Trusting to Learn: Trust and Privacy Issues in Serious Games

Miguel Malheiros, Charlene Jennett, Will Seager, and M. Angela Sasse

Dept. of Computer Science, University College London (UCL), Gower Street, WC1E 6BT, UK
{m.malheiros,c.jennett,w.seager,a.sasse}@cs.ucl.ac.uk

Abstract. Organizations are increasingly investing in technology-enhanced learning systems to improve their employees' skills. Serious games are one example; the competitive and fun nature of games is supposed to motivate employee participation. But any system that records employee data raises issues of privacy and trust. In this paper, we present a study on privacy and trust implications of serious games in an organizational context. We present findings from 32 interviews with potential end-users of a serious games platform called TARGET. A qualitative analysis of the interviews reveals that participants anticipate privacy risks for the data generated in game playing, and their decision to trust their fellow employees and managers depends on the presence of specific trust signals. Failure to minimize privacy risks and maximize trust will affect the acceptance of the system and the learning experience – thus undermining the primary purpose for which it was deployed. Game designers are advised to provide mechanisms for selective disclosure of data by players, andorganizations should not use gaming data for appraisal or selection purposes, and clearly communicate this to employees.

Keywords: trust, privacy, serious games, technology-enhanced learning.

Introduction

Organizations are increasingly turning to e-learning solutions to save time and travel costs associated with traditional training through outside courses [1]. *Serious games* – which facilitate learning whilst simultaneously entertaining and engaging learners – are emerging as a promising e-learning solution.The simulation of real-world experience is thought to improve transfer of learning to applied contexts [2],[3].Also, the competitive element of serious games is a source of motivation for players; thus serious games have already been deployedas part of some corporate learning programmes.

To develop competencies, serious games deployed in organizations need to collect and store personal data. Research suggests that privacy and trust can be important factors influencing user acceptance and the effectiveness of specific systems [4], [5], [6]. When these concerns are not addressed, the potential consequences of workplace monitoring include – low employee morale, chilling effects, deterioration of work relationships, reduced commitment to the organization, lower productivity and economic loss [7], [8], [9], [10].

Although some research has been carried out on the impact of privacy issues on technology-enhanced learning (TEL) [11], [12], [13], it has focused on types of data assumed to be sensitive, and how generic privacy technologies could be used to protect it. There is currently a gap in the literature regarding the specific privacy and trust issues of learning systems: (1) how learner-users perceive and react to different data practices and interactions with other stakeholders, and; (2) what impact this can have on system acceptance and effectiveness. There is also a lack of methods to help TEL developers incorporate privacy and trust considerations into the design of their systems.

In this paper, we describe an investigation of privacy and trust issues in TARGET, a platform for developing serious games. The aim of our research was to understand how the design and configuration of TARGET-based games might impact privacy and trust perception among employees, and to develop guidelines for designing and operating such games in organizational contexts. The first game being developed aims to support the rapid development of competence in project management skills. Thirty-two interviews were conducted with potential end-users of TARGET – 16 focused on privacy and 16 on trust – and analyzed using Grounded Theory. The results show that participants' perceptions of privacy risks depends on the validity of the data collected, the extent to which it is linked to an individual, and the data receiver, among other factors; while their level of trust in other players and management depends on the presence of trust signals, such as the existence of a code of conduct for players' behavior in the game, or a clear statement of purpose for the game. Based on these results, a joint framework of privacy and trust was created where the perception of privacy risks is related to having trusted relationships with other stakeholders.

In Section 2, we describe TARGET and review related research on privacy and trust. In Sections 3-5, we present our research aims, methodology and findings. In Section 6, we present our conclusions and several recommendations for practitioners.

Background

TARGET

TARGET (Transformative, Adaptive, Responsive and enGaging Environment) is a collaborative project 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 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 project management experiences that characterize the real-world [14]. TARGET also aims to foster the development of communities of practice [15], [16] and promote social learning, enabling players to interact with each other via multi-player gaming and other social tools. TARGET is intended for use within enterprise environments, academic environments and interest-focused communities.

Privacy in TEL and Multimedia Systems

Research on TEL has identified privacy as an important issue in the field – in particular, *linkability* of data, *observability* of data, *identity disclosure* and *data disclosure* [11], [12], [13]. These views reflect a "data-centric perspective" that

assumes that specific data items are sensitive; it does not take the contextual nature of users' privacy perceptions into account. Privacy is "*individually subjective and socially situated*" [17]– there is no specific type of information which is considered personal in all situations, and no situation which is seen as a privacy violation by all persons [18]. It is, therefore, necessary to understand which factors influence the way individuals perceive different data practices.

According to Adams [4], technology users' privacy perceptions depend on: (1) sensitivity of the information being broadcasted; (2) the information receiver, and; (3) usage of the information[1]. Users evaluate the sensitivity of the information they are broadcasting not in a binary way – sensitive vs. non-sensitive – but according to a "*scale of sensitivity*"; depending on how "personally defining" the information is deemed to be and how the user predicts others will interpret the information. If individuals think that the information being disclosed "*will be used to draw reliable and valid inferences about them*" and is relevant for the interaction they will consider it less privacy invasive [19].

The level of trust and the type of relationship with the information receiver also determines how an individual sees the privacy implications of a disclosure[19]. Data that can portray the user in a negative way is more sensitive if seen by someone she has a close relationship with –e.g. friend or colleague– than by a stranger[4]; for this reason, both current and future information flows should be clarified so that users know who will see their data [20].

Information usage is assessed by looking at the way the information is being used in the current moment and can be used in the future [4]. When data is recorded, for example, it gives more control to the data receiver. The receiver can then edit it or broadcast the data at a later date, which can cause it to lose contextual cues, increasing its sensitivity [4]. Although it is true that users evaluate the situation more negatively when they perceive a loss of control [19], they will make the trade-off if they think that the benefits of a specific current data usage outweigh the risks of a harmful future usage [4].

All the above factors are influenced by the context in which the interaction takes place. Trust in the organization deploying the system will affect how risky from a privacy point of view users think the technology is [4]. Auser's past experiences, knowledge and preconceptions of the technology, and the level of interaction s/he will have with it, will also have an influence on his/her perceptions [4], [18], [21].

Privacy has been addressed in TEL literature in a generic way, which does not take into account the context in which the learning technology is deployed, or the users' views of specific privacy issues with it. Since our research aim is to understand how privacy and trust influence user acceptance,a user-centered model – i.e. Adams' privacy model [4] –provides a suitable starting point forexamining how privacy is perceived in serious games in organizational contexts.

Trust in Technology-Mediated Interactions

Riegelsberger et al. [6] argue that trust and the conditions that affect it must become a core concern of systems development. *Trust* is defined as "*an attitude of positive*

[1] Adams' privacy model [4] is the result of empirical studies in multimedia communications but comprehensive enough to be applicable to other technologies.

expectation that one's vulnerabilities will not be exploited"[6], [22], [23], [24], [25]. In their framework, Riegelsberger et al. identify contextual and intrinsic trust-warranting properties that designers should provide to encourage trustworthy behavior and enable well-placed trust (also see [26]). Contextual properties are the most relevant for our purposes.

Contextual properties are attributes of the context that provide motivation for trustworthy behavior. There are three types: temporal, social and institutional [27]. A trustee's motivation to fulfill will increase if the trustee believes that they will interact again with a particular trustor (*temporal embeddedness*). *Stable identities* and *information about the likelihood of future encounters* will influence this property. *Reputation* information – e.g. honesty, reliability, dependability – provides an incentive to fulfill for trustors who are socially embedded, because of the trustee's interest in future interactions with trustors who may gain access to this reputation information (*social embeddedness*). Factors that influence the effect of reputation are: identifiability, the traceability of trustee actions, the social connectedness of the trustor, the topology of the social network, the cost of capturing and disseminating reliable past information, and the degree to which such information itself can be trusted to be truthful. Institutions can support trustworthy actions by providing incentives and sanctions (*institutional embeddedness*), but to have an effect on a trustee's behavior, his or her actions must be traceable, and the cost of investigation and sanctioning must be low compared to the cost of non-fulfillment.

Applying their framework to the context of voice-enabled online gaming, Riegelberger et al. [6] make a number of suggestions for how online games can support well-placed trust and trustworthy behaviors: stable identities, block lists, reputation scores, enforcement bodies, player-formed groups/organizations, profiles containing personal information, buddy lists (with presence indicators) and communication tools such as email and chat. Such features could also support trust in the TARGET platform – however, being a serious game for use in an organizational setting, it is possible that other factors would also be at play.

Research Aims

The frameworks of Adams [4] and Riegelsberger et al. [6] have revealed a number of factors for creating and sustaining privacy and trust in computer-mediated interactions. However, it is uncertain whether the same privacy and trust issues would be identified for serious games in an organizational context. Although Adams [4] does mention that trust in the information receiver (trustee)affects users' (trustors')decisions (see section 0) there is no elaboration of how which factors influence that trust decision, and in turn privacy. The current research aimed to extend upon the previous literature by answering the following questions:

1. What are the specific privacy risks that players associate with TARGET?
2. How do players expect their data to be used by key stakeholders, such as managers and other employees (trust dynamics)?
3. How do privacy and trust interact in this specific context?
4. What design recommendations can be made to support privacy and trust in TARGET and other learning platforms in organizations?

Interviews were conducted with 32 individuals (16 on privacy, 16 on trust) whose profile matched that of potential TARGET users. The data was then combined to explore the interplay between privacy and trust. It is a challenge to anticipate the privacy risks of a system before that system is fully developed. This study relied on: (1) a demo of a TARGET game to help participants envision the system, and how they would interact with it; and (2) scenarios of potential uses of player's data to contextualize the questions and elicit more realistic reactions from participants. (Scenarios are commonly used in privacy research – see [5])

1 Methodology

1.1 Participants

Participants had to have at least 1 year of work experience in large (more than 100 employees) organizations. 27 were recruited online and the remaining 5 through personal contacts. 17 were female, 15 were male. Ages ranged from 20-59, the median age being 26 years. 18 participants worked in the commercial sector, 11 in the public sector and 3 selected "other". The median sizeof participants' organizations was 800 employees. 25 participants had experience of playing digital games.

1.2 TARGET Demo Video

The demo video introduced participants to the TARGET platform. They were told that learners interact with other characters – real people represented by avatars or computer-based characters – within in a 3D virtual environment. The system provides several stories that the learner can play to develop skills such as leadership, communication, or conflict resolution. Within each story, the learner can develop multiple competencies. The system also provides a 'lounge' – a social space, where learners can interact with each other. Several types of data can be generated and/or stored by the system. These data types are explored in the scenarios.

1.3 Scenarios

Several scenarios and interview questions were created to elicit responses to privacy and trust. The scenarios were based on: (1) a workshop with TARGET developers, (2) focus groups conducted with prospective learner-participants, and (3) Adams' privacy model [4].The privacy scenarios portray situations with different data receivers, types of data, and data usages; with an emphasis on performance data:

1. displaying performance data as a score on a public scoreboard and alternatives to that option;
2. use of aggregated performance data to guide training decisions;
3. the use of performance data to guide internal recruitment decisions;
4. playing a scenario with other players with everyone using pseudonyms;
5. the player profile, the information it contains, and other players' access to it;
6. interaction with other players in the game scenarios and lounge.

Riegelsberger et al. [6] advocate not only designing to support well-placed trust, but to incentivize trustworthy behavior. The trust scenarios explore: (1) trust in TARGET, and (2) trust in other players of TARGET. The scenarios topics were:

1. implementation of TARGET in an organizational setting;
2. data access;
3. use of data, e.g. score boards, recruitment, identification of training needs;
4. initial contact with other players;
5. maintaining/limiting contact with other players;
6. realvs. pseudonymous identities.

1.4 Procedure

Interviews were semi-structured and conducted in a lab setting. Each participant was shown a 3 minute demo of TARGET and was briefed on the main features of the system. They were asked to imagine several scenarios related to the game and how they would respond if it happened at their organization. Privacy interviews lasted 60-90 minutes, and participants were paid £15. Trust interviews lasted 30-60 minutes and participants were paid £10. All interviews were audio-recorded.

Transcripts were coded using a qualitative methodology known as grounded theory [28]. Using open coding, axial coding and selective coding, two researchers created separate grounded theories for privacy and trust. The codes were pooled and underwent a further round of selective coding to create a joint framework, wherein privacy refers to vulnerabilities associated with game data, and trust refers to specific vulnerabilities associated with information receivers.

2 Findings

The framework shown in Figure 1 will be explained in three parts:

- Players'interaction with the system (1)
- Players' interaction with other stakeholders: player-manager interaction (2) and player-player interaction (3).

When numbers are given in support of codes, the number of participants from the privacy and trust interviews will be followed by P and T respectively.

2.1 Players' Interaction with the System

Players interact with the system through two game areas: game scenarios and lounge. When playing game scenarios, the performance of the player will be analyzed and transformed into a performance assessment. The time spent playing and the different game scenarios played can also be recorded. When players interact with other players in the lounge (by text or voice), the conversations could – from a technical point of view – be stored. Demographic and job-related data could be aggregated into a profile that would identify the player when interacting with others.

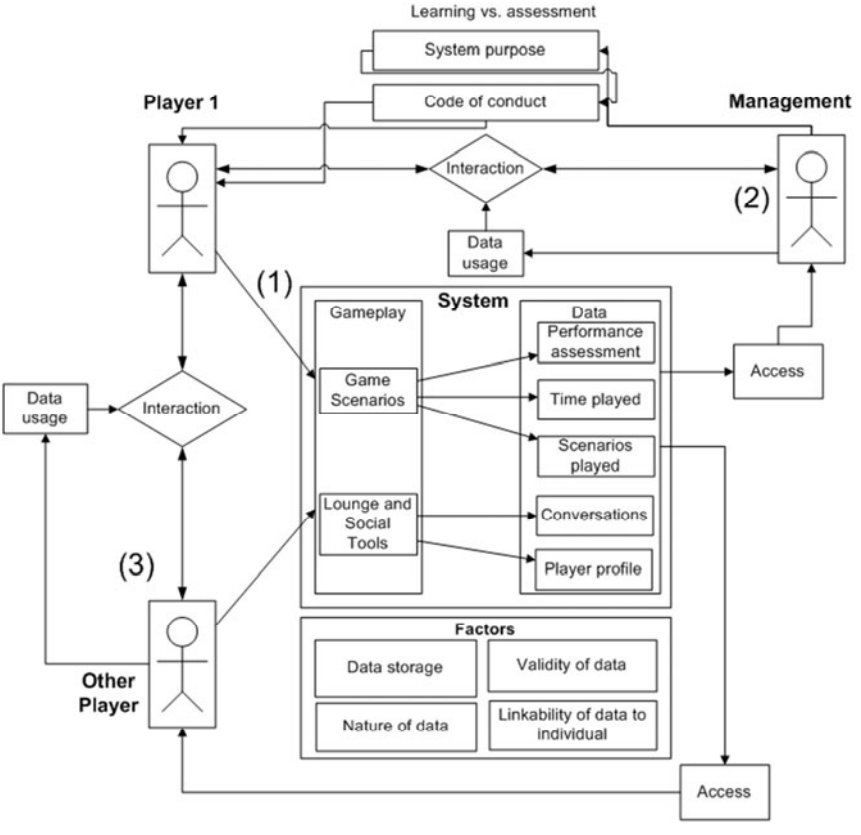

Fig. 1. Stakeholder interactions

Participants' privacy concerns centered around: (1) data storage (2) nature of the data; (3) validity of the data; and (4) linkability of the data to the player.5(3P, 2T) participants wanted to know where game data would be stored, and what kind of *security measures* would be deployed. One perceived risk was that the management of the data might be outsourced to another company, or even sent outside the country or the E.U. Another risk was that there could be a security breach that resulted in unauthorized people getting access to a player's personal data.

The *impression of the player* that the data projected to others was a major concern. If the data showed the player in a good light,s/he might not mind sharing it. If the data revealed weaknesses or shortcomings, the player would prefer it not to be public. 15 (7P, 8T) participants mentioned that a poor performance assessment could make other people in the organization think the player was not good enough to perform his job. Time spent playing and game scenarios played were also considered sensitive: by seeing which scenarios another player had played, it might be possible to infer his/her weaknesses. If a player had played the game for much longer or much less than what was expected in the organization, this could be perceived negatively.

25(13P, 12T) participants questioned the *validity of performance assessment*– i.e. the system's ability to correctly gauge real job-related competencies. One concern was that the game scenario might not be a realistic portrayal of the actual task because communication within the game occurs through a computer. Also, the game might not cover enough relevant aspects of the job domain; if this was the case, it was thought to be unfair to assess an employee based on their performance in the game.

5(3P, 2T) participants said they would prefer human assessment to an automatic one, because a human assessor can probe and ask questions, while a computer cannot. Another (1P) participant argued that an automatic assessment is fairer because it does not rely on the subjective judgment of a manager.

A further issue was external factors that couldhamper a player's performance: experience with computer games and computers in general; technical problems (e.g. the system crashing), and personal issues (e.g. returning from maternity leave, a recent family bereavement, or having a bad day). Participants proposed that player's overall personal context should be considered when assessing his performance, and that there should be a way for players to correct or erase erroneous data.

The extent to which game data is *linked to an individual*also affected players' perceptions. 13 (4P, 9T) participants mentioned that the use of pseudonyms instead of real names would have a positive effect on how they perceived the system. The use of pseudonyms couldallow a player to interact more freely with the system, feel less embarrassed, pressured, andthreatened.On the other hand, the use of pseudonyms could also make a player lose interest in the game – if a player's performance cannot be traced back to him/her, there is less incentive to take the game seriously (1P).

Regarding aggregationof performance data, 7 (7P) participants said that they would view this as less threatening than displaying individual data. This would make itmore difficult to identify individual players who did notperformwell. Players would feel free to experiment and choose riskier options. 3(3P) participants even argued that – since in most organizations work is usually done in teams – aggregation on a work group or team basis would be more appropriate.

A possible limitation of aggregation was the risk of "tarring everyone with the same brush" – e.g. one player could be given unnecessary training because s/he was part of team that had not performed well on a specific task (6P). If there is no way of knowing which individual had not performed well, some players might work less (3P).It was viewed as important to provide feedback at the individual level, so that the player would know what s/he had done wrong and whatto do to improve (4P).

2.2 Interactions with Other Stakeholders

Different *roles in the organization* should have different levels of access to their game data; but there was no consensusabout what those access levels should be for each role. Participants distinguished between *colleagues and management*. 19 (9P, 10T) participants said that management should have access to their game data, but not colleagues. 6 (3P, 3T) participants had the opposite view, arguing that it was precisely from people who *had power over them* that they would want to protect data from. One factor was whether the potential receiver had a*legitimate purpose* for accessing the data. Other factors included the personal and work *relationship* they had with that individual, how much they *trusted* him/her, and the department s/he belonged to (3P).

In the remainder of this section we will provide more detail regarding participants' perceptions of potential issues that can result from a player's game-supported interactions with management or other players.

2.3 Player-Manager Interaction

Managers would have an interest in players' game data because it provides an easy way of checking their employees' performance and assessing their skills. However, our interviews revealed that, if not handled in an appropriate way, such data use could be perceived as a major threat by employees. Participants were receptive to positive uses of game data that led to constructive criticism on their performance, or new job opportunities, but they were apprehensive about the use of game data for making decisions about promotions or redundancy. There were two perceived risks: (1) unfair assessment, and (2) negative perceptions of game play.

Regarding unfair assessment, one concern was that managers'*data use*would not be transparent. 18 (7P, 11T) participants worried that – if game data that for training purposes was subsequently used for assessment – they might be perceived negatively. While *training*was associated with exploration and trying out new approaches to problems, *assessment*meantemployeeshad to try their best. A player under the impression that the game's purpose was training might not perform optimally.

Another concern was that managers would *over-rely* on the performance assessment data to identify skill levels. Related to the *validity* of the performance assessment (see Section 5.1), participants did not want their data to be taken out of context. A distinction was made between *new recruits* and *current employees* (4T)– game scenarios might be too simple for senior employees. Also, whereas managers have little knowledge about the competencies of new recruits, they should already have knowledge of their current employees.

Negative assumptions can also be made about other game data(see Section 5.1). To overcome this perceived risk, participants wanted management to provide clear guidance in terms of *how much time* they would be expected to play the game, and *when* they should play it. For example, can they play the game anytime during work, or only during set hours? Can the game be played at one's desk, or only in a separate training environment away outside of the office?The possibility of conversations being *monitored* in the lounge or game scenarios was another concern. Monitoring was viewed as an invasion of privacy, and would put participants off networking.

2.4 Player-Player Interaction

Players are interested in interacting with each other because it can add to the fun of the game–socializing with colleagues and developing skills together. Butthere were two perceived risks of interacting with other players: (1) unpleasant interactions; and (2) negative use of information gained during game play.

Firstly, other players might act in an inappropriate manner during game play (e.g. swearing, abusive language). Participants wanted management to provide *clear guidelines* as to what behavior is and is not acceptable within the game environment. If the workplace made it clear that there would be reprimands for misuse of the game, participants believed that this would encourage trustworthy behavior from users.

Real-life consequences for good performance in the game would be further motivation for good behavior.

Secondly, information gained during the game interaction might be used against the player. Participants were worried that if they played against a senior colleague or manager and performed poorly, then *negative assumptions* might be made about their competence in real-life (3P, 8T).Bad performance in game scenarios could also be used by a player's peers to *humiliate*him/her (4P, 10T)–in the form of gossip, ridicule or bullying. Career-oriented colleagues might try to use that information to *gain leverage* on the player – if, for example, they were both competing for the same job or were in conflict (6P, 8T).

The use of pseudonyms was viewed as a way of protecting employees from the repercussions of low performance, by reducing the *linkability* of the data (see Section 5.1). Pseudonyms might prevent real-life biases and prejudices from contaminating in-game interactions and affecting performance. This could improve learning as players might interact in a more neutral way by starting from a "clean slate".

A perceived limitation of pseudonyms, was that it could have a negative impact on *socialization*. Players feeling less accountable for their actions might behave less responsibly.They might disclose more personal information if real identities were not known. Such behavior could have repercussions for their relationships in real-life, if their pseudonym identity was found out. 14 (8P, 6T) participants said that they would be reluctant to interact with other players if they did not know who they were; they would be wary of other players acting in an inappropriate manner, and find it difficult to determine the potential benefits of the interaction.

3 Discussion

The findings identified a number privacy risks that players associate with TARGET – data storage, nature of the data, validity and linkability. With managers, the risks are related to negative career consequences – being viewed as incompetent, or being made redundant.With other players, the risks are related to negative social effects – unpleasant interactions and humiliation.

Players want to keep a certain degree of separation between their real-world job and the game interactions. They did not want data that could show them in a negative light to transfer from the game to the real-world, or vice-versa. However, to achieve this, game playing would become a fairly insulated experience. Not only would this reduce the level of constructive feedback that players can get from their managers or other employees, but it could also work against organizational interests –such as integrating game experiences with social networking or communities of practice. Furthermore, in order to realize the benefits of serious games – where part of the motivation comes from the competitive element – it is important to allow players to compare their performances to each other while assuring that the data collected for that purpose won't be applied outside the learning context.One possible way forward is to allow selective disclosure of data by players and creating a trustworthy environment where they are not afraid to share data.

The actual purpose of the system, and the way the purpose is communicated to users, will have an impact on acceptance. The system described in this study is a

learning tool, with the primary focus of developing project management skills. But it could also be used for assessment– this makes gaming appear more risky to users, and undermines the primary purpose – learning.If assessment is used, there should be distinct modes for learning and assessment.

Whether the evaluation of players is human or automatic will also impact acceptance. There is a dilemma –human assessors are expensive, andmay have biases; but they allow players to explainand contextualize their performance. Purely automatic assessment would make it difficult for a player to explain his or her results. One possible way to address this issue is to have automatic assessment, but allow players to correct or erase erroneous data.

In some game situations, there could be a trade-off between trust and privacy. While the use of stable identities associated to avatars contributes to trustworthy behavior(by providing temporal, social and institutional embeddedness) and builds relationships between players [6], it can work against players if management use performance data to make decisions that have a negative impact for players' careers. Moreover, the game experience could be affected if real-life biases and prejudices transferred into the game. The use of pseudonyms can provide stable identities to increase embeddedness without reducing privacy.

A joint framework was created based on our analysis of the interaction between privacy and trust in the context of this system (see Figure 2). *Privacy risks* represent the possibility of the player's privacy being invaded, with consequences varying in severity. Whether these risks are perceived depends on the value of the factors described above (see Section 0)–e.g. high linkability or low validity of data might increase risk perception. If users think that the potential risks of using a system

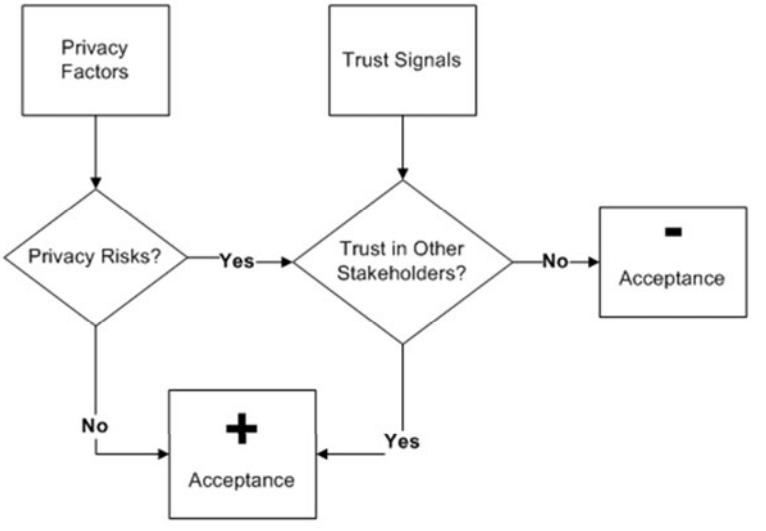

Fig. 2. Trust-privacy interaction

outweigh its benefits, they are likely to reject the technology [4]. But if players trust other stakeholders – colleagues or managers – not to exploit the vulnerabilities the player has identified, then the player will be more willing to engage with the system. Trust – in the context of this system – is assessed by looking at the contextual features identified by [6]. If the purpose of the system is clarified in the start, and there is regulation and sanctions to the organization in case of abuse, this is a trust signal for the player. A code of conduct for the interaction between players, sanctions and stable identities are signals for trusting other players. If players do not even recognize privacy risks in the first place, then there is no need for trust, and they will engage with the system. Previous research [4], [29], [30] found that people were more receptive to monitoring technologies if they trusted the people operating the system.

4 Conclusions and Recommendations

We have identified a number of factors that influence privacy and trust perceptions in TARGET, and propose a framework for how these factors affect the interactions between the player, the system, and other stakeholders. Our findings link the frameworks by Riegelsberger et al. [6] and Adams [4] by clarifying the relationship between trust and privacy –in the context of a TEL system deployed in an organizational context. The contextual properties of Riegelsberger's trust framework were present in our findings: stable identities; accountability and reputation; and institutional code of conductwere mentioned as promoters of a trustworthy environment. Also, the three main factors of Adams' privacy model were present: information receiver; information usage; and information sensitivity. The main take-away point resulting from the trust-privacy interaction is that if a serious-game is perceived by users to have privacy invasive features and is introduced in a low-trust organizational environment the acceptance will be low, while in a high-trust environment the privacy risks will have a smaller impact on acceptance. This phenomenon is not specific to serious-games but the work presented in this paper supports this conclusion in the context of serious-games.

Consistent with workplace privacy literature, our findings identifiedperceived risks associated with monitoring and the resulting employee evaluation[7], [8], [9], [10], [31]. Whereas past literature has focused on the employee-employer relationship, our research also acknowledges the potential risks associated with colleagues seeing data of fellow employees, which can damage reputation or lead to humiliation.

In addition to the factors mentioned in TEL literature –linkabilityand disclosure of data [11], [12], [13]– our research found that nature of the data and its validity also influence privacy perceptions of potential users.Our research also considered the organizational environment in which the technology is deployed and the tensions between theinterests of different stakeholders.

We now present several recommendations for practitioners –game designers and employers / management:

1. Game designers should emphasize the benefits of the system to the organization and give them guidance on how to incorporate the game into the working week. Managers must be on board, as they are the ones who will be implementing the system and deciding which employees should be given which game scenarios;

2. Management should inform employees of the purpose of deploying the system: assessment or learning.
3. Employees should be made aware of any consequences for their careers – negative or positive – resulting from playing the game;
4. Management should inform employees what data is being collected by the system, where the data is going to be stored and the security measures being used to keep it safe;
5. Players should have control over the disclosure of game data to other stakeholders; particularly, performance data, time playedand scenarios played;
6. Players should be provided with channels to challenge or justify their performances and correct or erase incorrect data. The performance assessment process should take into consideration the player's overall personal context;
7. Interactions that take place in the loungeshould not be monitored and/or recorded because there is an expectation of privacy in that area;
8. Developers should include game features that encourage trustworthy behavior – e.g. block lists, rating systems.
9. Managers should develop a code of conduct that is enforced by the workplace to remind players to act in a professional manner;
10. Real names are preferable for socializing in the lounge; in the game scenarios, however, the enforcement of pseudonyms could have a positive effect on the player's performance and learning experience.

The findings from our study were fed back to the TARGET developers and partner organizations planning to deploy it. To our knowledge, scenarios have not been employed before to aid the development of a privacy sensitive system – only in understanding its privacy issues.

In future studies, we plan to interview other stakeholders to obtain their perceptions of privacy and trust: managers in companies deploying TARGET and– once the platform is completely developed– actual players.

References

1. Clark, R.C., Mayer, R.E.: E-learning and the science of instruction: Proven guidelines for consumers and designers of multimedia learning, 2nd edn. Jossey-Bass/Pfeiffer, San Francisco (2007)
2. Van Eck, R.: Digital Game-Based Learning: It's Not Just the Digital Natives Who Are Restless. EDUCAUSE Review 41 (2006)
3. Fletcher, J. D., Tobias, S.: Using Computer Games and Simulations for Instruction: A Research Review. Society for Applied Learning Technology Meeting, New Learning Technologies, SALT, Orlando, FL (2006)
4. Adams, A.: Users' Perceptions of Privacy In Multimedia Communications. PhD. University College London (2001)
5. Iachello, G., Hong, J.: End-user privacy in human-computer interaction. Found. Trends Hum.-Comput. Interact. 1(1), 1–137 (2007)
6. Riegelsberger, J., Sasse, M.A., McCarthy, J.D.: The Mechanics of Trust: A Framework for Research and Design. Int. Journal of Human-Computer Studies 62(3), 381–422 (2005)

7. Fairweather, N.B.: Surveillance in Employment: The Case of Teleworking. Journal of Business Ethics 22, 39–49 (1999)
8. Ariss, S.S.: Computer monitoring: benefits and pitfalls facing management. Information & Management 39(7), 553–558 (2002)
9. Snyder, J.L.: E-Mail Privacy in the Workplace. Journal of Business Communication 47(3), 266–294 (2010)
10. Chen, R., Sanders, G.L.: Electronic Monitoring in Workplace: Synthesis and Theorizing. In: Proceedings of AMCIS (2007)
11. Anwar, M.M., Greer, J., Brooks, C.A.: 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, pp. 1–4. ACM, Markham (2006)
12. Jerman-Blazic, B., Klobucar, T.: Privacy provision in e-learning standardized systems: status and improvements. Computer Standards & Interfaces 27(6), 561–578 (2005)
13. Nejdl, W., Wolpers, M.: 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 (2004)
14. Andersen, B., Fradinho, M., Lefrere, P., Niitamo, V.: The Coming Revolution in Competence Development: Using Serious Games to Improve Cross-Cultural Skills. In: Online Communities and Social Computing, pp. 413–422 (2009)
15. Lave, J., Wenger, E.: Situated Learning. In: Legitimate Peripheral Participation. Cambridge University Press, Cambridge (1991)
16. Wenger, E.: Communities of Practice: Learning, Meaning, and Identity. University Press Cambridge, Cambridge (1998)
17. Ackerman, M.S., Mainwaring, S.D.: Privacy Issues and Human-Computer Interaction. In: Security and Usability: Designing Secure Systems That People Can Use, pp. 381–399. O'Reilly, Sebastopol (2005)
18. Hine, C., Eve, J.: Privacy in the Marketplace. The Information Society 14, 253–262 (1998)
19. Culnan, M.J.: How Did They Get My Name?: An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use. MIS Quarterly 17(3), 341–363 (1993)
20. Lederer, S., Hong, I., Dey, K., Landay, A.: Personal privacy through understanding and action: five pitfalls for designers. Personal Ubiquitous Comput. 8(6), 440–454 (2004)
21. Stone, E.F., Stone, D.L.: Privacy in organizations: Theoretical issues, research find- ings, and protection mechanisms. Research in Personnel and Human Resource Management 8, 349–411 (1990)
22. Corritore, C.L., Kracher, B., Wiedenbeck, S.: On-line trust: concepts, evolvingthemes, a model. International Journal of Human Computer Studies 58(6), 737–758 (2003)
23. Rousseau, D.M., Sitkin, S.B., Burt, R.S., Camerer, C.: Not so different after all: A cross-discipline view of trust. Academy of Management Review 23(3), 393–404 (1998)
24. Mayer, R.C., Davis, J.H., Schoorman, F.D.: An Integrative Model of Organizational Trust. Academy of Management Review 20(3), 709–734 (1995)
25. McAllister, D.J.: Affect- and Cognition-based Trust as Foundations for Interpersonal Cooperation in Organizations. Academy of Management Journal 38(1), 24–59 (1995)
26. Bacharach, M., Gambetta, D.: Trust as Type Detection. In: Castelfranchi, C., Tan, Y. (eds.) Trust and Deception in Virtual Societies, pp. 1–26. Kluwer, Dordrecht (2001)
27. Raub, W., Weesie, J.: The Management of Matches: A Research Program on Solidarity in Durable Social Relations. Netherland's Journal of Social Sciences 36, 71–88 (2000)

28. Strauss, A., Corbin, J.: Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory. SAGE publications, London (1998)
29. Melenhorst, A., Fisk, A.D., Mynatt, E.D., Rogers, W.A.: Potential Intrusiveness of Aware Home Technology: Perceptions of Older Adults. In: Proceedings Of The Human Factors And Ergonomics Society 48th Annual Meeting, pp. 266–270 (2004)
30. Alder, G.S., Noel, T.W., Ambrose, M.L.: Clarifying the effects of Internet monitoring on job attitudes: The mediating role of employee trust. Information & Management 43(7), 894–903 (2006)
31. George, J.F.: Computer-Based Monitoring: Common Perceptions and Empirical Results. MIS Quarterly 20(4), 459–480 (1996)