroom floor one more time - I am going to burn them!!

MY PRESENTATION

FROM A.STUDENT

Figure 1: Illustrative example of unwanted notification appearing during student presentation.

ABSTRACT

Technology-enhanced active learning (TEAL) spaces could represent a significant benefit to learning and teaching at universities. TEAL spaces support students in projecting presentations (e.g. from smart-phones) and sharing notes (e.g. from smart-watches) with peers. Importantly, this sharing is partly amongst their co-present small group but sometimes to the whole class. However, plugging personal things into smart spaces whose first requirement is to accept as many devices as possible is not without consequence. A projected notification of a political conversation, for example, has the potential to harm the individual both within the space and beyond, opening them to unwanted judgment, criticism and assessment.

The traditional argument from the usable security community is that of intervention prior to any use whatever: users need to be trained, taught and/or nudged to avoid such problems. We conducted an informal focus group with students in a pilot TEAL space, exploring issues around the privacy and security of using personal devices in such spaces. The reality is that it is hard to perceive the privacy and security challenges prior to using the space. We argue that such prior interventions are not only a significant barrier to student adoption of smart spaces, but ineffective in ensuring the safety of individuals in the long-term.

We argue that in designing smart spaces, both on-campus and off, designers need to adopt an approach of individually evolved privacy requirements to ensure an on-going safe, creative space for students. Two important features are: (a) as a small group develops bonds, its privacy level needs to be reduced over time and (b) the best privacy level depends on the whether the screen is currently shared with the small group or the large class.

CCS CONCEPTS

• **Security and privacy → Human and societal aspects of security and privacy**; **Social aspects of security and privacy**; • **Applied computing → Collaborative learning**;

KEYWORDS

usable security, technology-enhanced active learning, privacy

ACM Reference format:
Joseph Maguire and Steve Draper. 2017. Privacy of Personal Things in Active Learning Spaces Need Individually Evolved Requirements. In *Proceedings of SafeThings'17, Delft, Netherlands, November 5, 2017,* 6 pages.
https://doi.org/10.1145/3137003.3137009

1 INTRODUCTION

Technology-enhanced active learning (TEAL) with personal devices has the potential to change higher education significantly [8, 9], but its implementation must consider security and privacy challenges [13] to ensure a safe, creative space for learning: safe as in being secure against public shaming, and creative as in feeling free to speak without the inhibition that fear-based safe actions require.

The concept of active learning can be best understood in contrast to passive learning or 'teach-by-telling'. The prototypical example of passive learning is a lecture, where lecturers communicate concepts to large groups of students in theatres. The solution makes sense when knowledge is difficult to access and to transmit. However, the Internet has reduced the expense of transmitting and accessing knowledge. Consequently, a student is no longer reliant on a single lecturer to attain content: there are any number of authors available via the Internet.

Therefore, in active learning the lecturer sets a pre-session activity, for example in a usable security course, an investigation of the concept of *differential privacy*. Students sift through digital content using their smart phones, tablets or any other device. The lecturer then sets the in-class activity, say a short presentation on the investigated topic. Students can then craft a presentation on their personal smart phone and plug it in for display.

The use of personal devices is central to TEAL spaces. Some students will still use pen and paper as the tools of choice, others may use Facebook and Google. However, the concern is that students may not always be able to control their audience. In the prior example, an accidental notification could overlay any presentation as seen in Figure 1.

The reality is that universities must ensure a safe, creative space for students - even if those spaces embrace the Internet of Things. The concern is that universities have had decades, if not centuries, of experience in constructing lecture spaces that are safe and creative environments [1], e.g. at a minimum universities consider fire-exits, but also quiet spaces where audibility of speakers and usually also of audience questions is significantly better than public rooms such as churches or hotels usually provide. The concern is that universities are rapidly investing in active learning spaces without thinking of the dangers of plugging personal devices into equipment where the first requirement is to allow anything to connect.

The concern is that many universities may not be considering the security and privacy challenges of active learning spaces. Alternatively, some decision-makers may view such challenges as inconveniences, rather than challenges that may improve the actual overall experience. Nevertheless, even small decisions such as seat choice can reflect personal privacy decisions by students [12].

Consequently, we conducted a small user study discussing the security and privacy challenges of TEAL spaces. The users were students who had experienced a course delivered in a TEAL space. The contributions of this paper are:

- a small user study illustrating some of the challenges of security and privacy.
- discussion surrounding these issues and why designers should consider them when individuals are plugging personal devices into sophisticated smart spaces.

Our suggestion is that this user study may offer a starting point for decision-makers in thinking and discussing the security and privacy challenges of education in smart spaces.

2 BACKGROUND

Higher education across the world is being challenged by the free flow of knowledge across the Internet. Universities are under pressure to remain relevant and remain competitive to attract researchers and students alike. Sophisticated smart campuses that support active learning are increasingly being perceived as an investment that most universities will need to make [4].

Coccoli *et al.* analyse the challenge for universities of the emergence of pervasive networking and personal devices in the European context [3]. They argue that safety and health is one of the many important aspects that needs to be thoroughly factored in when designing smart spaces. Coccoli *et al.* argue that students are not just plugging in personal tablets, but applications and services as well, e.g. social networking services (SNSs).

The reality is that SNSs and other such applications could be vulnerable due to the intersection with the Internet of Things in the smart campus [2]. This suggests that while there may be concerns about peers observing privacy notifications being displayed, nefarious students could compromise an individual's privacy, e.g. by packet sniffing. Consequently, universities have a requirement to ensure the safety of students' data since they are promoting the use of personal devices. Universities must appreciate that students using personal devices in learning spaces will not normally be using the devices solely for learning activities, in contrast to devices such as desktops provided by the university for students.

Similarly, Crichton *et al.* demonstrated that students initially 'resented' the institution intruding on their personal devices [5]. They investigated the use of students using iPods, iPads and laptops in the classroom. Crichton *et al.* report that students were initially hesitant, this fades as they find the devices useful to completing 'work-based' tasks, e.g. reading a textbook etc. They also report that students prefer to use a range of devices, rather than a single device. This would suggest that smart spaces that support a range of personal devices could be desirable to students. However, Crichton *et al.* argue that sharing content and collaboration is still an emerging challenge for the use of such devices in education. It could be the case that students simply do not perceive personal devices as useful for learning [16].

Nevertheless, DeBarger *et al.* argue that while there may be challenges, there are also opportunities to improve the experience of the learner in TEAL spaces [6]. DeBarger *et al.* consider the use of Group Scribblers, an application that supports a mix of physical and electronic sticky notes to consider concepts in classrooms. DeBarger *et al.* argue such collaborative tools in the classroom afford students insight into the traditionally 'private' practice of teaching. Teachers frequently make decisions regarding the lesson and student in private. However, when collaborating in an active space, students have more exposure to the process of academic practice.

If such spaces are about refining collaboration skills, then focusing on the strategies and devices individuals use prior to entering may be the best starting point [7]. Lampe *et al.* investigated the use of SNSs to organise classroom activities [11]. They argue that success or failure at using such tools for collaboration hinged on how they used it, not how important they felt the tool was or their level of experience with it. The design and layout of the room is also crucial to ensuring a collaborative work environment. Rogers and Lindle argue the placement of large, interactive displays can impede efficiency and effectiveness of collaboration [14]. Nevertheless, Rogers and Lindle state that designers should strive to avoid making such displays a focal point, since some tasks will always be better with pen and paper.

However, students can also rip a blank piece of paper from a diary, rather than risk the exposure of personal notes to fellow students. The reality is that all individuals have considerable skills in the context of everyday life in managing collaboration and privacy. It is whether or not these skills are triggered when collaborating with applications and personal devices in active spaces.

The assumption is that either (a) these skills emerge quickly or (b) take time to form. The expectation is that skills that emerge rapidly within an active learning space are not new skills at all, but transfer of existing skills and preferences [15].

It is those slowly emerging or new skills that are more interesting. It takes time to develop a new skill in managing privacy with personal devices in a work space. The crucial argument is whether or not TEAL spaces are a safe environment to develop such skills.

The privacy and security challenges of such spaces may make them unsafe. A child may make mistakes when they are younger, but are typically shielded by their parents, e.g. their trousers fall down, the audience is understanding, the parents can reassure. However, students are adults and it is not clear how embarrassing situations can be recovered from. Figure 1 illustrates an example of an unwanted notification displayed in-class. That accidental display could be captured and shared on SNSs and consequently, preserved for all time. It is not clear how a student can recover.

Therefore, universities must ensure sophisticated smart spaces are a safe environment not only for learning, but also for forging new skills in managing privacy and collaboration. The first step is to develop a sense of the actual privacy and security challenges in active spaces.

3 PILOT SPACE

The user study relied on students that had experienced for the first time a course in a pilot TEAL space. Figure 2 illustrates the layout of the pilot TEAL space we studied. The space has four projectors and supports up to 60 students, arranged into tables with teams of six or eight individuals. Each table has a dedicated workstation and two monitors. The first monitor displays locally connected devices while the second displays whatever device is currently shared with the class, e.g. the console for the lecturer, or the workstation of another group.

The lecture console has an array of different display options and devices, e.g. workstation, back-lit white board and projectors. The central console also offers the lecturer control of the mode of the room, either 'lecture-style' or 'TEAL-style'. If in lecture mode, all displays only show content dictated by the central room console. However, in TEAL mode, individual tables can control what is displayed, including their own personal devices.

The table allows individuals to connect their personal devices over HDMI or wireless. There is also a control panel at each table, allowing members to select which personal device to share on the local display. The control panel also lets table members select which device to share with the whole of the class on the large projectors.

4 USER STUDY

The focus group was conducted as an activity in a Masters-level usable security course. The course had approximately 60 students and was delivered over several weeks, and the focus group was conducted towards the end of the course.

4.1 Participants

There were 21 participants involved in the focus group. Two participants did not consent to their responses being utilised for the purposes of research in education. The participants were all enrolled on a Masters course focused on usable security and had been involved in learning and teaching in a TEAL space for several weeks.

4.2 Apparatus

The focus group was conducted in the same pilot TEAL space used for delivering the usable security course. The students gave open-text responses using an in-class response system that they could access from their personal devices or table workstation. Paper was provided for those students that did not want to use the in-class response system.

4.3 Procedure

The focus group was delivered towards the end of a usable security course, that had been delivered in pilot TEAL space over a semester. Individuals were requested to give consent to use of comments for the purposes of research and evaluation via the in-class response system.

The individuals gathered at tables as teams and were asked to consider privacy and security challenges of collaborating in TEAL spaces. Teams were asked to devise at least one question to pose to the rest of the class. The question was to be designed to gain insight into an aspect they perceived as a privacy and security challenge for using such a space.

Teams could research the topic using their personal devices and/or the workstation at each table. Participants were asked to prepare their question for presentation to the rest of the class, again either on their personal device or the workstation for each table. The teams were then brought back together as a class.

Teams were then selected using a random-number generator, and were then instructed to use the control panel for their table to share their display, and consequently, their question with the rest of the class. The rest of the class were expected to submit an open-text response using the in-class response system. The responses were then reviewed and discussed with the rest of class.

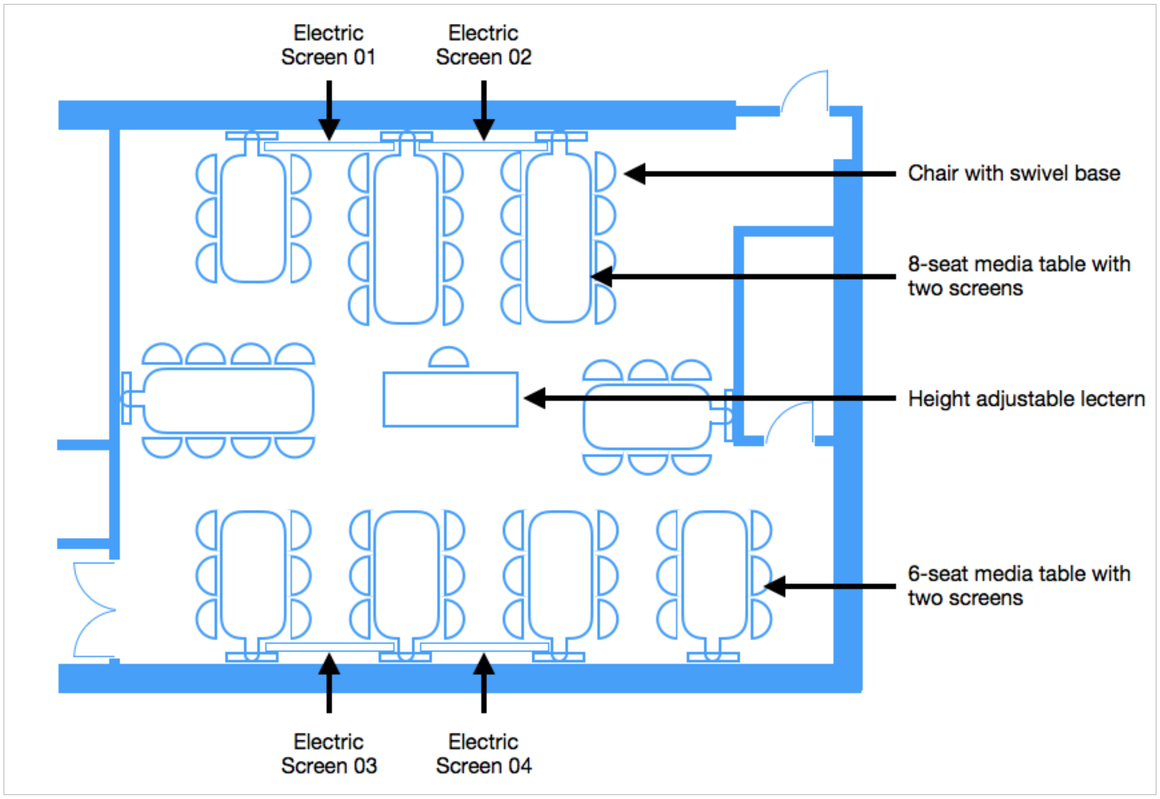


Figure 2: Layout of pilot Technology-enhanced Active Learning (TEAL) space

5 RESULTS

The participants are here referred to by a participant identification number, e.g. "P14". The first team selected, Team U, posed the question of whether team mates would share personal devices in such spaces.

> Would you let another person use your personal device?
> **Team U**

Thirteen participants provided an open-text response to the question posed by Team U. The majority of responses (62%) indicated that participants would let another individual at the table use their personal device with the minority (38%) stating they would not allow it. Nevertheless, while participants may permit others to use their device, it would not be without concern.

> "With supervision, not an issue, I can see what they are doing; but if I couldn't see the screen while they were working then I would be concerned."
> **Participant 19 (P19)**

The comment from P19 reflected the many comments that students would share their device while desiring some form of control. Similarly, P9 stated it "*depends, whether I trust him or not*". Indeed, even those participants that would allow others to use their personal device would only do so as the device would be properly configured. P12 stated, for example, that "*my personal files are hidden and protected*". The comment from P12 was evidence of a recurring theme of the discussion. The perception was that individuals should actually know how to use a room's equipment before collaborating within it. This is evident in some of the responses from the question posed by the next randomly selected team.

> Do you feel comfortable in connecting your personal device to the display for sharing with others?
> **Team V**

There were a total of 12 responses to the question from Team V. A small majority of participants responded (58%) that they were comfortable in connecting their personal device for sharing with others. However, the general sentiment from the group stated that individuals should know what they are doing. P12 stated, for example, "*you should know that you have to hide your personal data before connecting cables!*". Nevertheless, this was not the case for all participants as evident from the response from P4.

> "No. You don't know if its going to appear on the screen next to you, or on every screen in the room."
> **Participant 4 (P4)**

Similarly, P15 stated "*We're not always fully aware of the risks that may occur when we plug in our device in public*". The concern of the unforeseen was raised in the question from Team W.

> Do you have security concerns about the actual physical connectors?
> **Team W**

Team W felt individuals may have concerns about the physical connectors themselves. The team seemed to suggest that the university environment is relatively open and accessible. They suggested that nefarious individuals may interfere with connectors to capture data. Ten participants provided text responses to the question from Team W. However, a minority of students (40%) had concerns about the physical connectors. Nevertheless, those concerns may lead to individuals not participating in activities with their personal devices as indicated by P4.

> "You can't be 100% sure what you're plugging your device into, so the only way to protect your data is to not plug it in at all."
> **Participant 4 (P4)**

Furthermore, from those that did not have concerns, the theme of education emerged. P11 stated towards individuals that are concerned that they should "*encrypt your data*". Team X explored this further with their question, that probed whether individuals have concerns around personal data collection.

> Do you have concerns about the collection of personal data?
> **Team X**

Ten participants provided open-text responses to the question to Team X. The majority of individuals (70%) that responded to the question were concerned about data collection. P17 essentially expressed the sentiment on the group when they stated "*Yes, there might be personal data on a device or some confidential information that should not be shared*". Similarly, P15 indicated that individuals may need to adjust their expectation, suggestion that they may "*only have a reasonable expectation of privacy to a certain extent in any public space*". Nevertheless, P12 stated an alternative position.

> "No, it's not. I've already sold my soul to facebook"
> **Participant 12 (P12)**

Similarly, Team Y explored the types of personal data that individuals would actually be concerned about within such a space.

> What personal information are you concerned about?
> **Team Y**

Nine participants provided open-text responses to the question from Team Y. The responses were varied with some participants stating financial information, web browsing history, conversations. P19 stated what many students seemed to sense was the only real concern.

> "That my personal messages would pop up over the content."
> **Participant 19 (P19)**

The last team selected to pose a question was Team Z. The team asked the most important question of the group in many ways.

> Would you connect your personal devices to the space?
> **Team Z**

Eight participants provided an open-text response to the question. The majority of these responses (88%) were positive with individuals stating they would connect their personal devices to the space. Participant P7 seemed to summarise the sentiment of most of the group and discussion.

> "Yes but I would turn off the notifications."
> **Participant 7 (P7)**

6 DISCUSSION

The small study reported above concerns a situation which, although novel to the teacher and students involved, is by no means technologically radical. Yet it nevertheless illustrates a number of ways in which the usual security community approach is mismatched to reality. Firstly of course, by far the most common way in which people approach new information technology is to learn by doing: which conflicts with the usual idea in security that defences should entirely depend on prior training.

More importantly, active learning spaces in education are fundamentally about having students use their personal devices. While numerous professionals have two or more mobile phones, partly to manage privacy between work and private life, this is not currently the case with students. In this respect, our study represents a case a little more urgent in forcing an intersection of an individual's private and professional life. Yet in practice, this is a general issue since few professions can have a rigid policy of disallowing communications about family emergencies ever to reach someone at work: it is a general issue on how to manage such junctions safely and satisfactorily. The current issue in the education case is how to manage it, not just in terms of future software mechanisms, but right now with existing devices configured primarily to deal with private needs.

The study shows that there is not a single group to consider in this case, but at least two (the small group of about six at a table, and the larger whole-class group of about 60 in this case); and that transitions between these audiences occur very quickly (one button press) and moderately frequently. We are familiar with this in many social situations (e.g. in restaurants where again you are in both a small close group and a wide one of the whole room; closing the door at home to have a row with your partner not-in-front-of-the-kids), but this is seldom seen in software requirements. It illustrates the rapidity with which changes are made to audience control in everyday non-technological contexts, and the need for this to be do-able when using internet-connected ordinary devices for such connections to be (socially) safe.

Furthermore within a group, the level of privacy vs. openness changes over time (cf. the chill when an outsider joins a group and everyone changes the level of disclosure; or when two people chatting enter a space where others will overhear them). This is a widespread feature of groups, partly (as in the case of a new class) as they first get used to each other, but also rapidly in the first seconds of two people starting a conversation as in what linguists call "alignment" where two people talking converge quickly and unconsciously to a common loudness of speech, speed of talking, length of pauses, and many other things – so also, we suggest, do groups converge over time on a level of confidentiality in ordinary chat, that may be different in each group. It is also clear that a policy of safety first is not a solution: as one participant said, a group member hiding what they are doing will be censured when the group norm is sharing just as often as a person will be censured for broadcasting when the group norm at that moment is private discussion: the required privacy level moves both up and down.

This requirement for moderately frequent (perhaps every 5 to 10 minutes) and very fast (within a few seconds) changes in privacy settings is not covered by most current mechanisms of levels of permissions, or being in and out of a Facebook group which are much slower and clumsier to operate than these cases require.

7 LIMITATIONS

The study reported here is too limited in numbers, the range of devices involved, and in looking only at the educational context of a single country to be of interest as a representative of general student experience in technology enhanced active learning. However the combination of students learning about cyber security yet having a fresh personal experience and using their own personal devices made for a set of comments from personal reflection that are potentially more useful than other studies. If the students used devices provided for them, they would lack the range of different kinds of usage accumulated over long periods which actual personal devices have. If the students had no orientation to the issues of security, they would mostly comment on a few events that disrupted their immediate usage rather than attempting to foresee likely future issues. If they were already well indoctrinated in the research perspective on cyber security then they would probably already see it mostly as a matter of incompetent and lazy users not taking enough precautions. Thus this particular study may provide, not reliable data on how widespread each problem is, but a set of issues that may include some useful insights into possible security and privacy challenges of such a space. Therefore it could be the case here that relatively few students are enough to lead to relevant and valid insight [10].

8 CONCLUSION

How much real disruption in practice will be caused by issues like those raised above? The expectation is that TEAL spaces could represent a significant benefit to learning and teaching at universities. However, while universities have considerable experience in designing lecture theaters, they have little insight into TEAL spaces reliant on personal devices.

In this paper, we presented a small user study to explore what students, who had experienced a pilot TEAL space, perceived as the security and privacy challenges of using such a space. The perception from *those* students is that while they perceive many such challenges, they also acknowledge the real potential of such a space. The concern is that once a student's privacy has been compromised, the environment is no longer a safe space to learn. Consequently, it is important for universities and designers to ensure that learning spaces infused with technology are safe, creative spaces for students.

REFERENCES

[1] Sherry Ahrentzen and Gary W Evans. 1984. Distraction, privacy, and classroom design. *Environment and Behavior* 16, 4 (1984), 437–454.

[2] Luca Caviglione and Mauro Coccoli. 2011. Privacy problems with Web 2.0. *Computer Fraud & Security* 2011, 10 (2011), 16–19.

[3] Mauro Coccoli, Angela Guercio, Paolo Maresca, and Lidia Stanganelli. 2014. Smarter universities: a vision for the fast changing digital era. *Journal of Visual Languages & Computing* 25, 6 (2014), 1003–1011.

[4] Price Waterhouse Cooper. [n. d.]. The 2018 digital university: staying relevant in the digital age. ([n. d.]). https://www.pwc.co.uk/assets/pdf/the-2018-digital-university-staying-relevant-in-the-digital-age.pdf

[5] Susan Crichton, Karen Pegler, and Duncan White. 2012. Personal Devices in Public Settings: Lessons Learned from an iPod Touch/iPad Project. *Electronic Journal of e-Learning* 10, 1 (2012), 23–31.

[6] Angela Haydel DeBarger, William R Penuel, Christopher J Harris, and Patricia Schank. 2010. Teaching routines to enhance collaboration using classroom network technology. *Techniques for fostering collaboration in online learning communities: Theoretical and practical perspectives* (2010), 224–244.

[7] Terri A Fredrick. 2008. Facilitating better teamwork: Analyzing the challenges and strategies of classroom-based collaboration. *Business Communication Quarterly* 71, 4 (2008), 439–455.

[8] Richard R Hake. 1998. Interactive-engagement versus traditional methods: A six-thousand-student survey of mechanics test data for introductory physics courses. *American journal of Physics* 66, 1 (1998), 64–74.

[9] Michael J Hannafin and Susan M Land. 1997. The foundations and assumptions of technology-enhanced student-centered learning environments. *Instructional science* 25, 3 (1997), 167–202.

[10] Nielsen Jakob. 2000. Why you only need to test with 5 users. *Alertbox* (2000).

[11] Cliff Lampe, Donghee Yvette Wohn, Jessica Vitak, Nicole B Ellison, and Rick Wash. 2011. Student use of Facebook for organizing collaborative classroom activities. *International Journal of Computer-Supported Collaborative Learning* 6, 3 (2011), 329–347.

[12] Darhl M Pedersen. 1999. Model for types of privacy by privacy functions. *Journal of environmental psychology* 19, 4 (1999), 397–405.

[13] Jules Polonetsky and Omer Tene. 2014. Who is reading whom now: Privacy in education from books to MOOCs. *Vand. J. Ent. & Tech. L.* 17 (2014), 927.

[14] Yvonne Rogers and Siân Lindley. 2004. Collaborating around vertical and horizontal large interactive displays: which way is best? *Interacting with Computers* 16, 6 (2004), 1133–1152.

[15] Carol S Weinstein. 1982. Privacy-seeking behavior in an elementary classroom. *Journal of environmental Psychology* 2, 1 (1982), 23–35.

[16] Ben Woodcock, Andrew Middleton, and Anne Nortcliffe. 2012. Considering the Smartphone Learner: an investigation into student interest in the use of personal technology to enhance their learning. *Student Engagement and Experience Journal* 1, 1 (2012), 1–15.