International Conference on Information Systems (ICIS)

ICIS 2008 Proceedings

Association for Information Systems *Year* 2008

Privacy Design in Online Social Networks: Learning from Privacy Breaches and Community Feedback

Seda Gurses* Ramzi Rizk†

Oliver Gunther‡

*K.U. Leuven, seda.guerses@cs.kuleuven.be

†Humboldt-University, Berlin, rizk@wiwi.hu-berlin.de

‡Humboldt-University, Berlin, guenther@wiwi.hu-berlin.de

PRIVACY DESIGN IN ONLINE SOCIAL NETWORKS: LEARNING FROM PRIVACY BREACHES AND COMMUNITY FEEDBACK

Conception de la vie privée dans les réseaux sociaux numériques : apprentissage suite à des manquements et aux retours de la communauté

Research-in-Progress

Seda Gürses
Department of Computer Science
K.U.Leuven
Celestijnenlaan 200A - bus 2402
B-3001 Heverlee
Belgium
seda.guerses@cs.kuleuven.be

Ramzi Rizk
Institute of Information Systems
Humboldt-Universität zu Berlin
Spandauer straße 1 D-10178
Berlin, Germany
rizk@wiwi.hu-berlin.de

Oliver Günther
Institute of Information Systems
Humboldt-Universität zu Berlin
Spandauer straße 1 D-10178
Berlin, Germany
guenther@wiwi.hu-berlin.de

Abstract

The objective of this paper is to systematically develop privacy heuristics for Online Social Network Services (SNS). In order to achieve this, we provide an analytical framework in which we characterize privacy breaches that have occurred in SNS and distinguish different stakeholders' perspectives. Although SNS have been criticized for numerous grave privacy breaches, they have also proven to be an interesting space in which privacy design is implemented and critically taken up by users. Community involvement in the discovery of privacy breaches as well as in articulating privacy demands points to possibilities in user-driven privacy design. In our analysis we take a multilateral security analysis approach and identify conflicts in privacy interests and list points of intervention and negotiation. In our future research, we plan to validate the usefulness as well as the usability of these heuristics and to develop a framework for privacy design in SNS.

Keywords: Privacy, Social Software, Privacy Design, Privacy Negotiation, Systems Analysis and Design/ Development

Résumé

L'objectif de ce papier est de développer de manière systématique des heuristiques de confidentialité pour les services de réseaux sociaux en ligne. Dans ce but, nous analysons et catégorisons les brèches de confidentialité dans les réseaux sociaux et listons leurs propriétés spécifiques. Dans notre analyse, nous adoptons une approche par une analyse de sécurité multilatérale et nous identifions les conflits d'intérêt liés à la confidentialité ainsi que les points d'intervention et de négociation.

Introduction

Over the past few years, a veritable profusion of SNS have appeared on the Internet, designed to prod, 'poke' and seduce users into confessing ever-greater amounts of personal information. Today, online social networks like Facebook or MySpace are radically redefining the nature of social interaction on the Internet, and accordingly the substance of the online public sphere as such.

Socially, as well as economically, SNS are interesting. A number of disjoint user profiles floating around in cyberspace have limited worth, but once these profiles are associated with one another by means of 'relationships' their worth increases drastically for the owners of these profiles, and even more so for the providers. Microsoft's recent investment in Facebook valuated the latter at $16bn. With over 50 million users at the time, this put each Facebook user's worth at around $300.

Ever since SNS became mainstream, they have been rebuked for playing an active role in the 'privacy nightmare' on the Internet. SNS are held responsible for the naive voluntary auto-profiling of Internet users. Users of SNS are accused of being uninformed, in contradiction with their privacy concerns, or simply giving in to a badly conceived trade-off between their privacy and functionality (Berendt et al. 2005). These viewpoints currently dominate the privacy debate on SNS in academia and the media.

In this paper, we start with the assumption that SNS actually are an interesting space on the Internet for engaging in privacy (Albrechtslund 2008). By virtue of being public and popular, SNS make evident privacy problems elsewhere on the Internet e.g. emails, discussion forums, chats, e-commerce etc. In no other web applications are the user communities so actively involved in privacy debates. We also assume that privacy is not something concrete, in consensus and in constant danger. Rather, we conceive privacy as a set of practices to negotiate which should remain public or private in social contexts (Phillips, 2004). Legal and other regulatory frameworks and various social mechanisms are there to ensure that individuals can practice their privacy (Gutwirth 2002, Nissenbaum 2004).

We are concerned with the translation of these “privacy practices” into a software engineering problem. Although by now privacy research is well established in different sub-fields of computer science, the systematic application of those results while engineering information systems remains an open research field. For example, security engineers have developed Privacy Enhancing Technologies (PETs), identity management systems (Hansen et al. 2004) and privacy metrics; data miners have studied privacy preserving data mining methods (Vaida 2006); usability engineers developed usable privacy designs (Jensen 2005) etc. But, how and when should we apply this plethora of privacy tools and methods and which privacy breaches do these tools exactly engage with?

Universal definitions of privacy or definitions of privacy reduced to confidentiality are not adequate points of departure for engineering systems. Rather, it is important to determine what counts as privacy concerns from the perspectives of the different stakeholders in a specific domain. SNS, our domain of interest, contain both examples of breaches general to the Internet, as well as breaches that are specific to these applications. A deeper understanding of these specific privacy concerns from the perspective of the different stakeholders and possible design solutions to them is the topic of this paper.

The rest of this paper is organized as follows. Section two discusses major privacy breaches picked up by the SNS community and media. For each breach we map out the properties of the breaches. We group these into four main categories: indeterminate visibility, separation of identities, contested ownership and misappropriation, and propose design heuristics and other non-technical measures to protect against each. We conclude by discussing our results and pointing to future research.

Privacy Design through Analysis of Common Privacy Breaches in SNS

SNS are not free of common privacy breaches like communication intrusion, identity theft, phishing, stalking, information leakage etc. (ENISA 2007). However, certain characteristics of SNS open up possibilities for new kinds of privacy breaches. These breaches primarily result from the fact that users reveal detailed information to the public and map their real-life social relationships more explicitly than they would in emails or on public forums.

At the same time, these public revelations have an advantage when it comes to privacy. Users act as a community to notice and inform each other of privacy problems and on ways to avoid them. They use their relationships to put

pressure on SNS providers to make the relevant changes. Furthermore, user interaction might help to identify conflict in privacy interests, leading users to ask for mechanisms to negotiate these conflicts. In this sense, SNS are an interesting domain for promoting privacy practices on the Internet that are not only motivated by the profit interests of providers. They therefore provide an interesting opportunity for doing user-driven privacy design.

In the following we introduce our analytical framework for SNS privacy breaches. Methodologically, the analysis is a result of three studies. First, we studied literature defining different analytical frameworks on privacy breaches in information systems. In parallel, we studied prominent privacy breaches that occurred in Facebook and Myspace – two popular, and similar, SNS. In a cyclical manner, we refined our categorization of privacy breaches to the final four presented here and classified the different breaches under those categories.

The four categories are based on discussions of characteristics of privacy breaches by Phillips (2004), Braman (2006), Nissenbaum (2004) and Solove (2007). Phillips argues for the importance of negotiating the line between the public and the private. Solove classifies legally accepted cases of privacy breaches in the USA under the categories: information collection, processing and dissemination. Nissenbaum brings an alternative to universal accounts of privacy and breaches with her notion of contextual integrity. She argues that contexts are governed by information norms: norms of appropriateness and norms of flow or distribution. Lastly, Braman points to problems that arise under surveillance in combination with privacy technologies. These she calls misappropriation by memory, perturbation, abandonment of accuracy, and inference attacks.

The privacy breaches we study are selected from a greater pool of privacy breaches in SNS mentioned in news and the blogosphere. We conducted a series of queries in google news and digg.com[1] for articles published between October 2007 and March 2008 on privacy breaches in SNS. Of the 154 articles returned in digg and 380 articles returned in google, 55 in digg an 69 in google discussed privacy breaches which we tagged. The figures below show tag-clouds from those news articles, bigger words representing higher tag frequency.

Figure 1.Google result tag-cloud

Figure 2. Digg result tag-cloud

An emphasis of our framework is on the multilateral analysis of the privacy concerns of the stakeholders of social networks. Namely, we analyze privacy issues that arise among users, between users and SNS providers and between users and third party service providers.

Finally, our design solutions to the privacy breaches are supported by literature on privacy research in computer science as well as some critical points raised by Gutwirth (2002), Braman(2006) and Nissenbaum (2004).

Breaches related to Indeterminate Visibility

With *indeterminate visibility* we denote the problem of a user's profile information being visible to others without the user's explicit knowledge or approval. Given that SNS users want to make their information available such that their audiences can find them, this breach often arises after users volitionally but unwittingly publicize information to a wider audience than they actually intended. The indeterminate visibility problem arises for a number of reasons:

Poor usability: although all SNS offer some privacy controls by now, the functional effects are often not transparent enough. Previous studies suggest that users often use default settings (Mackay 1991, Gross 2005). Studies on Facebook suggest that users unwittingly make mistakes in their privacy configurations, find them time consuming (Lipford et al. 2008), or simply assume that their profiles are private (Rosenblum 2007).

[1] Google news: http://news.google.com, dig: http://www.digg.com

Promoting profile publicity: SNS providers have an interest in the wide release of data to a greater audience and to third-party providers. In its Privacy Policy (PP), Facebook admits that part of the user profiles may be made available to third party search engines (Facebook PP 2008). This may conflict with the users' interest to determine the visibility of their data, is likely to cause indeterminate visibility and requires legal as well as social intervention.

Relational information: *Relational information* is any information that is controlled by multiple users. Different users may have different or even conflicting visibility settings on their relational information. A good example of a relational information related conflict is the trail of crumbs left by users when they visit other users' profiles. StudiVZ.net users (StudiVZ 2008) can see which other users visit their profiles. StudiVZ allows users to turn that feature off, and invisibly browse through other users' profile pages. A conflict arises here: the owner of a profile may want to know who has visited their profiles, whereas the visitor may want that visit to remain anonymous.

Transitive access control: Social networks can easily be modeled as graphs with nodes representing users and edges represent relationships among users. With *transitive access control* we denote the granting of access to resources based on the existence of a path of certain degree in the network between two users. Therefore, making a resource visible to friends of friends (FoF) of user A, allows all users with a path the length of 2 to A to see her resources. In such a case, the visibility of certain information is co-defined by friends of A. Especially considering that in networks with small world properties, transitive visibility may result in revelations to the complete network, transitive access control contributes to indeterminate visibility. A bug in Facebook actually proved such danges when it revealed unique album ids when commented. This made private albums visible to the whole network. Finally, using different depths of transitive access control on different resources might lead to unintended information revelation or concealment.

Privacy Design Heuristics

Enhancing usability: A privacy-friendly design should explicitly require users to opt-in before profiles are made publicly visible. This goes hand in hand with numerous recommendations of privacy legislation and guidelines. Degrees of opting-in should support users in getting out of the trap of submitting all their information as a trade-off for functionality. At the same time, over-protective privacy settings should not limit users' freedom of activity.

The usability of privacy settings should be part of the design and validation process. Still, providing privacy settings should not absolve providers, third parties or even communities of their responsibilities. A multilateral security and privacy requirements analysis should be used to determine the distribution of privacy responsibilities (Gürses 2006).

Possible measures to alleviate indeterminate visibility breaches of privacy include clearly showing the visibility of each private object ('only friends are allowed to see this information', or 'only you can see this'). There is a need to define standardized visual cues for data that is public or private. Furthermore, SNS providers should provide easy to use tutorials and tips on privacy settings for users, as well as extended options for the more privacy-aware users.

Relational information negotiation: relational information problems, like the conflict between "visitor anonymity" vs. "profile privacy", as in the case of trail of crumbs, should be made explicit. Negotiation should be made possible and visual cues should inform users of these conflicts and ways of negotiating them.

Provider user negotiation: privacy settings in SNS can also provide users the possibility to negotiate their visibility with providers. Usability, context based vs. centralized privacy settings, legal enforcement of settings, as well as the complexities of relational information have to be taken into account when designing privacy settings for user-provider negotiation of privacy.

Simplifying Transitive Access Control: Transitive access control, which becomes even trickier when multiple layers of data have varying degrees of transitivity, poses demanding and interesting information theoretical inference problems. A systematic evaluation and validation of privacy settings with transitive access control is necessary. Currently, this kind of analysis is done ad-hoc by interested users – users communicate to confirm the visibility of resources despite their privacy settings. Visual cues i.e. this is the graph of all friends of friends and they can see these resources, can be used to inform users of the reache*s* of transitive access control.

Indeterminate visibility breaches are related but not limited to the security goal of confidentiality. Confidentiality guarantees that only authorized persons have access to the information in a system. Confidentiality is monotonic, once information has been revealed, the confidentiality of that information cannot be restored. The containment of visibility can be less strict. Users may decide to change the visibility of their profile as a part of their privacy goals. The concealment of previously public information or vice versa may be part of the privacy negotiation process. Therefore, the design of privacy needs to go beyond the security engineering view of confidentiality preservation.

Nevertheless, the validation of the transitive access control settings has to be done diligently.

Breaches related to Separation of Digital Identities and Aggregation

Separation of identities is the term used to refer to the construction of social identities by individuals that selectively reveal and conceal information in specific contexts and roles (Phillips 2004, Nissenbaum 2004). On the internet, *separation of digital identities* can be comparable and is as easily established as breached in SNS. We distinguish between two kinds of separation of identities in SNS.

Internal separation of digital identities: is about allowing users the freedom to strategically reveal different profile information to different persons in their SNS. Aggregation of data may easily breach users' internal separation of identities. One such breach happened in the early version of Facebook's feeds. Users were unaware that their information was being collected, aggregated, and posted to their friend's feeds (Boyd 2006).

External separation of digital identities: is about the ability of an individual to create multiple profiles on a given SNS or in different digital environments. We distinguish two kinds of privacy breaches in this respect:

1.User driven external separation breaches: These have to do with the advent of open standards and the possibility to exchange ones social graph between various SNS. What users make available to friends on one network is not necessarily something that they want to make available to friends on another network. This applies particularly to users' profiles on informal networks (Facebook, MySpace) where the settings might be looser, and the same users' profiles on professional networks (LinkedIn, Xing) where they might want to present themselves more formally.

2.Provider driven breaches: 'Facebook Beacon' is an example of a breach of external separation of identities driven by providers, including third party providers. Beacon is a tracking system, integrated on external platforms. It reports user activities to Facebook and informs a user's contacts of those activities. Facebook originally marketed Beacon to potential businesses by stating 'The user can choose to opt out of the story, but the user doesn't need to take any action for the story to be published on Facebook' (Facebook Beacon 2007). User outrage led them to rethink their privacy policy, and that statement was replaced by 'The user must proactively consent to have a story from your website published' (Facebook Beacon 2008)[2].

Privacy Design Heuristics

Managing internal separation of digital identities: Allowing users to have groups of friends and set visibility rights to each group is important to achieve internal separation of identities. Facebook has recently implemented highly granular access control settings enhancing internal separation of identities. Nevertheless, smart grouping methods and increasing the usability of such "end-user privacy administration" tasks is necessary.

The management of internal separation of identities can be enhanced through *mirrors* of the user's different profiles. This feature, once activated, could show what for example a friend vs. a colleague can see of the user, reflecting their various identities in the "mirror". Reflective features generally could help to visualize for the user his or her data traces before they are published.

A privacy-aware broadcast feature like the Facebook mini-feed could allow users more granular approval for the information they release in the feed. The approval feature could include details like which of their friends, or which groups of friends are allowed to see each feed. The recent introduction of 'lists', which allow Facebook users to group and categorize their contacts, is a good first step in that direction. Additionally, frequent and detailed prompts for data release approval may be critical to the usability of the privacy functionality. In response, users may prefer to turn off the functionality or revert to default settings, leading to privacy breaches (Lederer et al. 2004). The complete deactivation of such broadcast features must be available to the users.

Managing and guaranteeing external separation of digital identities: Providers may breach external separation of digital identities when different profiles of a user hosted by cooperating providers contain common identifying information. SNS therefore is a domain in which users can make use of linkability analysis tools and related identity partitioning tools (Berthold et al. 2007; Borcea et al. 2005). These tools can help users in managing multiple pseudonymous accounts in case the providers collaborate and alert users when two pseudonyms can easily be linked.

[2] Later announcements from privacy activists show that the opt-in is not only lacking, but also that Beacon continued to aggregate data. The data was simply not being shown to users' friends anymore.

Features that effect external separation of identities need to allow users complete control over what information is shared, with whom, and how. Providers should also make global deactivation easily accessible and usable. This is in stark contrast to Beacon's original purchase-by-purchase or vendor-by-vendor opt-out solution. In case users opt-in to cross-platform aggregation to be published on their SNS, the one-by-one approval function can be applied.

The overload from managing multiple platform aggregation may be diminished using P3P like policies (Preibusch et al. 2007). The aggregate data should be subject to previously defined guidelines, e.g. the Fair Information Practices (OECD 1980). We nevertheless beg caution, since policies and guidelines have little or no meaning if the necessary legal and social standards are not there to accompany them (Möller 2003).

External separations of identities breaches caused by porting social graphs across platforms require new negotiation mechanisms. Friends in one network must be able to refuse to be listed as friends in another. In this sense, the release of such information external to the original SNS is similar to an external transitive access control and requires further studies.

Breaches related to Contested Ownership

With *contested ownership* we describe the explicit and implicit definitions of data ownership that may lead to privacy breaches. Specifically, we distinguish between contested ownership issues upon joining and leaving an SNS.

Provider contestation of data ownership: Users practically surrender their "right to be let alone" as soon as they sign up to an SNS. The conditions of this deliverance are set up in SNS policy documents and often merge the provider's right to circulate the content world-wide and the ownership of the data. For example, Facebook's Terms of Use states: 'When you post User Content to the Site, you authorize and direct us to make such copies thereof as we deem necessary [...] By posting user content you grant the company an Irrevocable, perpetual, transferable license to use, copy, publicly perform, publicly display, excerpt and distribute such User Content for any purpose, commercial, advertising…' (Facebook ToU 2008). This statement actually accompanies another one suggesting that 'Facebook does not assert any ownership over your User Content'. Policy documents that are within themselves contradictory leave users in despair as to exactly what ownership means on SNS.

The complications in ownership with respect to relational information and aggregated data are often not addressed in privacy policies. It is usual that privacy policies pose the question of ownership as one that is between a single user and the provider of the SNS. This produces a grey zone with respect to data that belongs to many. Especially in the case of the aggregate data it is assumed that SNS providers reserve the right to all aggregated data and derivatives thereof. We will address aggregate data further in the Section on misappropriation.

User contestations of relational information ownership: Once the SNS membership is established, users inevitably start producing relational information. Relational information, as defined earlier, results in *ownership interdependency*. Who will identify when relational information will be visible, to whom, who will be able to alter and finally delete that information? For example, user A wants to publicize all her activities. She comments one of friend B's photos, only visible to friends. May A: publicize that she commented? show the content of the comment? the picture that was commented? Who actually owns the comment? So, whose privacy settings should this comment subscribe to, to that of the author of the comment, or the owner of the commented photo?

The ownership interdependency issue also occurs with regards to tags and links. Many SNS nowadays allow users to tag uploaded content. On photos, owners can tag a specific part of the photo and associate it with a friend by linking it to their profile. On face value, these tags confirm the presence of the tagged user on the SNS and link to his profile. As soon as a photo is tagged, the ownership questions arise by virtue of being relational information.

Profile removals and contestations of ownership: If SNS policies per default ask for a license to circulate profile information widely and to share it with third parties, it remains unclear exactly how the removal of a profile effects the circulated copies. Even worse, Facebook asserts in their Terms of Use that removing User Content amounts to an expiration of that license. But, how exactly User Content is removed is not explained. Actually, deleting an account in Facebook, as opposed to deactivating it, is a long and tedious process. Upon simple deactivation, the data remains on the servers. Users must go through a complicated process to delete their profile, including personally contacting Facebook staff, and in some cases, sending legal letters (Aspan 2008).

Finally, the ownership interdependency conflicts arise when a user decides to leave her SNS. Should all relational information related to her be deleted? How does that affect the privacy and the integrity of the interdependent users? All of these questions also arise when providers remove user profiles in response to breaches of their Terms of Use.

Privacy Design Heuristics

Distinguishing ownership from circulation rights: Privacy policies in SNS should distinguish between circulation of profile information and the ownership of data. If user data is going to be handled other than to make it available throughout multiple servers and mirrored sites, then the purpose of data use should be clearly stated.

Negotiating user-user interdependency: The interdependent ownership calls for negotiation mechanisms and the establishment of community standards. A simple solution to interdependent ownership would be to adopt the strictest settings that any of the involved users have. An alternative would involve the SNS to inform both parties of the ramifications of that particular interaction e.g. allowing user B to comment on this photo will make that photo available to her friends due to her current feed settings. Similarly, Myspace has a simple and elegant solution to tagging in photos. The users first have to accept photos tagged with them before those tags are made public. This is in stark contrast to Facebook, which allows automatic tagging, all the while allowing the tagged user to remove the tag. None of these basic solutions involve actual negotiations that would allow the users to decide together the visibility and treatment of relational information. That will be part of our future research in this field.

Removal of profiles and user negotiation: Leaving the SNS implies that the user's basic information, profile (and any comments made by others on that profile), uploaded content such as photos and videos (and any comments to those), their contact lists, their presence on other people's contact lists, and all other content be removed. This has an impact on the integrity of the other profiles. An interesting design solution would be to allow users to distinguish between kinds of relational information. Relational information is about sharing. In real life, sharing sometimes means lending something, in others it means giving something away i.e. like a gift. User may therefore be provided with functionality that specifies the conditions of ownership in relational information in a playful manner.

Removal of profiles and provider responsibility: Deletion of the data when a user removes their profile is the responsibility of the providers. Legal frameworks should make providers responsible for the complete deletion of profiles, which will inevitably have an impact on the sharing of the data with third parties. A good example in this direction is the user-friendly Terms of Service (ToS) and Privacy Policy (PP) of MySpace (MySpace TOS 2008 MySpace PP 2008). MySpace states that a user is in sole control of their data, albeit while asserting that the SNS has the right to use that data in some ways. They state that any use of PII (personally Identifiable Information) will only be done after informing users of the purpose, and receiving authorization from them.

Breaches related to Misappropriation

By *misappropriation* we refer to the use of SNS data out of context or for previously undefined purposes. This problem is typically manifested between users and providers, or users and third-parties, and rarely among users. Misappropriation often takes place on the aggregation of all user-interactions on the SNS: *the network information* i.e. the complete social graph, the user profiles and the user interactions. In its extreme case, this includes the aggregation of data from multiple providers.

Data mining and categorization: Results of data mining on network information can reveal additional information about users. Where is the user located in the network, is the user a desired customer; a connector between communities; participating in a community of interest that is of commercial or of other surveillance value? All of these observations are based on aggregate traces and information provided by users. But, it is assumed that this information is beyond users' control and is not related to their privacy.

The unwanted uses of network data that leads to discrimination of individuals based on categorization in population groups are seen as breaches of categorization privacy. The problems attached to surveilling networks and the resulting categorizations has often been ignored by the privacy debates (Nissenbaum 2004) but picked up by those in surveillance studies (Phillips 2004, Graham et al. 2003, Braman 2006)

Facebook actually provides a privacy option which allows users to turn off "social advertising", but nowhere do they state, exactly what part of users' "social data" or graph they observe for this kind of advertisement and what happens if friends in the same social graph have conflicting configurations.

Third-party provider misappropriation and relational information: A recent example of misappropriation concerns Facebook "apps"[3] . Apps require full access to profile information before users can interact with them. Facebook

[3] Apps are third-party applications that use an API provided by facebook to introduce new features and build on existing ones.

advises users to "use […] applications at [their] own risk" and provides apps with all profile information with no possibility for the user to set limitations. Since users have to proactively install an app, and explicitly consent to the use of their profile information, one could argue that this is not a case of misappropriation. However the recent discovery that apps then also gain access to sensitive information about their users' friends catapults this problem.

Facebook Beacon, another important example, misappropriates the mini-feed to indirectly market products to the friends of a user who made a purchase (Hill et al. 2006). This is an example of *appropriation*, "the use of the data subject's identity to serve the aims and interests of another" (Solove 2007).

Uninformed misappropriation: Beacons misappropriation of data was public by virtue of the properties of the application, although the technical implementtion and the complete effect of the feature remains a "trade secret". Recognizing misappropriation is a matter of expertise, if not impossible. It was only through multiple interventions publicized in blogs by experts that it became evident that Beacon uses a combination of cookies and pixels at partner sites that invoke javascript. A deeper analysis showed that Beacon contains further unwanted side-effects like tracking users that are off-line (Bertaeu 2008) and linking users with wrong information (Li 07).

Privacy Design Heuristics

Opening network information to scrutiny: OECD guidelines can be applied also to network information in SNS: Users can be informed on which part of their information has been shared and with whom, and have the right to scrutinize, edit or delete this information. Mechanisms can also be implemented to encourage users to scrutinize aggregate data and resulting categories, make corrections, or delete themselves out of unwanted categories. Information overload and the required expertise may inhibit such engagement. Revealing network information would also reveal information about other users. Even if the network is revealed anonymously, it may be possible to devise attacks and reidentify users (Backstorm et al. 2007). Using stronger anonymization techniques, especially those based on perturbation, would in return raise questions about the authenticity and accountability of data (Braman 2006). Transparency of network information is nevertheless an interesting question for future research.

Engaging the public: Misappropriation, albeit less flashy than the other categories of privacy breaches, is a silent assassin. In reality, only the providers themselves know about their doings with network information. SNS providers rely on that wealth of information for value creation. The more information they have on their users, their users' interactions, social graphs, habits, wishes, and purchases, the more these users are worth to potential partners of that provider. Users by now also know that once their information is 'out there', it is in one way or another public. Nevertheless, as more misappropriation stories hit the news and the users become aware, it will become inevitable to think about privacy design with respect to the use of network information.

Conclusion

There are three main contributions in this paper. Firstly, we consider privacy as a set of practices in negotiating the public and private divide. In that sense we depart from the view of privacy as confidentiality often encountered in computer science. From this perspective we lay the groundwork for dealing with privacy concerns systematically during systems engineering. We focus on the domain of SNS where conflicts and negotiation are central.

Secondly, we propose an analytical framework for characterizing privacy breaches in SNS. The analytical framework is based on characterizations of digital privacy in literature and news on privacy breaches in SNS. It includes an investigation of the properties of prominent breaches in SNS and how they are inter-related.

The categories in our framework are interdependent but they point out different aspects of privacy breaches. For example, if ownership is contested, then it is difficult for a user to determine the visibility of relational information. Misappropriation and indeterminate visibility often result in the breach of separation of identities etc. Nevertheless, the differences are helpful in conceiving the necessary privacy design heuristics. Those privacy design heuristics and discussions on their advantages and disadvantages make up the final contribution of this paper.

Clearly, neither the list of breaches nor the suggested privacy design heuristics are complete. In our text we pointed to important topics that require future research. We expect that as users are better informed about the inner workings of SNS and better articulate their privacy needs, providers will have increasing pressure to engage in privacy design. In which case, this analysis will have to be repeated.

An important issue we will look into next is whether, and why, providers would be willing to offer more privacy features, when the availability of user data is what gives their networks their value. Possible drivers for SNS providers include user retention, avoiding bad publicity which can lead to monetary loss, industry standards,

adhering to potential relevant legislation, or simply ethics (the age of "do no evil").

In order to deal with privacy conflicts more systematically, we will extend a method on multilateral security requirements engineering (Gürses 2006) as well as study agile design methodologies. Our long-term objective is to develop an agile framework for privacy design that would combine the negotiations and conflict resolution strategies mentioned in this paper, as well as agile development methodologies. Such a framework would allow providers and consumers to collaborate on developing and improving privacy aspects of social networks to the benefit of all.

References

Albrechtslund, A. "Online Social Networking as Participatory Surveillance", First Monday, (13:3), 2008.

Aspan M. "How Sticky Is Membership on Facebook? Just Try Breaking Free", New York Times, Published: February 11, 2008.

Backstrom, L., Dwork, C., and Kleinberg, J. "Wherefore art thou r3579x?: Anonymized social networks, hidden patterns, and structural steganography", in Proceedings of the 16th Conference on the WWW, 2007.

Bellotti, V. "Design for Privacy in Multimedia Computing and Communications Environments", In Technology and Privacy: The New Landscape, Agre, P. and Rotenberg, M. (Eds.). MIT Press: Cambridge, 1997.

Berendt, B., Günther, O., and Spiekermann, S. "Privacy in e-commerce: stated preferences vs. actual behavior", Communications of the ACM, Volume 48, Number 4, pp. 101-106, 2005.

Bertaeu, S., "Facebook's Misrepresentation of Beacon's Threat to Privacy: Tracking users who opt out or are not logged in", http://community.ca.com/blogs/securityadvisor/archive/2007/11/29/Facebook-s-misrepresentation-of-Beacon-s-threat-to-privacy-tracking-users-who-opt-out-or-are-not-logged-in.aspx, retrieved March 2008.

Berthold, S., Clauss, S. "Linkability estimation between subjects and message contents using formal concepts," in DIM '07: Proceedings of the 2007 ACM workshop on Digital identity management, 2007, pp. 36-45.

Borcea, K., Donker, H., Franz, E., Liesebach, K., Wahrig, H. "Intra-Application Partitioning of Personal-Data", in Proceedings of the Workshop on Privacy-Enhanced Personalization, 2005.

Boyd, D. "Facebook's 'Privacy Trainwreck': Exposure, Invasion, and Drama", Apophenia Blog. September 8. http://www.danah.org/papers/FacebookAndPrivacy.html, 2006, retrieved March 2008.

Braman, S. "Tactical Memory: The Politics of Openness in the Construction of Memory", First Monday (11:7), 2006.

ENISA Position Paper #1, "Security Issues and Recommendations for Social Networks", Giles Hogben (Ed), European Network and Information Security Agency, 2007.

Facebook Beacon. http://www.Facebook.com/business/?Beacon, retrieved March 2008.

Facebook Beacon, http://www.Facebook.com/business/?Beacon, retrieved December 2007.

Facebook Terms of Use, http://www.Facebook.com/terms.php, retrieved March 2008

Facebook Privacy Policy, http://www.Facebook.com/policy.php, retrieved March 2008.

Graham, S. and Wood, D., "Digitizing surveillance: Categorization, Space, Inequality", Critical Social Policy, (23:2), 2003, pages 227-248

Gross, R., Acquisti, A., and Heinz, H. J. "Information revelation and privacy in online social networks", in Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society, 2005.

Gürses, S., Berendt, B., Santen, T. "Multilateral security requirements analysis for preserving privacy in ubiquitous environments", in Proceedings of the UKDU Workshop Berendt, B., Menasalvas, E. (Eds.), 2006, pp. 51-64.

Gutwirth, S., "Privacy and the Information Age", Rowman and Littlefield:Maryland, 2002.

Hansen, M., Berlich, P., Camenisch, J., Clauss, S., Pfitzmann, A., Waidner, M. "Privacy Enhancing Identity Management", Information Security Technical Report, Volume 9, Issue 1, 2004, pp. 35-44.

Hill, S., Provost, F., Volinsky, C. "Network-Based Marketing: Identifying Likely Adopters via Consumer

Networks", Statistical Science, (21:2), 2006.

Jensen. C. and Potts, C. "Privacy Policies as Decision-Making Tools: A Usability Evaluation of Online Privacy Notices", in Proceedings of CHI, 2004.

Lederer S., Hong, J., Dey, A., Landay, J. "Personal privacy through understanding and action: Five pitfalls for designers", in Personal and Ubiquitous Computing, (8:6), 2004.

Li, C., "Close encounter with facebook beacon." http://blogs.forrester.com/charleneli/2007/11/close-encounter.html, November, 2007, retrieved in July, 2008.

Lipford H. R., Besmer A., and Watson, J., "Understanding Privacy Settings in Facebook with an Audience View," 2008 USENIX Workshop on Usability, Psychology, and Security, 2008.

Mackay W. "Triggers and barriers to customizing software," Proceedings of CHI'91, 1991 ACM Press, pp. 153–160.

Möller, J, "Legal localization of P3P as a requirement for its privacy enhancing effect", taken from: "Informieren oder Aushorchen - Eine Studie von Ernst & Young und Luther Menold zur Einhaltung von rechtlichen Standards bei Web-Auftritten", pp. 20-22, http://www.w3.org/2003/p3p-ws/pp/uld.html, 2003. Retrieved Aug. 2008.

Myspace Terms of Use. http://www.myspace.com/index.cfm?fuseaction=misc.privacy, retrieved March 5, 2008.

Myspace Privacy Policy, http://www.myspace.com/index.cfm?fuseaction=misc.terms, retrieved March 5, 2008.

Nissenbaum, H., "Privacy as Contextual Integrity", Washington Law Review, (79:1), 2004, pp. 119-158.

OECD. "Guidelines on the protection of privacy and transborder flows of personal data", 1980.

Sören Preibusch, Bettina Hoser, Seda Gürses, Bettina Berendt, "Ubiquitous social networks - opportunities and challenges for privacy aware user modeling", in Proceedings of the K-DUUM Workshop, 2007.

Phillips, D. J. "Privacy Policy and PETs", New Media and Society, (6:6)2004, pp. 691-706.

Solove, D. "A Taxonomy of Privacy", University of Pennsylvania Law Review, (54:3), 2006.

StudiVZ, STUDIVERZEICHNIS, http://www.studivz.net, retrieved Sept. 1, 2008.

Rosenblum, D. "What Anyone Can Know: The Privacy Risks of Social Networking Sites," IEEE Security and Privacy, Vol. 5, No. 3, ,2007, pp. 40-49.

Vaidya, J., Clifton, C., Zhu, M. "Privacy Preserving Data Mining", (19) in Advances in Information Security, 2006.

Zuckerberg,M. Facebook Blog. Entry on September 8, 2006, http://blog.Facebook.com/blog.php?post=2208562130, 2008.