Manifestations of Users' Privacy Concerns in a Formative Usability Test of Social Networking Site

Kimmo Tarkkanen, Ville Harkke

Manifestations of Users' Privacy Concerns in a Formative Usability Test of Social Networking Site

Kimmo Tarkkanen[1] and Ville Harkke[2]

[1] Information Systems Science, University of Turku, Turku, Finland
kimmo.tarkkanen@utu.fi
[2] IAMSR, Åbo Akademi University, Turku, Finland
ville.harkke@abo.fi

Abstract. Social media and social network sites (SNS) need to preserve users' privacy, in order to achieve full acceptance and to succeed in the application markets. Thus, SNS developers need to understand and take into account users' privacy concerns as early as possible in the development. It is difficult, however, to foresee how the system fulfills users' privacy expectations until the system is in actual use. Different user-centered techniques applied during the development can offer insights for developers into users' privacy expectations and concerns. In this paper, we empirically show what kinds of privacy concerns users spontaneously brought forth in a formative usability test of a social networking site and how these were attributable to different features of the application and related coping mechanisms. The identified manifestations of privacy concerns help SNS designers and evaluators to pay attention early to privacy issues as a natural part of user centered development.

Keywords: Privacy; Social Networking Site; Usability Testing.

1 Introduction

Many people perform their daily activities through different social online applications, ubiquitous services and social networking (and network) sites (SNS). In order to be useful and usable, these systems require us to share and disclose personal information. For example the personal tracking, monitoring and surveillance capabilities of new technologies may bring many useful applications to everyday life, be it about personal sports or targeted ads based on personal online consuming behavior. Despite their interest in the benefits, people are more and more concerned about what other people can see and how their personal information is used in the future, and by whom. In the era of popularity of social media and SNSs, privacy issues have become one of our major daily concerns, which are seemingly complex to manage in practice.[1]

From the system developer point of view, it is noteworthy that the users' privacy concerns and trust towards the system affects its future acceptance and adaptation [1].

[1] For example, numerous web pages exist to instruct SNS users for managing their privacy.

While some of the systems are only a channel for communication and some have become an "institutionalized" norm (such as Facebook), people as consumers and citizens do have the possibility to select which service, platform and SNS application they take into use. Systems that do not meet our expectations concerning security and privacy are most likely not the ones we want to use in the future and take into use in the first place. Thus, privacy becomes also one of the determinants for the success of social media applications in the consumer markets that businesses and developers need to be aware of and be prepared to design for.

However, it is often difficult to evaluate the effects of a certain technology on privacy [1]. One of the challenges for developers is to identify the evolving norms and values of users before they can take the application into use [2,3]. For example, the expanded use of Facebook has certainly shaped public opinion about privacy and created personal mechanisms for preserving it, which may have been difficult to foresee before launching such system. On the other hand, users' privacy concerns may be at their peak in the beginning of the use, but decrease over time [1]. One of the ongoing problems is that the privacy design toolbox for developers is rather technology-oriented and data protection centric. Developers may focus for instance on user authentication, user account settings and security of program code when designing privacy for their systems. Yet, with social networking sites and services, people have many strategies to preserve their privacy, other than the dedicated settings and features the system offers [4]. Thus, when designing these systems we need to understand people's personal privacy preferences i.e. how they construct and manage privacy in socio-technical interactions [5]. The lack of a clear link between privacy and design currently hampers this work. For example, the workshop of the latest popular HCI conference welcomes research that seeks to translate academic privacy insights into a set of guidelines and practices useful to design practitioners [6]. There is a need for privacy-centric design principles and effective methods for exploring people's privacy preferences [1,2], [5], [7].

During the software development process, the designers gather information about the target audience of the system and their specific needs and preferences. Usability and user experience evaluation methods are widely applied for these purposes. We believe that these common methods introduce a promising base for privacy inclusion in the design practice. A vast amount of privacy research in the field of HCI already shows a tight interconnection of privacy and usability concepts (e.g. [1], [7]). Like usability, privacy is a holistic property and a pervasive feature of interactive systems that cannot be an afterthought in the design process [1], [3]. In consequence, addressing privacy and usability problems during the system development with similar methods is worth studying in detail. The question is: How do these privacy concerns manifest themselves in a usability test and what kind of privacy issues such a classical method can reveal. In this paper, we conduct an analysis of what kinds of privacy concerns users naturally and spontaneously bring forward in a usability test of a social networking prototype, which aims at sharing content around real life events. By manifestation of privacy concern, we mean users' verbal and non-verbal behavioral indicators during the system use that could determine opportunities for encountering loss of privacy in the future. Our

perspective is on those users' privacy concerns at time of use that trigger potential coping mechanisms unless directly supported by the technology. The previous research has mostly studied the actual coping mechanisms after excessive use period (cf. [8,9]). Thus, originality of this research lays apart from scrutinizing usability testing as a method for revealing potential privacy issues, also in studying privacy concerns of first-time users with a short-term user intervention during the system development phase. We list the different privacy manifestations observed in the test. This helps SNS developers and evaluators to pay attention to privacy in a more elaborate way during similar design phases and eventually design their SNS for users' desired levels of privacy.

2 Privacy Concerns in Designing Social Networking Sites

The boundaries of social online network sites are somewhat blurred. Most sites share the core feature of a public or semi-public user profile that others can traverse and peruse with different intentions such as contacting, friending or dating [10,11]. However, the user profile may not be in the essence of the SNS usage, but the feed of shared content, mutual activities and communication in the extended social network. Social media, a close concept to SNS, can be defined through seven functional blocks as identity, presence, relationships, reputation, groups, conversations and sharing [12], or simply as being "all about sharing content with a community" [8].

A definition of privacy by Altman [13] states, that privacy is a process that paces and regulates our interactions with others. In social environments, people try to maintain an appropriate level of access they give of themselves to others. Altman's processual and dynamic view draws a sharp distinction between how much privacy users want and what they attain during the system use [7], [14]. The fit between the desired and the attained level of privacy is not only sound, but also may enhance individual's social relationships and benefits of SNS [9].

Definitions of privacy concern vary from "a loss of control over their personal information" [15] to ones that cover a broader range of human behaviors depending on the view on privacy. In Altman's view, privacy concerns can cover broadly any interpersonal action that serves regulation of one's social interactions [9]. For example, privacy concerns can be studied as individuals' concerns of suppressing their true identity (anonymity), losing control of unwanted information (intrusion) and control of distribution of personal information (autonomy), or being exposed to monitoring and tracking by others (surveillance) [16]. Following Altman's view, privacy concerns have been decomposed into three basic elements [7], [14]: 1) regulating social interactions, 2) giving access to and disclosing information about oneself and 3) managing own identity and self-presentation over time. Each can introduce a personal privacy risk when the boundaries of privacy are negotiated with the environment and in collaborative discourse with others (privacy as a discourse see e.g. [3]). The extent of the privacy risk can be determined by rationally evaluating our personal coping capabilities in this potentially difficult task or situation (privacy as an economic rationality, see e.g. [3]). In using SNS, usability of the system features and user interfaces will inevitably affect

how people perceive their personal coping capabilities, i.e. determine their self-efficacy, and thus further affects how concerned they are about their privacy [17]. People who feel confident about their survival capabilities over a potential risk (e.g. they have some privacy control mechanisms) experience less anxiety towards the system. Enabling every user to achieve their desired level of privacy should be in interest of SNS developers as well [9].

Different user strategies and coping mechanisms exist to preserve interpersonal privacy boundaries in social networking sites [4], [8]. These strategies can be distinguished between mechanisms supported by the user interfaces of SNSs and "coping mechanisms which are an individual's response outside of these confines to mitigate potential boundary interpersonal violations." [4]. Coping mechanisms can be divided into mental and behavioral, preventive and corrective, and further into collaborative and individuals' actions [8]. Users apply corrective coping mechanisms after a privacy risk has realized and preventive mechanisms before. For example, individuals apply a corrective mechanism when they are untagging a photo whereas when they ask approval before tagging a photo from the persons involved they apply a preventive collaborative mechanism. Karr-Wisniewski et al. [18] identified five types of boundaries that people regulate with different mechanisms, in order to achieve the desired privacy level in SNSs: network, territorial, disclosure, relationship and interactional boundaries[2]. For example, turning off the wall on Facebook is about controlling the interactional boundary, whereas removing someone's distracting comment from the personal wall is about controlling the territorial boundary [18,19]. In practice, these mechanisms need controlling actions by users such as filtering, ignoring, and blocking connections, withdrawal from sharing content, aggression, compliance and compromise [4].

Because not all of these identified coping mechanisms are implemented in current SNSs, understanding the privacy mechanisms people use within SNSs can help in pinpointing areas where personal privacy management can be supported by improving user interface design [4]. For instance, SNSs could implement more sophisticated filtering functions for generating relationships, support collaborative negotiation for co-owned content (e.g. about photos where one is tagged) and facilitate reconciling conflicts and motivations behind different actions e.g. due to unfriending [4]. Moreover, photo tagging features of SNSs could be redesigned with customized permissions, untagging and negotiation features [20] and online video media spaces could need for instance more fine-grained content control [7].

In this paper, we are mainly interested in coping mechanisms that technology does not support, in accordance with the aim of the classical usability test: to identify different usability problems of the system that need fixing. Our approach is both evaluative and constructive. Evaluative approach on privacy examines the users' preferred and achieved levels of privacy, whereas the constructive approach offers design solutions and principles [9]. In our study, this meant that privacy concerns expressed by the users

[2] We refer to these mechanisms by Karr-Wisniewski et al. (2011) [18] and Wisniewski et al. (2016) [19] throughout the results section and identify which mechanisms emerge in a usability test.

were traced back to the specific features and functions of the system so that practical design solutions could be suggested.

3 Research Method

3.1 Introducing the social networking site

We tested usability of a new social networking application developed by a global IT company. The idea of the application was to collect users' photos and videos taken in the same event to a single site. The situations where the application was deemed useful were family get-togethers, celebrations, large public concerts and sports events where every attendant could contribute to the shared content by taking and sharing photos and videos of that event. Depending on the privacy settings of the event in the application, the other application users could see the content. The disruptive innovation here was to replace photo sharing with USB sticks, provide a public or private space for photo sharing and allow each member to contribute and access to content.

We conducted one to one usability test sessions for 7 test participants in April, two weeks after the developer launched the beta version for public. The application was under continuous development and during the test only the main use case, creating an event and inviting friends, joining an event and publishing photos in it, was implemented. The application was downloadable free for all major mobile platforms as well as accessible free as a desktop version for computer use.

The application is used in practice as follows: A user creates a shared space for a certain event with the application, acts as the founder of the event and invites people to join the event. The event founder sets also other parameters, like the publicity, location, duration and the name of the event. The founder sends invitations by email or SMS as the current application version did not implement a list of friends attached to a user profile. Users could search events by the name or spot these in the location map as well as access published public ones. The users who had joined the event could download and 'like' photos and videos of the event. The feature that allowed commenting the content was under development during the time of the test, the developers planned integrating it with Facebook comments.

The application implemented characteristics of a social network site due to embedding a user profile, allowing connections with others through joined events, and aiming at sharing photos and videos with the connections. However, at the time of the study, the user profile feature was practically empty and contained only a profile picture, username, and a URL address for viewing events hosted and joined by the user (not accessible from mobile). Thus, a list of friends was not implemented in isolation from the events, and "a wall" feature attached to one's profile contained only events and was accessible only by following the given link with a browser. The application was closer to a social "networking" than a "network" site [11], because one's articulated network was missing and the connections to others were more temporary and indirect. On the other hand, the application would appear even more different from SNSs, if we took the event and the shared content as the unit of analysis (e.g. as a crowdsourcing application to collect photos from the event). Of the building blocks of social media [12],

the application did not explicitly reveal the presence of other users although this is implicitly inherent within events that last a limited time (i.e. users could assume that attendees are present in the application and in the real life event). Nor did it support written conversations, which were to be implemented. The application, however, did embed characteristics of the rest of the building blocks. As it has been found that photo tagging in SNSs caused users to lose their control over information disclosure and identity [20], it was important to identify such features that could be sources of users' privacy concerns and might prevent the desired level of privacy early in the design process.

3.2 Usability testing procedure

The usability test was the first usability test with real users for the application and it took place in laboratory premises. The test objectives were set in the two-hour discussions with the development manager. The test aimed at evaluating the usability of installation procedure (mobile app) and the usage flow of the main use case. The main use case was defined as creating an event and inviting friends, joining an event and publishing photos in it. Installing the application included registering and downloading the app from the particular app store into a mobile phone. The number of test participants, seven, was judged to be adequate for the purposes of this evaluation. In general, it is enough to find the majority of critical usability problems.

The usability test was incorporated into a real event marketed by the company. The event was the celebration of the 1st of May and targeted at university student associations who could compete against each other of the price of "the best event". We used this real event as a reference scenario for usability test tasks. Usability test included 13 test tasks, which covered almost all application functions (create event, search events, my events -functions). Short versions of the tasks were as follows: 1) Install the application into your mobile phone 2) Create your own event 3) Invite your friends to your event 4) Add a photo to your event 5) Add a video 6) Search an event nearby you and view its photos 7) View photos of the X event 8) Select the best photo 9) Send the best photo to your friend 10) Join to the Y event 11) Add a photo to the Y event 12) Save a photo 13) Delete your own event.

All the seven test sessions were video and audio recorded and analyzed later based on the recordings. The test participants were all university students, three females and four males, 20-39 years old recruited randomly. The basic information about the participants was collected with pre-test questionnaire including: Age, gender, mobile phone information, trials and continuous usage of different SNSs, photo sharing practices in the SNSs and regarding some specific events, and earlier use experience of the tested application. Two of the test participants had already downloaded the application and tried it once.

The testing procedure was an informal think aloud where the test administrator had an active role, which means that we exceeded the classical "keep talking" style [21] and took more interactive and relaxed communication style [22]. This meant that the administrator not only handed the tasks, but also asked actively what participants are trying to do and what they think of particular way of operating the system. The communication with the participants was not limited to test tasks, but continued during the post-

test questionnaire, which included, for example, the following open questions and the questions answered in Likert-scale: How fluent was adding photos to your event? How satisfied you are with the following features of the application? What was the best/worst in the application use? In what situation would you use the application in the future? Despite the active role of the test administrator any direct questions about privacy issues were not raised and those were not asked in the pre- and post-questionnaires. We emphasize that the test was of classical and standard nature where privacy concerns were not included in the objectives and targets of data collection. The case study presented in this paper exploits a retrospective data analysis, which, in contrast, had its target on privacy and its manifestations in a usability test. Data analysis was performed bottom-up with the final test report, related documents, notes, test recordings and transcriptions, iteratively building understanding about different types of privacy concern manifestations.

4 Results

The idea and the purpose of the application got very warm reception among the test participants. For example, one participant told that: "Personally I have had need for this kind of service for a long time."[3] (P1) The participants operated very fluently through the main use case, i.e. all the test tasks from installing the application to creating an event and sharing some content in it. The main use case was a logically flowing procedure and well understood by the users. No major usability problems were observed in the operation and, thus, the system usability was considered rather excellent in that regard.

However, the observations indicated that participants were more concerned of application use before and after the actual event took place. Largely, these were concerns of personal privacy, intimacy and security that were attributable to certain features and functions of the application. Before the event, the participants were mainly concerned of administrative rights of the founder of the event. The participants did not easily perceive their rights and responsibilities before creating and sharing the event to others. After the event and as a member of the specific event, the participants were mainly concerned of what rights and possibilities they have in downloading and deleting, possibly embarrassing, photos shared in the event. Such privacy concerns and related conceptual design directions were introduced as the main results of the test for the developers and discussed next in detail.

First, some of the privacy concerns were manifested explicitly, because the participants could identify and express a privacy problem in detail. For example, the majority of the participants spontaneously remarked that the event founder has a possibility to change the name of the event after people had already joined it. Others considered renaming a compulsory feature that should not redesigned, while the rest pointed out its problems if the founders misused the feature and the application did not inform the attendees about the name change. Although the participants' opinions were polarized,

[3] Participants' comments are translated from the original to English language. P1 refers to test participant 1.

they all identified and acknowledged the privacy risk attached with the feature. Renaming is possible also in other SNSs that allow creating groups and shared spaces (e.g. Facebook), which may be the reason for the sensitivity and awareness of the participants for this privacy concern. The studied SNS did not support users' need to regulate their territorial outward-facing boundaries, which means for example withdrawing from obscene content posted on user's wall[4]. As with other SNS, the participants needed to select a corrective coping mechanism with the risk (e.g. unjoin the event), because no other solutions were implemented or preventive coping mechanisms available.

Second, and in contrast to clear identification of the risks in advance, the participants were totally unaware of some of the privacy risks and consequences of features used. In particular, they had problems in understanding how the duration of the event affected on its visibility and accessibility (i.e. publicity). For example, one participant assumed that after the event reaches its end duration it will be not visible in the public map and accessible through the search functions of the application i.e. eventually it "becomes private" (P3). Instead of restricting public discovery, another participant interpreted that the duration only closes the possibility to upload more photos to the event. Privacy concerns then varied between disabling and blocking interactional boundaries (i.e. giving access to oneself) to regulating territorial inward-facing content (i.e. what appears in a "news feed"). Both assumptions about the functioning above seem to be justified, although wrong, interpretations about the of the feature: The duration only restricted new joining the event i.e. controlled network-discovery boundaries (i.e. access to network) and relationship boundaries, which regulate whom one lets be part of network. This example further shows how users can be unaware of or misinterpret privacy related consequences when they are not exactly sure about the meaning of a functionality. Moreover, such features may not be related to built-in "privacy settings" at all. Nevertheless, the participants seemed to naturally relate the use of these features of the SNS to privacy issues and made them part of their personal privacy management. The utmost problem of this type of concerns is that users may not identify and apply any coping mechanisms at all, as the privacy problem itself stays hidden in the first place. This kind of a situation leads users inevitably to corrective mechanisms after the risk has realized, although the effectiveness of the chosen mechanism may vary by case. Similar, unintended privacy violations were common in the context of P2P file sharing due to misunderstood logic and functions of the application [23]. For the developers, these types of privacy concerns indicate a need for clarifying the meaning of the feature in a way that decreases misunderstandings by the users and gives them all the potential to evaluate the threat to their privacy. In this case, the application could have implemented a simple text explaining the meaning of the event duration.

Third, a type of privacy manifestations became apparent when the participants had a clear expectation about how something should be working and a vision of to-be state of the system regarding the privacy issue. In this type of manifestation, they not only expressed and identified their potential privacy concern, but they were astonished about certain functions (i.e. they expect something else to happen) and/or had alternative

[4] Privacy boundaries and coping mechanisms are discussed based on Karr-Wisniewski et al. (2011) [18] and Wisniewski et al. (2016) [19].

(technical) solutions directly in their mind. For example, the participants raised a highly negative concern of someone uploading inappropriate photos to the service and, in the first place noted, about their inability to remove these photos. “If someone takes a photo of me vomiting and I cannot do anything for it without contacting the application developer, it is very sad. Ok, the same problem appears in other applications, also in Facebook […] but here I feel it is a bigger problem because this application has a different kind of character.” (P6) According the participants, an inappropriate photo of oneself – or even a photo where ones “hair is not washed or set correctly” (P7) – should be possible to delete. These privacy concerns relate to missing corrective mechanisms for regulating confidant-disclosure boundary, which occurs when someone publishes personal information about someone else. Deleting the uploaded content was possible only for the founder of the event. The event represents its founder’s “wall”, where the system supports both territorial outward-facing and confident-disclosure controls only for the founder. Because one’s own photos were not removable either, this privacy concern is also about controlling the boundary of self-disclosure, which considers what personal information one discloses in the network.

Another example about third type of privacy manifestation became during inviting people to the event. In the role of the founder of the event, the participants made an instant assumption that if they create a private event, they will know who have been invited in the event and that they can moderate invitations i.e. control who will get the invitation. The assumption was however false, because the invitations were sent with a code in an email or in a SMS message that could be shared further by the receivers. The situation weakens users’ trust towards the applications features and their own capabilities to preserve privacy of the photos and overall intimacy of the event: “If there is an option to create either a public or a private event, I suppose I should be able to monitor and moderate that private event… it is quite unpleasant situation if anybody can invite any friend, and at that stage, my trust is not very high that my shared photos will remain private… that can be a serious problem to someone.” (P7). Thus, regulating one’s relationship boundaries within the event in a preventive way was poorly supported. On the other hand, the participants found that the event founder could select and remove specific individuals from the event. However, the participants did not discuss this corrective mechanism as a solution to the initial controlling problem probably because the damage had been already done: The mechanism came too late (i.e. corrective) and was not effective for the initial problem that needed mechanisms that are more preventive. Now the participants implicitly employed a collaborative mechanism not to share the code with third parties.

Fourth, a type of privacy manifestation was related to use situations where the participants felt unconfident and uncertain about the actions they had taken and their effects within the application (e.g. what just happened?) or in some other way expressed distrust towards the system. For example, the application did not give any feedback whether the invitation message was delivered or not: “I suppose the message was sent” (P6), “You get a feeling that you should send the message again” (P5). The subsequent privacy related problem the participants experienced was that the founder did not know how many and to whom invitations were already sent, thus jeopardizing again their control of relationship-connection boundaries. The problems related to the technical

infrastructure, in this case mostly the slow speed of the mobile internet connection, introduced more these type of privacy concerns among participants. A common denominator is that these took place by accident. For example, five out of seven participants used their own smart phones in the test, which meant that their phones were of different quality and speed in internet connection during the test. Quite many suffered from poor quality of the touch screen (P7), slowness of the phone and the internet connection (P5, P6, P7), or slowness of the service response on the server side (P5), and dismissed point of touch (P1). These became privacy concerns, because participants were uncertain if and when something was touched, downloaded and uploaded and so forth: "I am always about to press twice because this does not show the download symbol…[waiting]…now it shows that it is going somewhere." (P6). For example, one participant meant to scroll the screen by wiping, but notified few minutes later that he had accidentally joined an event (i.e. pressed the join-button instead wiping). This raised a user requirement for the application to confirm whether "you really want to join?"(P5). With the dialog, users could better control their identity and self-presentation (see [7]). Adding photos and videos to the event introduced another accidental privacy threat that was due to inconsistent interface design and slowness, which similarly made participants feel unsure whether some action were already processing. Adding a photo from the photo gallery did not have any confirmation dialog (as when using the camera application) and users needed to pick the photo without viewing it in a full screen. That increased the risk of uploading a wrong photo: "Pretty odd that it did not ask if I want to share this photo but it directly shared it. What if I had touched the wrong photo?" (P3) Another participant (P5) uploaded two times the same video, because of the missing confirmation dialog and the slow internet connection, which prevented him noticing the ongoing video uploading. The fourth type of privacy manifestations tended to end up in users' distrust or in inventing preventive technical mechanisms. Confirmation dialogs for both photo uploading and joining the event, as well as system status feedback introduce simple preventive solutions for regulating self-disclosure when the corrective ones were not supported (e.g. deleting own photos).

5 Conclusions

Usability testing as a method for the evaluation of SNS prototypes seems to invoke spontaneous privacy concerns among test participants. The behavioral patterns of how privacy concerns emerged in the formative usability test of the application were of four distinct types (Table 1). Users either *expect* a certain system behavior, *identify* a privacy risk directly, *feel* unconfident about system behavior, or *are unaware and assume* potential privacy risks to be present. The types are not exclusive, but rather related and represent a continuum from users being ignorant or slightly worried to expressions that involve more detailed risk identification and suggestions for improvement. For example, when people have strong expectations about the desired level of privacy regarding some functionality and suggest some improvement, they presumably also can identify the risk in detail. Based on the case findings, we emphasize that users do not necessarily express any explicit concern. They can be unaware of the meaning and functioning of

some specific feature, which eventually will affect their achieved and experienced level of privacy. Thus, a privacy risk itself may stay hidden during use and require interpretation by the evaluators, in order to become exposed and eliminated by redesign – as is the common case with usability problems analysis in general. This work is complicated by the wide range of system features that have an effect on privacy, but that are not part of official privacy settings at all. Most likely, these "hidden" features are in the majority and lead to users' false assumptions or stay unrecognized during the first-time use. For example, "often participants did not know that private information was being shared at all and blamed the site"[5] and did not exploit interface controls available for information disclosure. Respectively, users may explicitly express a privacy concern related to some feature when it actually does not have an effect on their privacy. However, there are no false positives when experiencing something: The desired level of privacy is based on personal experiences and satisfaction, and it is important to collect these experiences and fix the misunderstandings caused by the design.

Table 1. Types of manifestations of users' privacy concerns during a formative usability test

Types of privacy manifestations	**How manifests in a usability test?**	**Example in the case study**	**Unsupported mechanisms[6]**
Users *expect* a certain system behavior	Users require corrective and preventive functions	Removing own and others' photos of oneself; disseminating invitations to strangers	Confidant-disclosure; Relationship-connection
Users *identify* a privacy risk directly	Users point out how a feature can be misused	Obscene renaming of the event by the founder	Territorial outward-facing
Users *feel* unconfident and express distrust	Users wish for preventive functions, more control and consistency of features	Confirmation dialogs for joining the event and uploading content; technical infrastructure problems	Relationship-connection; Self-disclosure
Users *are unaware* of risks or assume potential	Users misunderstand a meaning of a feature	Setting the duration of the event	(Experienced by the users:) Territorial inward-facing; Interactional disabling and blocking

The procedure of the usability testing applied in the case study was very classical in nature. The industry and practitioners employ widely this kind of formative usability testing for the systems and prototypes under development. The interactive and relaxed think-aloud protocol applied in the study is the most used protocol in usability testing [21]. The chosen think-aloud protocol affects very little on the number and type of usability problems found [24]. Therefore, we must emphasize that, in this setting, the test participants brought up the privacy issues naturally and spontaneously in discussion about system features and usability. This natural approach for privacy exploration, the lack of explicit privacy questions and exploring concerns of first-time users is different from research settings found in literature. For example, Sadeh et al. [25] deliberately

[5] [18] p.5

[6] Coping mechanisms that the studied SNS did not support (see [19]).

designed their study for understanding people's attitudes and behaviors towards privacy when they interact with an application. That kind of predefined and experimental approach to study privacy would naturally be the most beneficial in improving the match between the preferred and implemented levels of privacy during the system development. On the other hand, this is not always possible and a need arises to observe privacy related concerns and behavior as a natural part of user-centered methods, in which this paper has contributed. Spontaneity of privacy concerns drives us to note that usability is a privacy issue, equally as it has shown to be a security issue [26]. Users can desire some level of privacy only to the extent they are conscious of such state. Achieving a certain level of privacy depends on the usage skills of the user as well as on what the system offers. In that regard, the users' both privacy states, desired and attained, are phenomena that traditional usability testing can help to explore. The coping mechanisms presented by [8], and [18,19] help us in understanding the nature and causes of the issues unearthed in testing as well as in making more adequate suggestions for system redesign.

In our case, we could especially observe situations where the users experienced too low privacy levels [9]. This is because usability testing is a problem-centric technique that does not strive for positive findings i.e. it is not targeted at identifying situations where the system exceeds all the expectations of the users. Moreover, the users' concerns and coping mechanisms in the test were not real behavioral adaptations in the long term, but their intentions and conceptions due to the first time and short-term use situation. Originality of this research lays, apart from scrutinizing usability testing as a method for revealing potential privacy issues, also in studying privacy concerns of first-time users with a short-term user intervention during the system development phase. Users' intuitive and instant opinions about system privacy have definitely practical value in systems development, but may also offer analytical insights into how privacy concerns change over time; what kind of system features are involved in these considerations; and how SNSs can provide new controls and support mechanisms in the future. These are also interesting new research areas.

The types of privacy concern manifestations presented here are to help design practitioners pay attention to privacy as a natural part of practicing user-centered design methods. The found types do not represent a complete set of all possible user behaviors, nor are all technological and interpersonal coping mechanisms found in the literature present and applicable in the context of this research (cf. [18,19]). Our analysis leans on one usability test only. The studied application was very simple system compared to features and purposes of the most popular SNSs. Built around real-life events, without a list of friends to traverse or interpersonal relations as its primary focus, the application could only involve few mechanisms for regulating personal privacy. The method used here could be used to discover different privacy coping mechanisms applied within different kinds of more complex SNSs in the future.

References

1. Iachello, G., Hong, J.: End-user privacy in human-computer interaction. Foundations and Trends in Human-Computer Interaction 1(1), 1-137 (2007)

2. Vitak, J., Wisniewski, P., Page, X., Lampinen, A., Litt, E., De Wolf, R., Kelley, P.G., Sleeper, M.: The Future of Networked Privacy: Challenges and Opportunities. In: Cosley, D., Forte, A., Ciolfi, L., McDonald, D. (eds.) Proceedings of the 18th ACM Conference Companion on Computer Supported Cooperative Work & Social Computing, pp. 267-272. ACM, New York (2015)
3. Dourish, P., Anderson, K.: Collective information practice: Exploring privacy and security as social and cultural phenomena. Human-computer interaction, 21(3), 319-342 (2006)
4. Wisniewski, P., Lipford, H., Wilson, D.: Fighting for my space: Coping mechanisms for SNS boundary regulation. In: Konstan, J.A., Chi, E.D., Höök, K. (eds.) Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 609-618. ACM, New York (2012)
5. Lampinen, A., Stutzman, F., & Bylund, M.: Privacy for a Networked World: bridging theory and design. In: Tan, D., Begole, B., Kellogg, W.A. (eds.) CHI'11 Extended Abstracts on Human Factors in Computing Systems, pp. 2441-2444. ACM, New York (2011)
6. Workshop at CHI 2016: Bridging the Gap between Privacy by Design and Privacy in Practice. Call for Participation. https://networkedprivacy2016.wordpress.com/call-for-participation/
7. Boyle, M., Greenberg, S.: The language of privacy: Learning from video media space analysis and design. ACM Transactions on Computer-Human Interaction, 12(2), 328-370 (2005)
8. Lampinen, A., Lehtinen, V., Lehmuskallio, A., Tamminen, S.: We're in it together: interpersonal management of disclosure in social network services. In: Tan, D., Fitzpatrick, G., Gutwin, C., Begole, B., Kellogg, W.A. (eds.) Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 3217-3226. ACM, New York (2011)
9. Wisniewski, P., Islam, A. K. M., Knijnenburg, B. P., Patil, S.: Give Social Network Users the Privacy They Want. In: : Cosley, D., Forte, A., Ciolfi, L., McDonald, D. (eds.) Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing, pp. 1427-1441. ACM, New York (2015)
10. Gross, R., Acquisti, A. (2005). Information revelation and privacy in online social networks. In: Atluri, W., De Capitani di Vimercati, S., Dingledine, R. (eds.) Proceedings of the 2005 ACM workshop on Privacy in the electronic society, pp. 71-80. ACM, New York (2005)
11. boyd, d. m., Ellison, N. B.: Social network sites: Definition, history, and scholarship. Journal of Computer-Mediated Communication 13(1), 210-230 (2008)
12. Kietzmann, J. H., Hermkens, K., McCarthy, I.P., Silvestre, B.S.: Social media? Get serious! Understanding the functional building blocks of social media. Business Horizons 54, 241-251 (2011)
13. Altman, I.: The Environment and Social Behavior - Privacy, Personal Space, Territory, Crowding. Brooks/Cole Publishing Company, Monterey (1975)
14. Palen, L., Dourish, P.: Unpacking privacy for a networked world. In: Cockton, G., Korhonen, P. (eds.) Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 129-136. ACM, New York (2003)
15. Tan, X., Qin, L., Kim, Y., Hsu, J.: Impact of privacy concern in social networking web sites. Internet Research 22(2), 211-233 (2012)
16. Metzger, M. J., Docter, S.: Public opinion and policy initiatives for online privacy protection. Journal of Broadcasting & Electronic Media 47(3), 350-374 (2003)
17. Yao, M. Z., Rice, R. E., Wallis, K.: Predicting user concerns about online privacy. Journal of the American Society for Information Science and Technology, 58(5), 710-722 (2007)
18. Karr-Wisniewski, P., Wilson, D., Richter-Lipford, H.: A new social order: Mechanisms for social network site boundary regulation. In: Sambamurthy, V., Tanniru, M. (eds.) Proceedings of Americas Conference on Information Systems, pp. 1-8. AIS, Detroit (2011)

19. Wisniewski, P., Islam, A.K.M. N., Richter Lipford, H. Wilson, D.C.: Framing and Measuring Multi-dimensional Interpersonal Privacy Preferences of Social Networking Site Users. Comm. of the AIS. 38, 235-258 (2016)
20. Besmer, A., Richter Lipford, H.: Moving beyond untagging: photo privacy in a tagged world. In: Mynatt, E., Fitzpatrick, G, Hudson, S., Edwards, K., Rodden, T. (eds.) Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 1563-1572. ACM, New York (2010)
21. Boren, T., Ramey, J.: Thinking aloud: Reconciling theory and practice. IEEE Transactions on Professional Communication 43(3), 261-278 (2000)
22. Hertzum, M., Hansen, K. D., Andersen, H. H.: Scrutinising usability evaluation: does thinking aloud affect behaviour and mental workload?. Behaviour & Information Technology 28(2), 165-181 (2009)
23. Good, N. S., Krekelberg, A.: Usability and privacy: a study of Kazaa P2P file-sharing. In: Cockton, G., Korhonen, P. (eds.) Proceedings of the SIGCHI conference on Human Factors in Computing Systems, pp. 137-144. ACM, New York (2003)
24. Bruun, A., Stage, J.: An Empirical Study of the Effects of Three Think-Aloud Protocols on Identification of Usability Problems. In: Abascal, J., Barbosa, S., Fetter, M., Gross, T., Palanque, P., Winckler, M. (eds.) Human-Computer Interaction - INTERACT 2015. LNCS vol. 9297, pp. 159-176. Springer International Publishing, New York (2015)
25. Sadeh, N., Hong, J., Cranor, L., Fette, I. Kelley, P., Prabaker, M., Rao, J.: Understanding and capturing people's privacy policies in a mobile social networking application. Pers. Ubiquit. Comput. 13, 401–412 (2009)
26. Whitten, A., Tygar, J. D.: Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In: Treese, W. (ed.) Proceedings of the 8th USENIX Security Symposium, pp.169-184. Usenix, Washington, (1999)