Friend Inspector: A Serious Game to Enhance Privacy Awareness in Social Networks

Alexandra Cetto, Michael Netter, Günther Pernul, Christian Richthammer, Moritz Riesner, Christian Roth, Johannes Sänger
Department of Information Systems
University of Regensburg
firstname.lastname@ur.de

ABSTRACT

Currently, many users of Social Network Sites are insufficiently aware of who can see their shared personal items. Nonetheless, most approaches focus on enhancing privacy in Social Networks through improved privacy settings, neglecting the fact that privacy awareness is a prerequisite for privacy control. Social Network users first need to know about privacy issues before being able to make adjustments. In this paper, we introduce Friend Inspector, a serious game that allows its users to playfully increase their privacy awareness on Facebook. Since its launch, Friend Inspector has attracted a significant number of visitors, emphasising the need for better tools to understand privacy settings on Social Networks.

Author Keywords

Serious Games, Privacy Awareness, Social Network Sites

INTRODUCTION

Over the last decade, Social Network Sites (SNSs) have gained importance as a medium for social interaction, allowing people to stay in touch with existing contacts and to create new relationships. Hereunto, SNSs ease social interaction by offering a centralised point to communicate with contacts from different social spheres (e.g. family members, close friends, and colleagues).

Despite these positive social outcomes, the rise of SNSs has been accompanied by privacy concerns. Besides the broadly discussed SNS service providers' handling of personal data, privacy is also threatened by a SNS user's contacts (often referred to as "friends") [29]. On general-purpose SNSs such as Facebook, "unimaginably complex social relations collapse to the infinitely thin plane of a single profile" [20]. As a result, it is difficult for a SNS user to simultaneously meet the expectations and respect varying social norms of conflicting social spheres [5]. This might put the user at risk of offending one (or more) of these social spheres, ultimately leading to social exclusion. A SNS user, for instance, may struggle with targeted sharing sensitive family-related pictures with close friends and family members while hiding these pictures from his colleagues who have also access to his SNS profile. Generally speaking, privacy is threatened if shared personal items are visible to contacts for whom they are not intended.

However, these privacy issues are not primarily due to a lack of appropriate privacy settings, as popular SNSs offer a wide range of fine-grained controls to adjust the visibility of shared items [23]. Instead, it has been shown that an item's visibility is often only defined once when it is shared and subsequently left unchanged [27]. Over time and due to the large number of shared items and contacts, users become unaware of who has access to which shared items [18]. Awareness of inaccurate privacy settings, however, is a prerequisite for being able to make necessary changes. Put differently, users first need to know of misconfigured privacy settings before being able to make adjustments.

Especially for young people, a careless attitude towards SNS privacy puts their future prospects (such as when applying for a job) at risk and may lead to social exclusion. On the one hand, the age group of people between 13 and 25 is most active on SNSs. On the other hand, the "cyber personae they spawned in adolescent efforts to explore identity have taken on permanent lives in the multiple archives of the digital world." [25] Hereunto, early and playful education of privacy risks on SNSs can contribute to responsible usage and empower those people to harness the strengths of SNSs. In this paper, we adopt the concept of serious games in order to strengthen privacy awareness on SNSs. It has been widely accepted that games can provide an engaging and motivational environment for learning [13]. In [7], the efficacy of game-based approaches for behavioural change has been demonstrated. Besides, it has been shown that serious games have the potential to increase awareness of important societal issues [22]. Our resulting serious game, termed *Friend Inspector*, is a browser-based application that allows Facebook users to playfully check their knowledge of who can see their shared personal items and provides personalised recommendations on how to improve privacy settings.

The remainder of this paper is structured as follows. After examining related work in the following section, an in-depth discussion of the concepts of privacy and serious games as the

two foundations of Friend Inspector is provided. Based thereupon, the conceptual design of Friend Inspector is presented. Finally, we discuss implementation details and conclude the paper.

RELATED WORK

Raising privacy awareness on SNSs has been the subject of both practical and theoretical approaches. Practical approaches such as Profile Watch[1], Privacy Check[2], and Privacy Scanner[3] analyse privacy settings and publicly shared items of a Facebook profile. Subsequently, results are summarised and recommendations that offer guidance on how to improve privacy on Facebook are provided. Unfortunately, two of the three approaches were not fully functional as of November 2nd, 2013. Friend Inspector differs from these approaches as these sites only analyse publicly available items instead of all shared items. From an educational perspective, due to their informatory-only approach, these sites are of limited value for sustained learning compared to Friend Inspector, which allows users to actively test their knowledge of their SNS privacy settings in a playful manner.

Aside from tools to check privacy settings, game-based approaches such as Realistic Facebook Security Simulator[4] and Privacy Game[5] exist. Realistic Facebook Security Simulator presents a set of privacy-related questions, asking the user to specify his prefered visibility for typical information shared on SNSs within a limited amount of time. At the end of each round, the answers are evaluated. The user passes to the next round if the answers were correct, otherwise the game is over. Unlike Friend Inspector, this game-based approach does not employ items from the user's Facebook profile but solely operates on a static set of questions, making it difficult for users to relate the results to actual privacy issues on their profiles. Besides, Privacy Game is a general-purpose game for privacy education. The game operates on a set of predefined information pieces, requiring each player to make decisions whether to reveal particular information such as by trading it for gifts on a shopping site. Privacy Game differs from Friend Inspector in several ways. On the one hand, it is not specifically designed to raise privacy awareness in SNSs. On the other hand, the game lacks personalisation as it uses fictitious information pieces rather than using the player's actual personal items from his SNS profile.

From the viewpoint of academic research, raising security awareness has been the focus of few game-based approaches such as CyberCIEGE [11] and Control-Alt-Hack [8]. However, their objective is to playfully learn about security in general. Unlike Friend Inspector they do neither specifically focus on the awareness aspect of privacy nor on SNSs in particular. Besides these two games, few visualisation-based approaches to increase privacy awareness on SNSs exist that
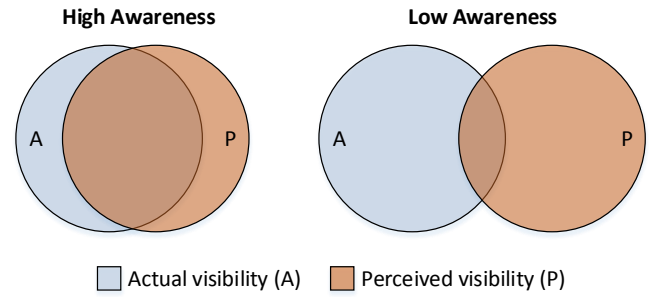
---

[1] http://www.profilewatch.org/

[2] http://www.rabidgremlin.com/fbprivacy/

[3] http://www.reclaimprivacy.org/

[4] http://toys.usvsth3m.com/realistic-facebook-privacy-simulator/

[5] http://www2.open.ac.uk/openlearn/privacy/game/

Figure 1. Privacy Awareness (Venn diagram)

provide a readily understandable presentation of privacy settings [15, 16, 4, 3]. While offering different views on the visibility implications of privacy settings, these approaches are only of informing nature and lack any game-based elements.

BACKGROUND

In this section, we explicate the concepts of privacy in SNSs and serious games as the two foundations of Friend Inspector in order to arrive at a common understanding. Both foundations significantly influence the learning objectives as well as the design of the proposed game.

Privacy in SNSs

In order to develop a game-based approach to improve privacy awareness on SNSs, first a common understanding of both terms (privacy and awareness) is needed.

Literature offers a variety of privacy conceptualisations such as *control over personal information* [26], *confidentiality or secrecy of personal information* [6], or *freedom to construct one's identity* [1]. For this work, we build upon Nissenbaum's view on privacy as *contextual integrity* [19], which is commonly used to understand privacy issues in an environment of voluntary information disclosure such as SNSs [10]. Privacy in the sense of contextual integrity is about respecting the social norms (established by culture, history, and conventions) in a given situation (context). Based on this definition, sharing personal information per se is not a privacy issue [14]. Privacy is only threatened if this information is shared outside the context in which it was initially shared. Applying contextual integrity to SNSs, sharing family-related pictures with one's parents, for instance, preserves contextual integrity and does not violate privacy. In contrast, privacy is violated if such pictures leave the intended context and become available to one's colleagues or employer.

Privacy awareness on SNSs can be defined as an individual's knowledge of who can access which shared personal information. In more detail, privacy awareness is the degree to which *actual* and *perceived* visibility of shared items match [18]. Figure 1 illustrates privacy awareness using set theory. Two sets can be defined: perceived visibility settings P and actual visibility settings A. A user is highly privacy aware if the sets A and P largely intersect, i.e. the perception of who can access which items largely corresponds to what is defined on the SNS. Likewise, a minor or no intersection of A and P implies a low privacy awareness.

Currently, several factors have a negative impact on privacy awareness on SNSs. Firstly, users typically share a large number of items on SNSs with a large number of contacts[6]. As a consequence, it becomes increasingly difficult after a while to remember which contacts can see which personal items. Secondly, it is highly context-dependent whether or not an item is considered private. A user's shared picture of him being drunk at a party, for instance, may not be considered highly sensitive from a close friend's perspective but is highly private to the user with regard to potential future employers and may lead to social exclusion. Lastly, current SNSs are optimised for information sharing rather than for gaining privacy awareness [15]. Hence, existing means to review visibility settings are tedious to use as they often require a user to manually check each shared item.

As a result of the previous discussion, the following two privacy-related objectives can be derived for the design of a privacy awareness game:

- **Preselection of Sensitive Items:** Reduce complexity by focusing only on few privacy-relevant items. As privacy is context-dependent, players themselves must specify the sensitivity of their items.

- **Comparison of Actual and Perceived Visibility:** For the selected items, provide simple means to compare a player's perceived visibility with the actual visibility.

Serious Games

It has been widely accepted that games can provide an engaging and motivational environment for learning [13]. While entertainment can be seen as the main motivation of traditional games, serious games that combine both computer and video games for non-entertainment purposes have become popular in the last decade [17]. A precise definition of the notion of serious games is still difficult to formulate due to rapid technological and artistic developments and innovations made in the virtual and gaming environments [17]. For this work we use Marsh's definition who tried to fill that gap:

"Serious games are digital games, simulations, virtual environments and mixed reality/media that provide opportunities to engage in activities through responsive narrative/story, gameplay or encounters to inform, influence, for well-being, and/or experience to convey meaning. The quality or success of serious games is characterised by the degree to which purpose has been fulfilled. Serious games are identified along a continuum from games for purpose at one end, through to experiential environments with minimal or no gaming characteristics for experience at the other end." [17]

In this work, we focus on digital game-based learning in an experiential environment as one aspect of the serious games continuum. In experiential environments, an inductive learning approach is used. By contrast, traditional instructional design usually includes methods to encourage deductive learning [2]. Thereby, a concrete concept or solution is presented followed by exercises to practice. Inductive learning, in contrast, is based on discovery. It allows students to "invent" a

---

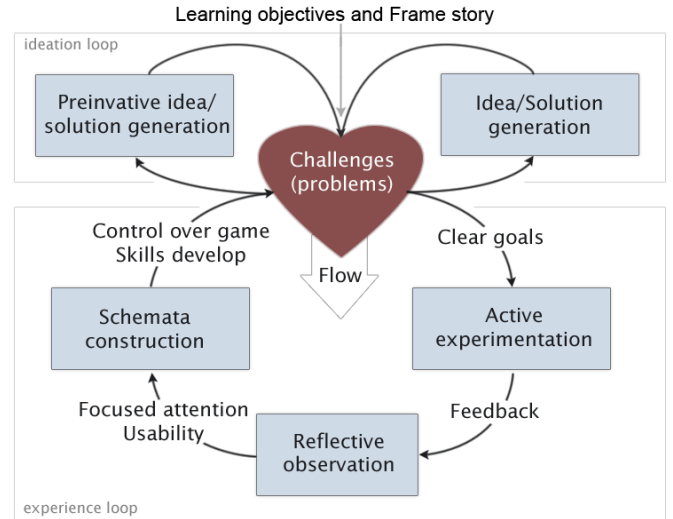[6]For instance, the average Facebook user has 190 contacts [28].

Figure 2. Experiential gaming model (based on [13])

solution or concept by experimentation which is often considered a more effective approach [21].

A framework that tries to combine experiential learning theory (inductive), flow theory and game design is the experiential gaming model proposed in [13]. The experiential gaming model depicted in Figure 2 on which Friend Inspector is based "describes learning as a cyclic process through direct experience in the game world" [13]. The starting point of the experiential gaming model are the learning objectives. Based on these, a player is presented with one or several challenges / problems. While solving these problems, the learner runs through a cyclic process that involves both an experience loop where the learner conducts active experimentation, reflective observations, and schemata construction and an ideation loop where ideas or solutions are generated. Although the experiential gaming model works as a tie between educational theory and game design, it does not cover the whole gaming process. Thus, a frame story is needed that integrates the challenges into a larger task or a problem [13].

Based on this, the following two components / concepts have to be elaborated during the design process:

- **Frame story**: Provide a frame story that motivates the learner and integrates the challenges into a meaningful context.

- **Experiential gaming model**: Design the learning phase using the experiential gaming model to achieve the learning objectives.

CONCEPTUAL DESIGN OF FRIEND INSPECTOR

Based on the foundations of privacy awareness and serious games, forming the pillars of our work, in this section we present the design of Friend Inspector. The design has been iteratively improved during several refinement cycles.

Frame story and learning objectives

The general idea of Friend Inspector is to create an environment in which users can playfully discover their privacy
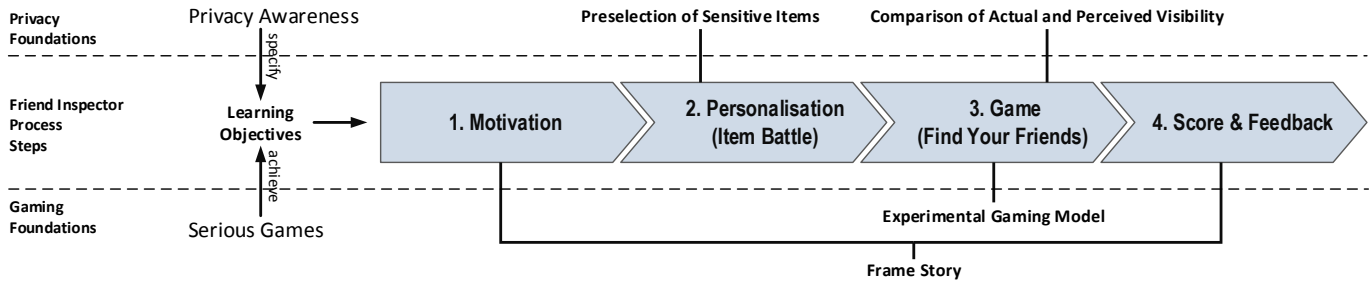
3

Figure 3. Friend Inspector Process Flow

settings on Facebook and find out who can see their shared items. Based on this, they can ultimately increase their privacy awareness. To this end, the central element of Friend Inspector is a memory-like game, where players are asked to guess the visibility of a presented item within a limited amount of time. A score is calculated based on the correctness of the answer and the time needed to complete the task.

In order to provide a meaningful context for this challenge, the frame story is to motivate SNS users to test their privacy awareness about items they shared on their Facebook profile and to reach the best possible score. To increase the game's competitive element, the score can be shared on the user's Facebook wall to challenge other contacts to beat his score. As a user's social value on SNSs is created by sharing interesting things, sharing a Friend Inspector score creates a positive feedback loop in which people in a user's network of contact mutually try to beat each other and share a higher score.

Based on the previous analysis of privacy awareness in SNSs, the following two learning objectives should be reached:

- **Enhance privacy awareness**: We want users to recognise the properties and consequences of their privacy settings. Thereby, we want to decrease the gap between perceived and actual visibility.

- **Learn about privacy settings**: By giving recommendations, we want to empower users to improve their privacy settings based on their desired preferences.

Process flow
To reach the learning objectives, we designed Friend Inspector as a four-step process flow (see Figure 3). The process flow integrates the concepts of *privacy awareness*, which specifies the learning objectives, and *serious games* in order to achieve these objectives. Each step of the four-step process flow is preceded by a briefing window that provides the learner with basic instructions. The first step (Motivation) and the last step (Score & Feedback) form the frame story, integrating the challenges into a meaningful context that invites a Facebook user to play Friend Inspector. Step two (Personalisation) is used to reduce the total number of items for the subsequent game step and elicit those items the user considers especially sensitive. Step three (Game) contains the main element of Friend Inspector, building upon the experimental gaming model. During this step, the user has to guess the

visibility of a presented item by selecting the respective people from a set of depicted contacts. Step three is repeated five times before the game continues with the final Score & Feedback step.

In the following sections, the conceptual design of each step is presented in detail.

Motivation step
Figure 4 depicts Friend Inspector's initial landing page. At the very beginning of the game, a potential user is teased by the question "Do you know who can see your Facebook profile?". As motivation is important in this context, the objective of this phrase is to gain the users' attention and invite them to test their knowledge of the privacy settings of their Facebook profile. The subtopic "Playfully discover who can see your shared items and get advice to improve your privacy." aims to further clarify the objectives and their relevance. It hints at the underlying game-based approach that distinguishes Friend Inspector from purely educational or information giving approaches such as presented in the related work section. The design of the landing page follows the first two components of Keller's ARCS (attention, relevance, confidence, satisfaction) model for motivational design, using a question as attention strategy (inquiry) and the worth for the user as relevance strategy (presented worth) [12].
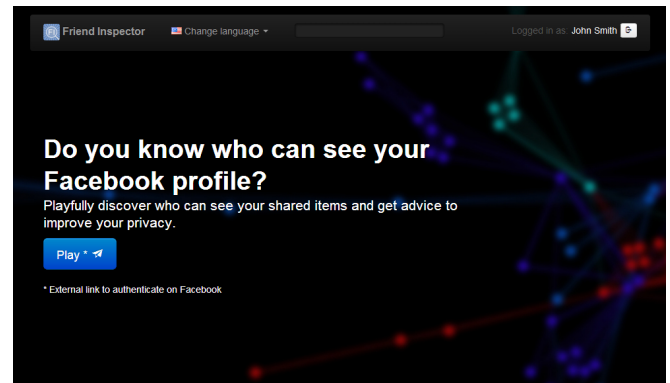

Figure 4. Friend Inspector landing page (step 1)

Personalisation step (Item Battle)
Step two is concerned with adapting the game to the player's Facebook profile. Personalisation is crucial, as adaption to
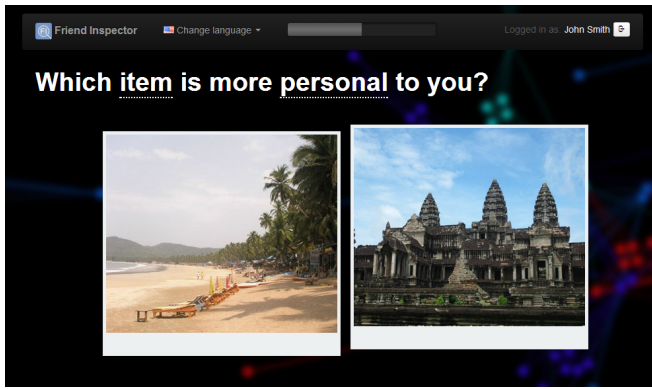
Figure 5. Item Battle (step 2)

Figure 6. Find Your Friends (step 3)

learners is considered a key aspect for the success of serious games [24]. In the context of Friend Inspector, personalisation deals with integrating the player's own items and their privacy settings into the game and preselecting sensitive items.

To perform the personalisation, Friend Inspector initially retrieves a user's contacts as well as his shared items and the corresponding privacy settings from Facebook. Subsequently, sensitive items (for which the user has strong visibility preferences) need to be determined from the set of all shared items. Friend Inspector offers a playful way to determine the sensitivity of items. To this end, a pair-wise comparison of two displayed items is used, asking the user to select one of the two items which is more personal to him[7]. This comparison, termed Item Battle, is executed in ten rounds with varying items and implicitly results in an ordered list of items ranked by sensitivity. Figure 5 shows Item Battle for two exemplary items. A subset of the most sensitive items is then used during the actual gaming step.

Game step (Find Your Friends)

The third step of the Friend Inspector process flow contains the actual game which is termed Find Your Friends. The game consists of five rounds, whereas Figure 6 depicts the interface of a single round of Find Your Friends. The left area shows one of the user's sensitive items that have been determined in the previous step. The right area contains a set of 20 profile pictures that consist of the user's contacts as well as randomly selected strangers[8].

The subsequently described flow of Find Your Friends follows the experimental gaming model presented in the background section. The main *challenge* for the learner is to demonstrate his privacy awareness, i.e. his knowledge of who can see his shared items. Following the experimental gaming

model, the *clear goal* for each round is to select those profile pictures that can see the presented item in order to reach the maximum score. Find Your Friend provides immediate *feedback* based on the user's answer. A correctly selected profile picture is framed in green. Incorrect answers result in a red-framed profile picture. Additionally, the score is reduced by 1000 points and one of five hearts. A round is lost if either no heart is left or the score has fallen to zero points. Starting with a score of 10000 points for each round, the score is automatically reduced by 200 points each second to achieve *focused attention*. With each round, the player gains new insights about his visibility settings, enabling him to gain *control over the game* and reach higher scores.

It is notable that with increased privacy awareness, the game story shifts from a self-centred challenge to a community-centred one. Self-centred challenge refers to a player simply trying to learn who can see his shared items. With increasing control over the game, beating the score shared on Facebook by contacts becomes the main challenge instead of plain knowledge of the items' visibility. Yet, both challenges can be seen as motivational factors that contribute to the learning objectives.

Score & Feedback step

After five rounds of Find Your Friends, Friend Inspector continues with the fourth step of the process flow (cf. Figure 3). The objectives of this step are to summarise the results of Find Your Friends, to calculate the overall score, and to provide personalised recommendations to improve privacy settings.

Figure 7 depicts the Score & Feedback interface. The upper part shows the overall score together with a smiley that allows the learner to easily put the score in context[9]. Below the overall score, a detailed calculation allows the learner to understand how the score is composed of single item scores. Further information is available for each item through an expendable panel, showing incorrect answers.

---

[7]Friend Inspector uses the Elo rating [9] to rank items.

[8]Note that only a subset of the user's contacts is presented for each round to increase usability. The people's names are shown on mouseover. In order to increase the challenge, the composition of presented profile pictures depends on the current item's visibility settings. As an example, contacts and random strangers are equally distributed if the item is visible to all contacts. In contrast, if the item is only set to be visible to a specific set of contacts, then the composition of presented people largely uses the user's contacts.
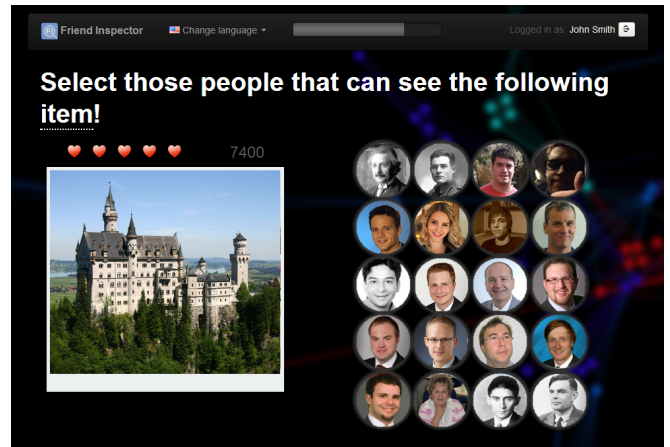
[9]Friend Inspector includes three different smileys: "Sad" smiley (<15000 points), "Neutral" smiley ($15000 - 32500$ points), "Happy" smiley (>32500 points).
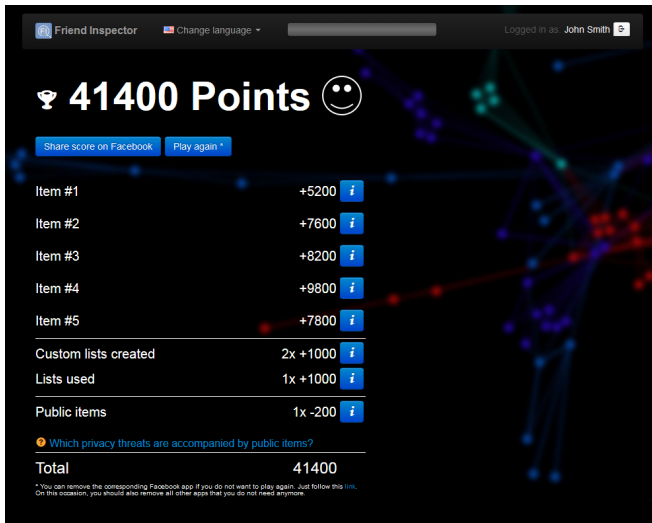
Figure 7. Score & Feedback (step 4)

Additional bonus points are assigned for the definition and the use of friend lists on Facebook[10]. Moreover, the player's score is reduced by 200 points for every item that is publicly shared. Reducing the score for publicly shared items raises the player's awareness for the high privacy risks of such a visibility setting.

Finally, based on the results and the user's Facebook profile, a set of personalised recommendations is displayed. Recommendations comprise instructions such as how to create friend lists, how to share personal items in a targeted manner, and how the term friendship on SNSs differs from friendships in the physical world. Following Friend Inspector's inductive learning, after experimenting with their privacy settings, these recommendations provide guidance and empower users to actually improve their privacy settings.

IMPLEMENTATION AND DISSEMINATION
Based on the conceptual design, we implemented Friend Inspector as a browser-based application which is publicly available[11]. In order to offer an acceptable gaming experience, Friend Inspector imposes minimum requirements on the user's Facebook profile such as at least seven (non-public) shared items (pictures and status messages).

Software architecture
With respect to privacy issues regarding the software itself, Friend Inspector was developed as a client-side single-page application following a three-tier architecture. Thereby, the logic tier is designed according to a model-view-controler (MVC) approach. Figure 8 gives an overview of the architecture.
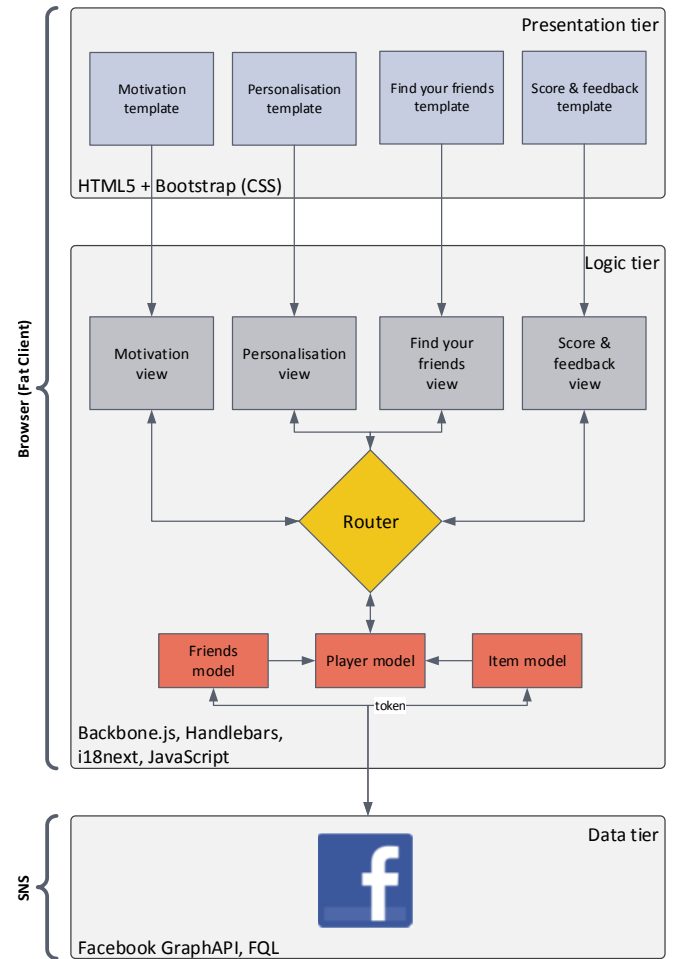
---

[10]Friend lists improve targeted sharing of items and thus contribute to privacy. For up to five lists, a user gets 1000 points for the definition and use of every list.
[11]http://www.friend-inspector.org/

Figure 8. Schematic view of Friend Inspector's architecture

The data tier provides personal data, namely items, friends and privacy settings of a learner's profile. Since these private and sensitive data should not be stored persistently somewhere other than facebook, the GraphAPI serves as single persistent read-only data source/store. A connection to Facebook is established using the official Facebook SDK for JavaScript[12] (GraphAPI and FQL). In order to collect user data, the application must request a unique access token from Facebook, which is bound to the user, the application and the specific permission set.

The logic tier is completely implemented in JavaScript using backbone.js to enable the implementation of the whole logic functionality on the client-side (fat client). Backbone.js[13] is a commonly used MVC framework that is suitable for the development of single-page websites. The framework involves models, collections, views and routers. The models (red rectangles in Figure 8) represent Facebook entities as local transient instances. The router (orange rhombus) serves as a handler that guarantees a flawless process flow triggered by events. Moreover, it acts as a link between the models and

---

[12]https://developers.facebook.com/docs/reference/javascript/
[13]http://backbonejs.org/

the single views for each process step. The views (grey rectangles) render the allocated data and fill the templates (blue rectangles) of the presentation tier. For a clear separation of logic and design, we integrated the template engine Handlebars[14].

The website presented to the user (presentation tier) is built on top of Bootstrap 2[15] and HTML5. Bootstrap is a widely used and recognized CSS framework that can improve the usability and trustworthiness of the game using a familiar layout theme.

Secure and trusted implementation

As Friend Inspector operates on the user's personal Facebook data, a secure and trusted implementation is of major importance to gain acceptance. Therefore, Friend Inspector is conceived as a client-side application that solely runs in the user's browser with no server-sided functionality required. As a result, personal data requested from the Facebook profile does not leave the user's domain at any time and is not transmitted to any server. Prior to the first use of Friend Inspector, users are informed about the game's access to their profile and must approve this action. This approach ensures ethical data capture and use of personal information within the game. Additionally, the source code of Friend Inspector has been released under the Apache License 2.0 and is publicly available to further increase trust in the application, allowing interested users to verify its integrity and security.

Dissemination and usage

Friend Inspector is aimed to raise privacy awareness of as many SNS users as possible. Consequently, disseminating the game has been of major importance. To this end, Friend Inspector uses i18next[16] to add multilanguage support, which also allows to add easily new language files. Friend Inspector is currently available in two languages (English and German).

Friend Inspector was launched on June 26th, 2013 and has been widely covered in national and international media (press, radio, and television). Within five months, the Friend Inspector site has been requested more than 100,000 times. Note that detailed usage statistics are not available, as Friend Inspector does neither store nor analyse log files for privacy reasons. Amazon's Elastic Compute Cloud[17] (Ireland) is used to host Friend Inspector for performance reasons and to cope with traffic peaks.

CONCLUSIONS

In this paper, we introduced Friend Inspector, a serious game developed to enhance SNS users' privacy awareness. Friend Inspector addresses the current challenge of SNS users, namely to understand who can see their shared personal items. In order to address especially younger users and protect them from social exclusion due to the consequences of poor privacy awareness, a game-based approach has been chosen. The conceptual design of Friend Inspector is based on two foundations: firstly, an in-depth understanding of privacy awareness as the match or mismatch between perceived and actual visibility of shared items. Secondly, an inductive learning approach that allows its users to experiment and play with their own Facebook data in order to actively learn about the visibility of their personal items.

Friend Inspector is implemented as a web application for the SNS Facebook. In the five months since its launch, Friend Inspector has attracted a significant number of visitors, which further emphasises the need for better tools to understand privacy settings on SNSs.

REFERENCES

1. Agre, P. E., and Rotenberg, M. *Technology and Privacy: The New Landscape*. MIT Press, Cambridge, MA, USA, 1998.

2. Amory, A., and Seagram, R. Educational Game Models: Conceptualization and Evaluation. *South African Journal of Higher Education 17*, 2 (2003), 206–217.

3. Anwar, M., and Fong, P. W. L. Access Control Policy Analysis with a Visualization Tool for Social Network Systems. Tech. rep., University of Calgary, 2011.

4. Anwar, M. M., Fong, P. W. L., Yang, X.-D., and Hamilton, H. J. Visualizing Privacy Implications of Access Control Policies in Social Network Systems. In *Proc. of the 2nd International Conference on Data Privacy Management and Autonomous Spontaneous Security (DPM '09)*, Springer (2010), 106–120.

5. Binder, J., Howes, A., and Sutcliffe, A. The Problem of Conflicting Social Spheres: Effects of Network Structure on Experienced Tension in Social Network Sites. In *Proc. of the SIGCHI Conference on Human FActors in Computing Systems (CHI '09)*, ACM (2009), 965–974.

6. Committee on Privacy in the Information Age, National Research Council. *Engaging Privacy and Information Technology in a Digital Age*. The National Academies Press, 2007.

7. de Freitas, S., and Liarokapis, F. Serious Games: A New Paradigm for Education? In *Serious Games and Edutainment Applications*, M. Ma, A. Oikonomou, and L. C. Jain, Eds. Springer, 2011, 9–23.

8. Denning, T., Lerner, A., Shostack, A., and Kohno, T. Control-Alt-Hack: The Design and Evaluation of a Card Game for Computer Security Awareness and Education. In *Proc. of the 2013 ACM SIGSAC Conference on Computer & Communications Security (CCS '09)*, ACM (New York, NY, USA, 2013), 915–928.

---

[14]http://handlebarsjs.com/

[15]http://getbootstrap.com/

[16]http://www.i18next.com/

[17]http://aws.amazon.com/en/ec2/

9. Elo, A. E., and Sloan, S. *The Rating of Chess Players, Past and Present*. Ishi Press International, 2008.

10. Hull, G., Lipford, H. R., and Latulipe, C. Contextual gaps: Privacy Issues on Facebook. *Ethics and Information Technology 13*, 4 (2011), 289–302.

11. Irvine, C. E., Thompson, M. F., and Allen, K. CyberCIEGE: Gaming for Information Assurance. *IEEE Security and Privacy 3*, 3 (May 2005), 61–64.

12. Keller, J. M. Development and Use of the ARCS Model of Instructional Design. *Journal of Instructional Development 10*, 3 (1987), 2–10.

13. Kiili, K. Digital Game-Based Learning: Towards an Experiential Gaming Model. *The Internet and Higher Education 8*, 1 (2005), 13–24.

14. Leenes, R., Van den Berg, B., Pötzsch, S., Pekárek, M., Roosendaal, A., Kuczerawy, A., Borcea-Pfitzmann, K., and Beato, F. D1.2.1 Privacy Enabled Communities. Tech. rep., PrimeLife Project, 2010.

15. Lipford, H. R., Besmer, A., and Watson, J. Understanding Privacy Settings in Facebook with an Audience View. In *Proc. of the 1st Conference on Usability, Psychology, and Security (UPSEC '08)*, USENIX Association (2008), 2:1–2:8.

16. Lipford, H. R., Watson, J., Whitney, M., Froiland, K., and Reeder, R. W. Visual vs. Compact: A Comparison of Privacy Policy Interfaces. In *Proc. of the 28th International Conference on Human Factors in Computing Systems (CHI '10)*, ACM (2010), 1111–1114.

17. Marsh, T. Serious Games Continuum: Between Games for Purpose and Experiential Environments for Purpose. *Entertainment Computing 2*, 2 (2011), 61–68.

18. Netter, M., Riesner, M., Weber, M., and Pernul, G. Privacy Settings in Online Social Networks – Preferences, Perception, and Reality. In *Proc. of the 46th Hawaii International Conference on System Sciences (HICSS '13)*, IEEE (2013), 3219–3228.

19. Nissenbaum, H. *Privacy in Context - Technology, Policy, and the Integrity of Social Life*. Stanford University Press, 2010.

20. Peterson, C. Losing Face: An Environmental Analysis of Privacy on Facebook. *Social Science Research Network (SSRN) Working Paper Series* (2010).

21. Prince, M. J., and Felder, R. M. Inductive Teaching and Learning Methods: Definitions, Comparisons, and Research Bases. *Journal of Engineering Education 95*, 2 (2006), 123–138.

22. Rebolledo-Mendez, G., Avramides, K., de Freitas, S., and Memarzia, K. Societal Impact of a Serious Game on Raising Public Awareness: The Case of FloodSim. In *Proc. of the 2009 ACM SIGGRAPH Symposium on Video Games*, Sandbox '09, ACM (2009), 15–22.

23. Riesner, M., Netter, M., and Pernul, G. Analyzing Settings for Social Identity Management on Social Networking Sites: Classification, Current State, and Proposed Developments. *Information Security Technical Report 17*, 4 (2013), 185–198.

24. Romero, M., Usart, M., Popescu, M., and Boyle, E. Interdisciplinary and International Adaption and Personalization of the MetaVals Serious Games. In *SGDA*, M. Ma, M. Fradinho, J. B. Hauge, H. Duin, and K.-D. Thoben, Eds., vol. 7528 of *Lecture Notes in Computer Science*, Springer (2012), 59–73.

25. Rosenblum, D. What anyone can know: The privacy risks of social networking sites. *IEEE Security and Privacy 5*, 3 (May 2007), 40–49.

26. Solove, D. J. Conceptualizing Privacy. *California Law Review 90*, 4 (2002), 1087–1155.

27. Strater, K., and Lipford, H. R. Strategies and Struggles with Privacy in an Online Social Networking Community. In *Proc. of the 22nd British HCI Group Annual Conference on People, Computers: Culture, Creativity, Interaction (BCS HCI '08)*, British Computer Society (2008), 111–119.

28. Ugander, J., Karrer, B., Backstrom, L., and Marlow, C. The Anatomy of the Facebook Social Graph. *CoRR abs/1111.4503* (2011).

29. Ziegele, M., and Quiring, O. Privacy in Social Network Sites. In *Privacy Online. Perspectives on Privacy and Self-Disclosure in the Social Web*, S. Trepte and L. Reinecke, Eds. Springer, 2011, 175–189.