UCL DEPARTMENT OF
COMPUTER SCIENCE

Research Note
RN/11/08

Individual and organizational perspectives on data use in serious games

9 March 2011

Miguel Malheiros

Will Seager

Martin Ruskov

M. Angela Sasse

Abstract

In order to save time and costs, organizations are increasingly investing in technology-enhanced learning systems to fulfil their employee training requirements. Serious games are one possible approach to technology-enhanced learning where learners play game scenarios designed to facilitate competence development as they entertain. Previous research suggests that privacy is an important factor affecting the acceptance of information systems in organizations. Research on privacy in technology-enhanced learning has usually focused on data types assumed to be sensitive without user input on how they perceive the data. Additionally, proposed solutions consist in applying generic data protection techniques to already designed systems as opposed to trying to include privacy considerations during the design process. In this paper, we describe preliminary research into the potential privacy risks of serious games for competence development. We present findings from a workshop with developers of a serious game system and three focus groups with prospective learner-participants of the same system. Our findings indicate some potential areas of user concern e.g. the collection and retention of performance data for internal recruitment purposes, and the association of avatars with real identities inside the game environment. We conclude by making some initial recommendations concerning the privacy issues that employee and organizational representatives should be aware of when negotiating the deployment of a learning system of this type.

Individual and organizational perspectives on data use in serious games

M. Malheiros, W. Seager, M. Ruskov, M. A. Sasse
Department of Computer Science
University College London
London, UK
{m.malheiros, w.seager, m.ruskov, a.sasse}@cs.ucl.ac.uk

***Abstract*—In order to save time and costs, organizations are increasingly investing in technology-enhanced learning systems to fulfill their employee training requirements. Serious games are one possible approach to technology-enhanced learning where learners play game scenarios designed to facilitate competence development as they entertain. Previous research suggests that privacy is an important factor affecting the acceptance of information systems in organizations. Research on privacy in technology-enhanced learning has usually focused on data types assumed to be sensitive without user input on how they perceive the data. Additionally, proposed solutions consist in applying generic data protection techniques to already designed systems as opposed to trying to include privacy considerations during the design process. In this paper, we describe preliminary research into the potential privacy risks of serious games for competence development. We present findings from a workshop with developers of a serious game system and three focus groups with prospective learner-participants of the same system. Our findings indicate some potential areas of user concern e.g. the collection and retention of performance data for internal recruitment purposes, and the association of avatars with real identities inside the game environment. We conclude by making some initial recommendations concerning the privacy issues that employee and organizational representatives should be aware of when negotiating the deployment of a learning system of this type.**

Keywords - privacy; technology-enhanced learning; competence development; serious games

I. INTRODUCTION

Organizations are increasingly turning to e-learning solutions to save training time and travel costs associated with traditional face-to-face learning [7]. *Serious gaming* is emerging as a viable e-learning solution and has already become a critical component within some corporate learning programmes [17]. Serious games facilitate learning whilst simultaneously entertaining and engaging learners. Also, the simulation of real-world experience is thought to improve transfer of learning to the context in which the learning is applied [17].

Research into technology use within organizational environments suggests that privacy can be an important factor influencing the user acceptance and effectiveness of specific systems [11]. Given that serious game systems concerned with competence development rely on the collection and retention of some personal data, is seems probable that their success will depend in part on how well each system addresses the privacy concerns of individual learners and other users. Failure to adequately address these privacy concerns could result in a system that learners are reluctant to use at all or else reluctant to fully engage with.

Although some research has been carried out on the impact of privacy issues on technology-enhanced learning (TEL) [12, 15], it has focused on types of data assumed to be sensitive and on how to use generic privacy technologies to protect it. There is currently a gap in the literature regarding the specific privacy risks of learning systems, on how learner-users perceive and react to different data practices and interactions with respect to their privacy, and what impact privacy infringements can have on system acceptance and effectiveness. There is also a lack of methods to help TEL developers incorporate privacy considerations into the design of their systems.

In this paper, we describe some preliminary findings from on-going investigation into the privacy issues associated with serious games for competence development. These findings are drawn from two research activities: a workshop with developers of a specific serious game system and focus groups conducted with prospective learner-participants of this system. We adopt a participatory design approach, involving multiple stakeholders at an early stage in the system development process. By adopting this approach, we hope to minimize privacy infringements and thereby maximize user acceptance.

In the next section, we outline some related research into privacy in technology-enhanced learning and discuss its limitations. In the following section, we provide some details of the proposed TARGET serious game. We then describe how our research was carried out and present our findings. Finally, we present our conclusions and initial recommendations, and some future research directions.

II. BACKGROUND

In computer science research, privacy is commonly defined as the users' ability to control the flow of their personal information. Most privacy-related research in computer science has been carried out in the human-computer interaction (HCI) and security areas. HCI research has focused on providing users feedback about their personal information, while the security approach is to

provide encryption and anonymisation techniques that allow them to protect their information and avoid surveillance.

Privacy has been identified as a key issue in the technology-enhanced learning literature. Researchers identify *linkability* of data, *observability* of data, *identity disclosure* and *data disclosure* as potentially important privacy risks [5, 12, 15]. These views reflect a 'data-centric perspective' that fails to take into account user perceptions of particular data types within the context of different systems [2, 3]. In addition, the proposed solutions are usually limited to the generic privacy-enhancing technologies (PETs) proposed as solutions across a wide range of technologies [8] with an over-emphasis, in some cases, on identity protection [5].

There are few examples of research into the specific privacy issues associated with technology-enhanced learning In particular, there is little research into how the users of these systems perceive the privacy risks associated with different data types, processes and uses. Privacy is "*individually subjective and socially situated*" [1], which means that no type of information is considered personal in all situations and there is no situation that will be perceived as a privacy violation by all persons [10]. According to Adams [2, 3] there are three main factors that influence users' privacy perceptions while interacting with multimedia technologies: 1) information sensitivity, which relates to how the user perceives the information being transmitted and how it is going to be interpreted by the receiver; 2) information receiver, which regards the trust and relationship the user has with the receiver; and 3) information usage, which refers to how the user perceives the information is going to be used now or in the future. These inter-related factors are, in turn, influenced by the context of the interaction, and by the user's previous experiences and preconceptions.

III. TARGET

TARGET (Transformative, Adaptive, Responsive and enGaging Environment) is a collaborative project partially funded by the European Community under the Seventh Framework Programme. The main aim of TARGET is to research, analyze, and develop a new genre of Technology Enhanced Learning (TEL) environment to support the rapid competence development of project managers. TARGET adopts a serious games approach to competence development. Learners encounter realistic game scenarios that simulate the complex and challenging project management experiences that characterize the real world [4]. TARGET also aims to foster 'communities of practice' and promote social learning, enabling players to interact with each other via multi-player gaming, virtual social spaces, and other social tools. TARGET is intended for use within enterprise environments, academic environments and interest-focused communities. This paper focuses on the identification and exploration of privacy issues within the enterprise environment scenario.

A. Stakeholders

With reference to the enterprise organizational environment, four main stakeholder roles have been identified, each with interests in the competence development process of TARGET:

Organization. The strategic needs of the organization guide the individual learning goals of employees, which in turn influence how each employee uses TARGET. Some organizations may wish to use TARGET not just as a learning tool; they may also wish to use TARGET as a way to assess and monitor individuals' mastery of particular competences e.g. as a basis for recruitment and/or internal competence management. The collection, retention and use of data within each organization will reflect wider information management policies which, in some cases, will be negotiated with employee representatives. Organizational strategic needs and information policies will vary from organization to organization.

Learners. Individual employees will be the main users and beneficiaries of the TARGET platform. While policies concerning data collection and retention will be decided by the organization they work for, learners will likely have some influence over what personal information they want to share in different situations.

Mentors. With the TARGET learning process, human mentors will support individual learners. They will help them to reflect on their learning experiences and help them to tailor their learning plans.

Developers. The developers are stakeholders responsible for the development and maintenance of the TARGET platform. Some may also be involved after the deployment of TARGET within a particular organization, helping to maintain and adapt the platform to the changing needs of the organization.

IV. METHOD

To identify potential privacy issues in TARGET, we conducted two research activities. The first was a one day workshop with system designers and developers of the TARGET system. The workshop included representatives of a large commercial organization that has agreed to be an early adopter of the TARGET system. The workshop began with a brainstorming session where all participants had a chance to share any concerns regarding the privacy implications of the project. This was followed by a more systematic discussion that focused on identifying data and user types and the minimum level of access that would be required for each user type. This discussion was supported through the collaborative construction of a 'data/user' table, where the columns represented different types of learner data, and rows represented different user types (TABLE I. For each cell in the table, participants discussed whether a specific user would require access to that data type in order for TARGET to function properly. For some areas of the table, there was unanimous or near unanimous agreement. For other areas, there was considerable debate e.g. some workshop participants advocated that a particular stakeholder should have open access to all data types, while

others drew attention to the potential privacy concerns that could arise and questioned whether the stakeholder really access to the data.

TABLE I. SAMPLE OF DATA ACCESS REQUIREMENTS TABLE

User Type	Data Types			
	Learner Profile Data	***Competence Profile***	***Social Contact Data***	***Learning Plans***
Other Learners	Yes, but anonymous	Yes, but anonymous	No	No
Mentor	Yes for people they are responsible for	Yes	No	Yes
Supervisors	Yes for people they are responsible for	Yes	No	Yes
Competence Managers	No	Yes in an aggregated way	No	No
Internal Recruiter	Yes, but anonymous	Yes, but anonymous	No	No

We adopted this approach for the following reasons. Due to the early stage in the development process, there was no documentation outlining the system architecture or data models, and most decisions in this regard were yet to be taken. By working collaboratively to identify user types and data types and then determine the level of access in each cell, we were able to systematize the discussion in the absence of these documents.

Our approach is consistent with Adams' privacy framework [2, 3] and her recommendations concerning how the framework can be applied in design. The *information receivers* are the different user of the system, i.e., learners, mentors, HR personnel, etc. The *information sensitivity* was implicitly represented by the different data types and the workshop participants anticipation of how they could be perceived by end users. However, in order to actually measure how sensitive each data type is, actual user perceptions will have to be studied. Finally, *information usage* emerged from the discussion of why – to which end - users should be able to access certain data.

The project does at this point not have actual learners. To add their perspective, we organized privacy workshops with student participants taking on the role of learners. In 90 minute sessions, participants were introduced to the TARGET system through a demonstration video. The demonstration presented the main social space within the game environment (a 3D 'lounge' area where players could interact with each other via avatars) and a game scenario. In the game scenario, a player interacted with a computer-based character to achieve a project task. During and after the demonstration, participants were asked to comment freely e.g. about what they liked and disliked about the game, what they would they change to improve the game etc. During the discussion, participants were asked how they felt about the collection and retention of certain types of data (e.g. game performance data) in view of certain potential uses (e.g. internal recruitment). They were also asked about their preferences with regard to their identity and game performance data vis-à-vis other players e.g. were they happy to have profiles listing their real name. Additionally, participants were asked about how they would like to give consent to the collection and use of their personal data.

V. FINDINGS

We carried out a thematic analysis of the collected data and focused on the issues which were mentioned by the most people and more frequently since we believe these are good indicators of the most serious privacy risks. Participants are identified with a letter (D for developer and P for focus group participant) and a code number.

The concerns raised were based on a corporate deployment scenario, i.e., where learners are employees of a company. The majority of issues identified were related to performance data and how it could be used by colleagues or HR personnel. Other topics that were covered include the matching of system data to real-world data, feedback and consent, control over game data, the possible stigma associated with using a learning tool and interaction between TARGET and HR systems. Findings from workshop, focus groups and interview were combined and organized by topic.

A. Performance Assessment

The TARGET game will provide feedback to players regarding their performance within different game scenarios. Although this feature has yet to be implemented, it was frequently discussed in both the developer workshop and the focus groups.

1) Sharing with Colleagues

After viewing a demonstration of the system, many focus group participants were very keen for the game to include more competition elements. One suggestion was to provide players with scoreboards at the end of game scenarios, to allow them to compare their performance with the performance of other players. However, some participants expressed concern with the potential *"friction"* that could result from everyone being able to see everyone else's score. Others suggested that scores could be used by colleagues against each other in the real world. One participant (P1-3) suggested a feature that allowed players in a team exercise to post feedback about their team mates' performance. Again, others (P1-1 and P1-2) suggested that this feature could also lead to friction, and potentially reduce user motivation to play the game, since many people would not want negative comments to be posted. These comments suggest that performance data is potentially sensitive. While allowing players to see the scores of other players could enhance competition, it may also generate friction.

Adams [2] argues that data that can portray the user in a negative way is more sensitive if seen by someone he or she has a close relationship with such as a friend or colleague. When the data does not portray the user in a negative way, it is less sensitive. In fact, some participants (P2-1 and P2-3)

mentioned they wouldn't see any problems in sharing their game performance results if they were good.

2) Monitoring by Human Resources

Within each focus group, it was suggested that Human Resource (HR) personnel might want to monitor and store player performance data, and that this data could be used to guide internal recruitment. Most participants reacted negatively to this possibility. One (P2-2) said he would be reluctant to play the game if his performance data was stored and used in this way. Another participant (P2-1) said that this data use would change how she played the game: she would try to play the scenarios that she was good at and avoid the ones where her performance was not as good. If she was not good at any, she would not want to play the game. By contrast, if her performance scores were anonymous, she would *"feel free to explore stuff that I am not good at and try to learn from it."*

According to Adams [2], the privacy implications of an interaction are greater when the data receiver has power over the individual disclosing the data. In this case, performance data becomes more sensitive when the recipient is someone in the HR department that can use the data to allocate employees to specific roles. The possibility that some players would be put off by this data usage and engage in protective measures would defeat the purpose of deploying such a system and constitute a serious risk for the employer. In particular, if users avoid exploring or experimenting with scenarios they are not good at, then their learning experience would be greatly undermined.

While most participants had a negative attitude towards this use of performance data, some noted some potential positive implications. Two (P3-1 and P2-2) argued that it could provide an opportunity for career driven people to *"climb up the ladder"*. One of these participants (P3-1) added that knowing that game performance could be used for monitoring competence levels would make her *"play to win."*

3) Type of assessment

Some focus group participants questioned whether performance assessment carried out by the learning system could correctly reflect the real world capabilities of learner and, therefore, whether decisions based on this information could ever be fair or effective. One participant (P2-3) said: *"you can just click something in that game and it doesn't really say if you do it as good in real life"*. She thought that certain 'human' elements, such as facial expression and body language, that normally form part of recruitment decisions would be missing if the recruitment process relied solely on performance assessment information produced by the system. An alternative point of view was that recruitment based solely on automatic assessment was likely to result in fairer decisions, since the process would be less biased than a face-to-face evaluation, where people are *"judge[d] by the way they look"*. However, one participant (P3-2) was quick to add that the prejudice could still exist even with automatic assessment if the final decisions were made by humans.

These comments suggest that the degree to which learners perceive performance data as sensitive may depend on how the data is used (e.g. for recruitment purposes) and on the particular process employed (e.g. will it replace other recruitment processes or augment them?). In addition, it suggests that perceptions are likely be influenced by how existing processes are viewed. Some individuals may favor face-to-face evaluation because they believe they can more easily control the disclosure of information. Other individuals may favor the automatic process because some data items, like physical characteristics, are impossible to hide in face-to-face interviews.

The type of assessment and how it is presented has also an impact on sensitivity. As a participant mentioned (P3-2), a psychological score has a different level of sensitivity than an arcade game like score.

B. Identifying information

Several focus group participants thought there shouldn't be a connection between the game data and real world data, that is, it should not be possible for players to link the game profiles of other players to the actual person. In another focus group presented with this issue argued that knowing the real name of other players increased realism and the competitive element of the game, but that could also be used against them – when aggregated with performance data – by their colleagues. One participant (P3-2) of this group was of the opinion that only details like first name, job, and age should be public, so that it would become possible to ask them for help or advice directly. It would also enhance the team building aspect of the game since *"one part of team building is getting to know people and that involves asking questions and talking to people."* If the game provided all the information about a person immediately he felt that element would be lost.

Individuals manage their relationships through selective disclosure of personal information [13]. Since the learning experience of TARGET is sometimes based on group exercises it should be left to players to decide how, when and what part of their identifying information to disclose to their fellow players. In fact, some participants expressed a desire to control what part of their profiles would be visible.

In any case, stable identities, connected to real identities or not, are important because they allow participants in repeat transactions to build up trust across time. If participants are able to recognize each other and think they will interact again they have an incentive to fulfill each other's requests [16].

C. Feedback and consent

When discussing consent forms in one group, a participant (P3-2) mentioned that the form should inform the players of who has access to their data and who has not so as to avoid any misunderstandings. He added that this form should be accessible to the player after he had signed in a read-only format. In the workshop, a participant brought into attention the fact that if an employee is under pressure to use the learning system then there is no true consent even if he signs a form. Friedman et al. [9] consider voluntariness a necessary condition for informed consent, i.e., the

individual should not be coerced or manipulated into giving consent.

D. Control

A member of another group (P2-2) argued that game data should be kept within the company that deployed the game since the game was specific to that company. When data is transferred out of its context it can lose important contextual cues which cause it to be misinterpreted [2]. On the other hand, since TARGET focuses on transferable skills such as project management, it could be valuable for an individual to be able to take his performance data outside the organization where it was collected. For example, if he was applying for a new job, he might want to prove he had specific competences by providing this data.

E. Stigmatisation

One issue that came up during the workshop with the developers was that employees do not want to be profiled as needing some kind of special education or training. One of the developers present (D1) had previously worked in a project aimed at updating certain employees' technical knowledge. That project was met with a lot of resistance because potential users perceived that being singled out for training meant that their future employability within the company was affected. In the words of the developer, they thought *"I am one of these who will be the first to be laid off when the company shrinks"*.

The possible stigmatization effect of being selected for training indicates that the simple fact of using a competence development system can constitute sensitive information for the player. This is something that has to be taken into consideration by the developers of learning systems, especially if they're deployed in business environments.

F. Interaction with HR systems and personnel

It is likely that TARGET will interact with the HR systems of the organizations where it is deployed. In the workshop it was acknowledged that this would introduce new privacy concerns. Aggregation of data stored in various systems can have the effect of sensitizing data that alone was not sensitive. Data collected or disclosed in a specific context which is then used in another context looses important contextual cues that affect how it is interpreted [2].

Companies have review processes to make sure that these issues are considered before approving access to HR systems. In any case, it is possible that HR personnel will be able to match a user profile to a real person for internal recruitment purposes.

VI. Conclusions and Initial Recommendations

These exploratory inquiries into possible privacy issues in TARGET have allowed us to identify some general sources of concern with regard to privacy in competence development tools. Most of the identified concerns result from a dichotomy between the interests of learners in keeping certain information private and the interests of companies deploying the system in using that information to fulfill certain organizational needs. However, it is our belief that fulfilling the learners' privacy requirements is also in the best interests of the organizations deploying competence development systems, since it will reduce negative attitude towards the system and improve the learning experience.

The privacy issues identified are not simply dependent on the type of learner related data that is collected; they also depend on who has access to that data and what they do with it. Thus, our findings are consistent with Adams' [2, 3] privacy model, and suggest that the model is applicable in domains beyond multimedia applications.

Before competence development systems are deployed in organizations there is usually, depending on the country, a negotiation process between representatives of the employees that are going to use the system – such as trade unions – and the employer. We propose that our list of initial findings (TABLE II. can be used as a guide or checklist of concerns that need to be addressed during that negotiation process.

TABLE II. Checklist of Privacy Concerns

Theme	Issues	Benefits
Performance assessment	If performance assessment/scoreboards are public it cause friction between colleagues (if linked to real people)	Increases competition elements of experience. Becomes more like a game.
	Feedback from colleagues on each other's performance could cause friction	
	Fear that performance assessment can be used by colleagues against each other	Can be used as an additional item for the organization to make internal recruitment decisions
	Using assessment to guide internal recruitment can lead users to reject technology or manipulate it to obtain good results impacting the learning experience	Can increase effort on the part of players to achieve learning objectives.
	Automatic performance assessment carried out by system could be perceived as not translating to real world capabilities	Automatic assessment less biased that face-to-face assessment. How you look does not matter.
	Automatic performance assessment carried out by system can be susceptible to abuse.	Opportunity for career driven people.
	Using the system to aid internal recruitment can mean that system has to interact with organization's HR systems	
Selecting employees for competence development	Employees can feel stigmatized for being singled out for training. Associated with being more prone to be laid off.	Employees can develop their competences

Identifying information	Increases sensitivity of performance assessment data.	Linking game profiles/avatars to real people increases realism.
	If system provides too much identifying information off the bat than team building element is lost. Part of team building is asking questions.	
Consent and feedback	Relying on employment contract as consent to collect and use learners' data and not providing a specific consent form for this system can be perceived by the users/trade unions as insufficient feedback on data practices	

VII. FUTURE WORK

In the next phase of this research, we will carry out one-on-one interviews with potential users of the system. The objective will be to elicit any fears or perceptions that potential users of the system have with regard to the collection and usage of their personal data. During these interviews, potential users will be confronted with scenarios that depict how specific data types may be collected and used by their employer. The aim will be to see what they are comfortable and uncomfortable with and why. It will also be necessary to talk to stakeholders of the companies that are going to use the system at this point in order to understand how they plan to use the data present in the system. Finally, when a working prototype of the system is available, diary studies will be conducted with potential users. The aim here is to evaluate how real users interact with the system to corroborate earlier evidence and identify privacy related issues that have not been previously identified. This last phase is especially important because it has been showed that people find it difficult to reason about privacy in the abstract [14] and that there is often a discrepancy between reported privacy attitudes and actual behavior [6].

REFERENCES

[1] Ackerman, M.S. & Mainwaring, S.D., 2005. Privacy Issues and Human-Computer Interaction. In *Security and Usability: Designing Secure Systems That People Can Use*. Sebastopol, CA: O'Reilly, pp. 381-399.

[2] Adams, A., 2001. Users' Perceptions of Privacy In Multimedia Communications. PhD. University College London.

[3] Adams, A. & Sasse, A., 2001. Privacy in Multimedia Communications: Protecting Users, Not Just Data. In A. Blandford, J. Vanderdonckt, & P. Gray, eds. People and Computers XV - Interaction Without Frontiers: Joint Proceedings of HCI 2001 and IHM 2001. London: Springer, pp. 49-64.

[4] Andersen, B., Fradinho, M., Lefrere, P. & Niitamo, V., 2009. The Coming Revolution in Competence Development: Using Serious Games to Improve Cross-Cultural Skills. In *Online Communities and Social Computing*. pp. 413-422.

[5] Anwar, M.M., Greer, J. & Brooks, C.A., 2006. Privacy enhanced personalization in e-learning. In Proceedings of the 2006 International Conference on Privacy, Security and Trust: Bridge the Gap Between PST Technologies and Business Services. Markham, Ontario, Canada: ACM, pp. 1-4.

[6] Berendt, B., Günther, O. & Spiekermann, S., 2005. Privacy in e-commerce: stated preferences vs. actual behavior. *Commun. ACM*, 48(4), 101-106.

[7] Clark, R. C., & Mayer, R. E., 2007. E-learning and the science of instruction: Proven guidelines for consumers and designers of multimedia learning. San Francisco: Jossey-Bass/Pfeiffer. Second edition.

[8] El-Khatib, K., Korba, L. & Lee, G., 2003. Privacy and security in E-learning. *International Journal of Distance Education Technologies*, 1(4), 1-19.

[9] Friedman, B., Lin, P. & Miller, J.K., 2005. Informed Consent by Design. In *Security and Usability: Designing Secure Systems That People Can Use*. Sebastopol, CA: O'Reilly, pp. 495-521.

[10] Hine C. & Eve J., 1998. Privacy in the Marketplace. *The Information Society*, 14, 253-262.

[11] Iachello, G. & Hong, J., 2007. End-user privacy in human-computer interaction. *Found. Trends Hum.-Comput. Interact.*, 1(1), 1-137.

[12] Jerman-Blazic, B. & Klobucar, T., 2005. Privacy provision in e-learning standardized systems: status and improvements. *Computer Standards & Interfaces*, 27(6), 561-578.

[13] Kitts, J.A., 2003. Egocentric Bias or Information Management? Selective Disclosure and the Social Roots of Norm Misperception. *Social Psychology Quarterly*, 66(3), 222-237.

[14] Lederer, S., Hong, I., Dey, K. & Landay, A., 2004. Personal privacy through understanding and action: five pitfalls for designers. *Personal Ubiquitous Comput.*, 8(6), 440-454.

[15] Nejdl, W. & Wolpers, M., 2004. European E-Learning: Important Research Issues and Application Scenarios. In *Proceedings of ED-MEDIA 2004, World Conference on Educational Multimedia, Hypermedia & Telecommunications*. Lugano, Switzerland: Association for the Advancement of Computing in Education (AACE).

[16] Riegelsberger, J., Sasse,A. & McCarthy, J.D., 2007. Trust in Mediated Interactions. in Joinson,A., McKenna,K.Y.A. Postmes,T., Reips, U. D. (ed.) *Oxford Handbook of Internet Psychology*. Oxford: Oxford University Press, 53-69. ISBN: 978-0198568001

[17] Van Eck, R., 2006. "Digital Game-Based Learning: It's Not Just the Digital Natives Who Are Restless," *EDUCAUSE Review*, vol. 41.