TILBURG UNIVERSITY

Tilburg University

Privacy in Social Software

van den Berg, B.; Pötzsch, S.; Leenes, R.E.; Borcea-Pfitzmann, K.; Beato, F.

Published in:
Privacy and identity management for life

Publication date:
2011

Document Version
Peer reviewed version

Link to publication in Tilburg University Research Portal

Citation for published version (APA):
van den Berg, B., Pötzsch, S., Leenes, R. E., Borcea-Pfitzmann, K., & Beato, F. (2011). Privacy in Social Software. In J. Camenish, S. Fischer-Hübner, & K. Rannenberg (Eds.), *Privacy and identity management for life* (pp. 33-60). Springer.

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

Take down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Download date: 06. Nov. 2022

Chapter 2
Privacy in Social Software

Bibi van den Berg, Stefanie Pötzsch, Ronald Leenes, Katrin Borcea-Pfitzmann, and Filipe Beato

Abstract While using social software and interacting with others on the Internet, users share a lot of information about themselves. An important issue for these users is maintaining control over their own personal data and being aware to whom which data is disclosed. In this chapter, we present specific requirements and realised solutions to these problems for two different kinds of social software: social networking sites and web forums.

2.1 Scenarios and Requirements

In recent years, a new generation of the Internet has emerged, also known as 'Web 2.0'. One often quoted definition of Web 2.0 states that this term refers to a "set of economic, social, and technological trends, that collectively form the basis of the next generation of the Internet – a more mature, distinct medium characterised by user participation, openness, and network effects" [MSF09]. Web 2.0 has four fundamental characteristics that set it apart from the first generation of the Internet ('Web 1.0'):

- Internet users have changed from passive consumers of information (searching for information and reading materials provided by others) into *active creators of content* [Tap09, How08, Lea08]. In Web 2.0, users can share their knowledge and information via a wide range of channels. Blogs, YouTube movies, wikis, file-sharing and consumer reviews are examples in case.
- In Web 2.0, social interaction plays a central role. This is why Web 2.0 is also called '*the social web*'.
- In many Web 2.0 environments, sharing and creating content and knowledge is not a solitary enterprise, but quite the reverse: the production and dissemination of information and entertainment services has a highly co-operative character. *Participation* and *co-creation* are key aspects of Web 2.0.

- Web 2.0 also differs from the first generation of the Internet in a technical sense: technology developers now create applications that are *embedded* into the Internet, and are accessible via any browser. Thus, the Internet has become the central platform for users to access different types of software [O'R07]. Moreover, software is offered to users as a service rather than as a product to buy separately.

Since Web 2.0 is a new phenomenon – the term was first coined in 1999 but the massive take-off of this latest generation of the Internet is only a few years old – much is still to be learned with regards to both the benefits and the risks for users, businesses and governments in this new domain. Privacy issues relating to modern technologies have been high on the agenda of both government officials around the world, researchers, and the broader public, and for good measure, since it is obvious that the emergence of Web 2.0 currently generates a wide range of new issues relating to privacy and security.

As said, the success of the social web is based on the active participation of users, and on their willingness to contribute to the creation and improvement of content on the Internet by sharing data and knowledge [SGL06, O'R07]. By using social software, a lot of personal data is disclosed either directly – think of real names and birth dates on social networking sites – or indirectly, for instance through editing specific topics in a wiki, commenting on blog entries or posting statements in a forum [GA05, EGH08]. Furthermore, personal data can be generated by establishing connections with, or disclosing information by, second parties with or without the consent of the respective person. While the possibilities of the social web may enrich people's lives on the one hand, there are also privacy risks involved. Five central privacy issues can be distinguished with respect to information and communication technologies in general, and Web 2.0 applications in particular :

- When sharing data and knowledge in social software, users lack an overview of who has access to this information – they cannot adequately judge the size and makeup of their *audience* [PD03, Tuf08].
- Information and communication technologies enable anyone to collect, copy, link and distribute the (personal) data of others, thus allowing for the creation of extensive profiles of individual persons. Information may also easily be copied outside the original domain, thus making it even harder for users to know who has access to their information [Hou09].
- Information and communication technologies allow storage of data for a nearly indefinite time period, thus making it impossible to erase or forget this information [MS09].
- Participatory information and communication technologies such as social software enable anyone to publish another individual's personal data, which may have serious consequences for the other's reputation [Sol07].
- Individuals' lack of privacy-awareness when using social software may lead to information leaks and leaving unintended and/or unobserved virtual traces.

To find out which guises privacy issues take in the new generation of the Internet, much research has been conducted with regards to privacy in social software in

recent years, and especially in social network sites. One of the central points with regards to information sharing and privacy in social network sites is aptly summarised by Acquisti and Gross. They write: '*... one cannot help but marvel at the nature, amount, and detail of the personal information some users provide, and ponder how informed this information sharing is*" [AG06]. Individuals use social networking sites for two main goals: (1) to *present themselves* to others in a virtual domain, and (2) to engage in, manage and strengthen *relationships*. Both of these involve several privacy risks as Scenario 1 (Sect. 2.1.1) will show.

A much less researched, yet highly relevant domain for privacy issues in Web 2.0 is that of *collaborative workspaces* and *forums*. Users primarily use these environments to create and share *content*, rather than to present themselves and build relationships. However, while participating in these workspaces, they may inadvertently disclose information about themselves that can undermine their privacy as we will show in Scenario 2 (Sect. 2.1.2)

2.1.1 Scenario 1: A Social Network Site

Natalie Blanchard is a member of the biggest social network site in the world: Facebook. She has a profile page, detailing information about her person, her hobbies and preferences. Through Facebook, she stays in touch with a number of contacts, both close friends and acquaintances. Natalie knows that users must be careful about sharing their personal information in social network sites because of privacy issues, so she has changed the privacy settings of her profile to 'visible to friends only'. This means that only the members of her contact list can see the information she posts there. Natalie regularly posts pictures to her profile page, for instance of a trip she took to the beach, or of parties that she attended with friends.

One day in 2009, Natalie receives a message from her insurance company, telling her that they will terminate the monthly payments she has received for the last year and a half because she is on sick leave – she had been diagnosed with depression in 2007. Inquiries reveal that the insurance company had used Natalie's Facebook page to investigate the validity of her ongoing claim for monthly payments, and had used the pictures of her, happy at the beach or laughing with friends, to conclude that Natalie was unjustly receiving these payments. It remains unclear how the insurance company gained access to the profile page, if Natalie had indeed shielded it from everyone who was not on her contact list.

This scenario reveals that unintended audiences may sometimes access personal information in social network sites, and thus receive information that was not posted with them in mind. Based on what they see there, these unintended audiences may draw conclusions, and even undertake actions, that may harm the individual involved. Sharing information without having a clear grasp of the makeup and the extent of the audience, as is the case in social network sites, may thus have serious repercussions for users.

2.1.2 Scenario 2: A Forum

Hannes Obermaier works as a salesman in a big electronic company and his favourite hobbies are his family and gambling. He plays poker well and has even won a small amount of money in an online poker room. Unfortunately, Hannes forgot to indicate this earning in his tax declaration and therefore he has a problem with his tax office. Seeking for advice in this situation, Hannes finds a forum on the Internet where all kinds of questions related to online gambling are discussed. Hannes hopes to find help and creates a forum post in which he describes his problem. After a few minutes, another forum user has written the first reply to Hannes post saying that he has experienced similar problems and asking about some more details of Hannes' case. During the next few days, Hannes spends a lot of time in the forum. He has gotten to know a lot of the other users and with three of them he really feels like they have been friends for ages. Of course, Hannes has told them not only about his problem with the tax office, but he also shared some funny stories from his everyday life and posted a link to a cute picture of his son from his personal homepage.

One day, a new user who calls herself WendyXY appears in the forum and starts to post insults and allegation about Hannes, not just once but repeatedly. The scary thing is that she seems to know Hannes' name, where he lives and for which company he works. Later, Hannes realises that WendyXY may have found his personal homepage since he had posted the link to the picture of his son. His personal homepage contained Hannes' real name and his residence. Knowing this information, it must have been easy for WendyXY to infer where he works since Hannes has briefly mentioned his job in earlier posts and there is only one big electronics company in his local area.

The story becomes even worse when one of Hannes' major clients finds all the allegations about him on the Internet and cancels an important contract for fear of a negative image.

This scenario may seem artificial, yet a similar case was reported by the German newspaper *Zeit* in 2009 [Bur09]. It illustrates that the sharing of personal data with possibly millions of unknown people on the Internet is a critical point from a privacy perspective and may result in negative consequences, such as bullying, cyberstalking or harassment. However, note that the sharing of personal data with an *intended* audience – in the scenario for example talking about the tax office problem with other online gamblers – is the main reason to use forums or similar collaborative workspaces.

2.1.3 General Requirements

In both scenarios, users' privacy could be protected through the use of *audience segregation* [Gof59], i.e., the compartmentalisation of different social circles, so that individuals can show different sides of themselves in each of these circles, without

running the risk that information from other domains of their lives undermines the current self-presentation. In technical terms, one could argue that *selective access control* based on access control rules specified by the user is one feasible means to realise audience segregation. Due to the differences between social network sites and collaborative workspaces such as forums, different requirements emerge with respect to the way selective access control is implemented.

In social network sites, users are directly connected to other members, whom they know (at least to some degree). This means that generating selective access control in social network sites refers mainly to the fact that users must be able to make information visible to specific contacts (yet not others). This can be realised by enabling users to create multiple profile pages in a social network site, and to cluster contacts in subgroups so that information disclosure becomes more targeted and precise. We will outline these principles in more detail in Section 2.2.

In collaborative workspaces, such as forums, users are generally not connected to others, and they may not know any of the other members of the workspace. In these collaborative workspaces, privacy-enhancing selective access control can be realised based on general properties of the intended audience, without having to "know" each user in particular as we will show in Section 2.3.

2.2 Two Prototypes for Privacy-Enhanced Social Networking

2.2.1 Introduction

Social network sites are one of the most flourishing branches of the social web. In 2008, Facebook, the biggest social network site of all, had over 100 million users [Gri08]. In October 2010, the same social network had grown to more than 500 million *active* users worldwide – 'active users' are defined by this network as individuals who access the network every single day on average [Fac]. Users who have accessed the network only once, or use it less frequently, are not even counted in this number anymore, which means the total number of users must far exceed the phenomenal 500 million that Facebook focuses on. And Facebook is not the only social network site. There are literally thousands of different social network sites on the Internet. Roughly 200 of the biggest ones are listed on a Wikipedia page, which reveals that, on average, these sites gather hundreds of thousands of unique users and many go up to millions [Wik]. In March of 2009, Nielsen Online, an information and media company that analyses online audiences and their behaviours, published a report that shows that the use of social network sites and blogs is now "*the fourth most popular online activity, ahead of personal email*" [BM09].

While social network sites have become immensely popular worldwide, at the same time stories of privacy breaches on these sites are a regular topic in popular press. There is an abundance of examples of social network site users who have not managed to find a job [Man10], lost a job [Yok07], had to paid extra income

taxes [Ind08], or lost their right to health insurance payments [New09] because of information they had revealed through social network sites. Many empirical studies have been conducted in the previous years to reveal (a) how users perceive privacy on social network sites, and (b) how (mis)perceptions of privacy in relation to users' own behaviour can lead to privacy violations in these domains.

2.2.2 Privacy Issues in Social Network Sites

One of the most fascinating aspects of users' self-presentation in social network sites is the fact that they put such detailed and personal information about themselves in their profiles [Tuf08, YQH09]. In an article on the privacy risks for individuals using Facebook, Grimmelmann points out:

> "Facebook knows an immense amount about its users. A fully filled-out Facebook profile contains about 40 pieces of recognizably personal information, including name; birthday; political and religious views; online and offline contact information; sex, sexual preference and relationship status; favorite books, movies, and so on; educational and employment history; and, of course, picture. [...] Facebook then offers multiple tools for users to search out and add potential contacts. [...] By the time you're done, Facebook has a reasonably comprehensive snapshot both of who you are and of who you know" [Gri08].

What's more, "[a]*ll of this personal information, plus a user's activities, are stored in essentially a huge database, where it can be analyzed, manipulated, systematized, formalized, classified and aggregated*" [RG10]. When viewed from a European legal perspective on privacy, almost all of this information (details on sexuality, religion, politics etc.) is considered 'sensitive' and hence requires "*particular conditions and safeguards* [...] *when processed*" [EB09].

After an extensive analysis of articles on privacy issues in social network sites, we conclude that such privacy problems may arise in five categories with respect to users [1]. In some respects, these categories overlap with themes we have discussed in the introduction to this chapter, when discussing privacy issues in online worlds in general. However, on social network sites, these themes come together in a particular way. We will discuss each of them in turn.

2.2.2.1 Who is the Audience?

In social network sites, "*audiences are no longer circumscribed by physical space; they can be large, unknown and distant*" [PD03]. It is difficult for users to know who exactly sees their information. The audience, to phrase it differently, is not transparent. On almost all social network sites, users can protect the visibility of the

[1] Privacy issues caused by third party businesses and by the providers of the social network site themselves are another serious threat. These types of privacy issues were discussed in Deliverable 1.2.5 of the PrimeLife project. We have chosen to focus on privacy issues amongst users here only, since those are the issues that we attempted to solve primarily in building our Clique demonstrator.

information they share through so-called 'privacy-settings'. Generally, these enable them to set the visibility of their profile to one of four options: 'visible to everyone' (i.e., all users of the social network site), 'visible to friends' (i.e., visible to all the contacts listed in their contact list), 'visible to friends-of-friends' (i.e., visible to all the contacts in their contact list *and* to the contacts in the lists of all of these individuals), or 'visible to no one'. As it turns out, many users – aware of the possible privacy risks in social network sites because of all the media attention for these risks – set their profile visibility to 'friends-of-friends'. This sounds restricted enough to be 'safe' from prying eyes, yet open enough to find new contacts, and to stay in touch with a larger social circle than one's own strict group. Moreover, many users understand the phrase 'friends-of-friends' to refer to, roughly, the group of people one would encounter when going to a friend's birthday party. However, this is a grave misperception. On average, users in Facebook have 130 friends in their contact list. Aside from the fact that this so-called collection of 'friends' must consist of more than real friends, simple multiplication reveals what setting visibility to 130 friends-of friends means: when 130 friends of 130 friends are allowed to view an individual's profile information, this means that almost 17.000 people have access to that information – a very large group of people indeed. A non-transparent audience may easily lead to privacy problems, because users may unintentionally make information available to the wrong people, or to an unforeseen amount of people.

2.2.2.2 Context Collision or Lack of Audience Segregation

Another key element of the fact that users do not have complete control over, or full awareness of, who sees the information they post in a social network site is what Raynes-Goldie has called '*context collision*' [RG10]. When she conducted research on the disclosure of information in Facebook, participants told her they were very frustrated by the fact that in this social network site (and in many others) all contacts are clustered into a single group, without distinction between the myriad of social relations and the various levels of intimacy one has with different contacts in real life. This leads to a

> "... flattened Friend hierarchy, where by default, everyone is given access to the same personal information. As a result a user's teetotaller boss sees the same things as their best friend, the party animal. This can cause problems when trying to decide what to share about yourself, or trying to manage how people from different life contexts might perceive [information]. What is appropriate for a user's friends to see may not be appropriate for their employer" [RG10].

Context collision entails that individuals are no longer able to meet the various behavioural requirements of the many different social settings in which they normally operate, since one and the same audience sees all of their behaviours. Whereas individuals can keep various social settings separate in real life, for instance because these social settings are connected to distinct physical places (work, home, public space, etc.), in virtual worlds such as social network sites "*intersections of multi-*

ple physical and virtual spaces, each with potentially differing behavioral requirements" may arise [PD03].

When phrased in the vocabulary of the twentieth century sociologist Erving Goffman, whose perspective on identity and self-presentation was influential in our analysis of social interaction in social network sites, what users in social network sites lack is a means for '*audience segregation*' [Gof59]. Goffman emphasises the fact that human beings need such a segregation between audiences, since they perform different, possibly conflicting, *roles* throughout their everyday lives, and the impressions they aim to foster in each of these roles must not be contaminated by information from other performances. With segregated audiences for the presentation of specific roles, performers can 'maintain face' before each of these audiences. In social network sites, the clustering of social relations into a single list of contacts defeats this important feature of social life in the everyday life. Context collision and context collapse in social network sites are caused by users' lack of means for audience segregation. When the audience consists of individuals from many different contexts of an individuals' life, brought together in one group to view all of the individuals' behaviours in a social network site, then it is clear that this diminishes the individuals' chances of protecting and maintaining his various 'faces'. Thus, it may lead to minor or more serious privacy risks.

2.2.2.3 Persistence of Information

As we have seen above, the persistance of information in online worlds forms a threat to users' privacy. As Palen and Dourish say, "*the recordability and subsequent persistence of information, especially that which was once ephemeral, means that audiences can exist not only in the present, but in the future as well—*" [PD03]. This also applies to social network sites. Information posted on one's social network site profile may be accessed by (known and unknown) individuals in years to come. Moreover, since information can be copied, saved and stored easily and indefinitely, information placed on one's profile on a social network site at any particular moment may come back to haunt the individual years down the line. This means that the audience is not only unlimited in terms of its size and makeup (in contrast to audiences in the physical world), but also in terms of temporality.

2.2.2.4 Peer Surveillance, Snooping and Gossiping

Users of social network sites can use the search functionality of these sites to find others' profile pages, and may navigate through the profiles of others using the contact lists of individuals they have befriended. Depending on the visibility settings of each profile page, quite a significant amount of information about others may thus be gleaned. Navigating the profile pages of other users in this way possibly invites socially undesirable or even harmful behaviours. For one, gossiping and snooping are facilitated by it. As Hough points out,

> "[t]oday, technology enables us to gossip or otherwise exchange information with millions of people instantaneously. [...] Social network sites such as Facebook, reunion.com, and classmates.com enable the resurrection of those embarrassing youthful escapades and awkward photographs we all wish would stay buried. Often, the postings are captured on camera-enabled cellphones without the knowledge of the subjects and uploaded without their consent, leading to instant notoriety, long-lasting embarrassment, and a loss of reserve that may never be recaptured" [Hou09].

Other researchers have pointed out that social network sites are breeding grounds for surveillance between peers. Adam Joinson writes that

> "social networking sites like Facebook may [...] serve a surveillance function, allowing users to 'track the actions, beliefs and interests of the larger groups to which they belong' [...]. The surveillance and 'social search' functions of Facebook may, in part, explain why so many Facebook users leave their privacy settings relatively open [...]. [Social network sites offer users a] . . . unique affordance [...] [to] view other people's social networks and friends [...]. This ability to find out more about one's acquaintances through their social networks forms another important surveillance function"' [Joi08].

Peer surveillance, snooping and nosing around may all lead to privacy issues for the parties subjected to them.

2.2.2.5 Who Controls a User's Information?

On social network sites, users can create a user profile on which they can present themselves. This profile page is the starting point for setting up connections with other users within the same environment. On the profile page, users can choose what information to share about themselves and as we've explained above – to some extent – who can view this information (i.e., everyone, friends only etc.). Therefore, in theory at least, users have some control over the image they create of themselves on their profile page. As research has shown, young people especially perceive themselves as having a considerable degree of control over their disclosure of personal information online, and it turns out that they share such information in full awareness of the associated risks, because they have a high degree of confidence in their ability to manage potentially negative outcomes [BK09].

However, the control that users have over their own profile page and personal information in social network sites only goes so far. Other users can add or change information in a user's personal profile, put pictures or information about him or her on their own or other people's profiles, and tag pictures to reveal the identities of those portrayed in them. This can have serious consequences: placing a picture of another person online affects the image of that person to the audience viewing it, and hence may have an effect on the (current and future) self-presentations and impression management of that individual.

2.2.3 Clique: An Overview

In our research, we have developed two demonstrators that may contribute to solving some of the privacy issues in social network sites that we have discussed above. The first demonstrator is a privacy-enhanced social network site called '*Clique*', in which we have turned theoretical notions on audience segregation and context collision into a real-world online practice. The key solutions implemented in Clique are:

- providing users with the option to create their own 'collections' in which social contacts can be clustered;
- providing users with the option to create multiple 'faces' to mimic the practice of audience segregation in real life;
- providing users with fine-grained options to define the accessibility of their postings and content in social network sites, thus mimicking the rich and varied texture of relationships in real life.

Clique was built using Elgg Open Source software for developing a social network site.[2] The key ideas developed in Clique are:

- mimicking 'audience segregation' in a social network by (1) providing users with the option to create their own 'collections' in which social contacts can be clustered, and (2) providing them with the possibility to create multiple 'faces' to compartmentalise their online social visibility;
- providing users with fine-grained options to define the accessibility of their postings and personal information in Clique.

2.2.3.1 Audience Segregation in Clique

The first principle we realised in Clique to enhance users' ability to protect their privacy and to increase their options for adequate and realistic self-presentation was a translation of Goffman's notion of 'audience segregation'. This is implemented through two mechanisms:

- Users can divide their list of contacts into 'collections', clusters of contacts that are socially meaningful, relevant and efficient for them. Each cluster contains one or more contacts; contacts may be listed in as many different collections as the users likes;
- Users can create multiple profile pages for their account. We call these pages 'faces'. On each profile page, users can show different 'sides' of themselves, thereby mimicking audience segregation through physical distantiation (e.g., showing different sides of oneself at home than at work) in real life.[3]

[2] See http://www.elgg.com

[3] Note that Clique uses a separate social graph for each face to ensure that audiences are indeed kept separate. The social graph collects all of the contacts a user has in relation to this specific

As we have explained above, on many social network sites, all contacts in a user's network are lumped together into one category. No distinction is made between the different social spheres to which individuals belong in their everyday lives. This means that all contacts are exposed to the same information shared by the individual, regardless of how close they are to that individual. This issue has been solved in Clique through the use of 'collections'. By allowing users to create 'collections' within their network of contacts, they can cluster social relations according to their own preferences, and thereby mimic the actual practice of building and maintaining separate social spheres in real life. We have gone to great lengths to ensure that users themselves are in control of the creation and labeling of collections. After all, they themselves know best what the fabric of their own social lives consists of and how it could be divided into relevant and meaningful categories. In Clique, users can choose (1) how many collections they wish to make (i.e., how granulated they want their audience control to be), and (2) which labels to use for each collection. However, to enhance user-friendliness we also provide them with a set of predefined collections, for instance 'family', 'colleagues', and 'acquaintances'.

Below are some screenshots that show the way in which the creation and management of collections is implemented in Clique. Figure 2.1 shows the way in which users can add a new collection to their profile page. They begin by typing in a name for the collection, in this case 'My favourite colleagues'. Then individual contacts from the user's contact list -' that is, individuals that he or she has befriended beforehand -' can be added to the collection by clicking through the alphabet and selecting those individuals the user wants to include in this collection. The letters of the alphabet are bold if there is a contact whose user name starts with that letter, and grey if not. After selecting one or more contacts to add to the collection, the user can click 'save' and the collection is added to his profile. Figure 2.2 shows an overview of the collections this user has made and outlines how many contacts are in each collection.

The second way of realising audience segregation revolves around the idea of creating 'faces', so that users can show different 'sides' of themselves to different audiences through the use of multiple profile pages. On most social network sites, users are allowed to create only one profile per person, and hence can create only one context in which all of their information is gathered. However, in real life, individuals move from one context to the next throughout their everyday life – they go to work, visit friends, or spend time at home with their families. To solve the risk of 'context collision' many users currently maintain different profile pages on different social network sites. For instance, they have a work-related page in LinkedIn and a page for family and friends in Facebook. This is a time-consuming and cumbersome solution, since users have to log onto different platforms to manage their profiles and keep track of contacts and their activities in each domain.

To solve this issue, we enable users to create multiple'faces' in Clique to mimic the various social contexts in which they participate in real life (for instance, a work face, a private face, a face for the tennis club etc.). When a user accesses his profile

profile page, and designates the relationships between them. Collections are a means of assigning access rights to each of the nodes (i.e., contacts) in the social graph.

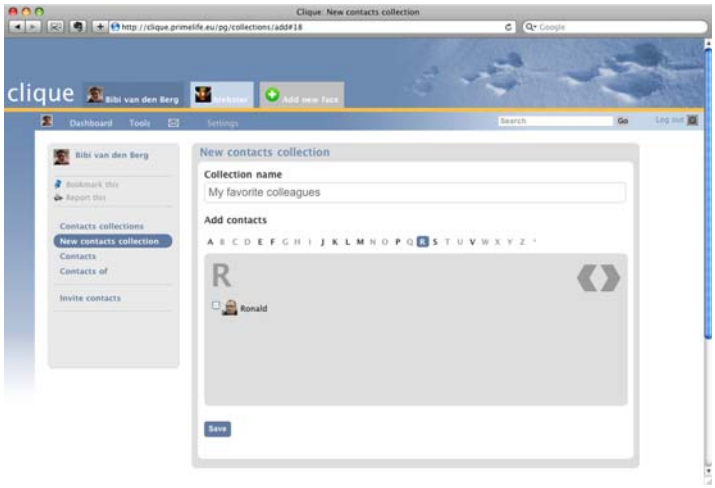


Fig. 2.1: Creating a new collection in Clique.

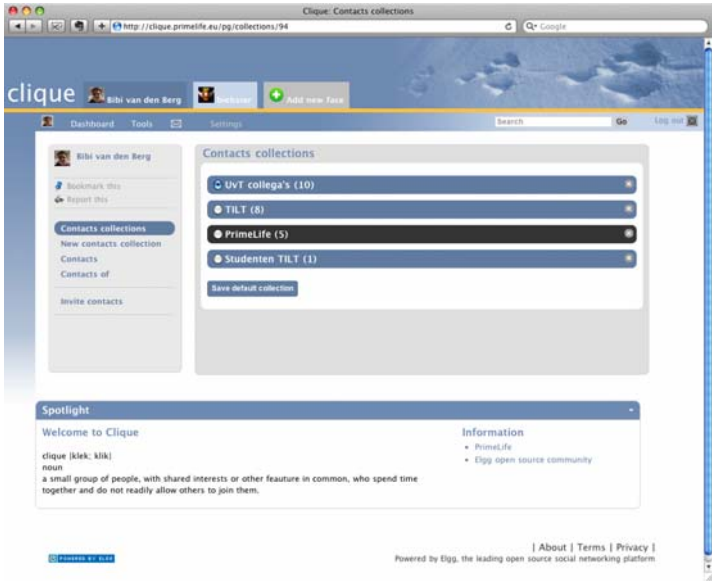


Fig. 2.2: Overview of a user's collections.

in Clique, his various faces are visualised with separate tabs. By clicking on the tabs the users can access the page attached to that face. Figure 2.3 shows a screenshot of the author's faces in Clique. New faces can be added by clicking on the tab at the far right, which reads '+ Add a new face'. As the figure shows, existing faces can be enabled, temporarily disabled or removed entirely. Each of these faces has its

own list of contacts and its own list of collections. Using tabs to distinguish between different faces is a visually appealing and easy way for the individual to manage his or her own profile and the various faces contained therein. Information added to one of the tabs is invisible in all other tabs, and hence it is easy for the user to manage who sees what.

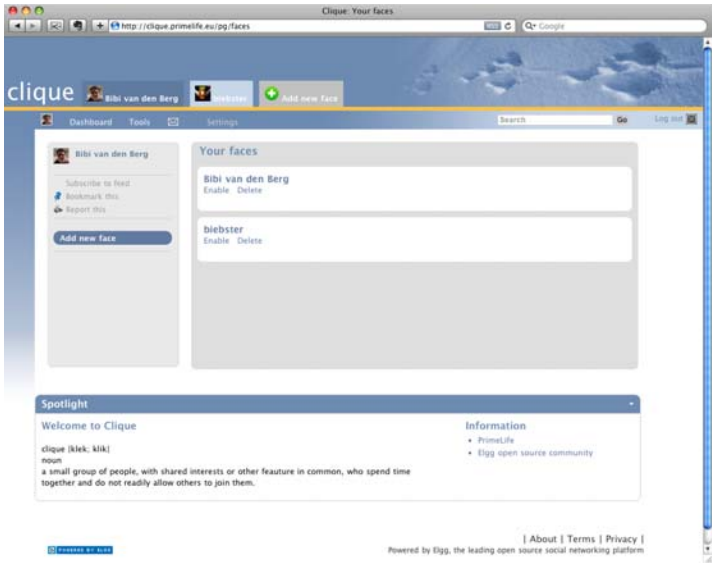


Fig. 2.3: 'Faces' in Clique.

2.2.3.2 Control Over the Visibility of Individual Items of Information in Clique

To further strengthen users' capacity to control who sees which information in Clique, we've added two more features. First, each time a user posts an item of information (pictures, blog entries, messages), the system asks the user (1) in which 'face' he wants to make it available, and (2) to which collections and/or individual users. Second, when disclosing personal information on their profile page, users are also asked, with each separate item of information (i.e., a telephone number, place of residence etc.) to make these choices. These measures further prevent information from spilling over from one context to the next or leaking to unintended audiences. While this feature is demanding on the part of users – it requires them to go through one extra step each time they want to share information with others in Clique –, it is explicitly designed to raise user awareness with respect to audiences and the disclosure of personal information. Moreover, we have designed the interface in a

user-friendly way, so that users can go through this process quite quickly[4] and in an intuitive way. Figure 2.4 shows the screen for setting visibility rights in Clique.

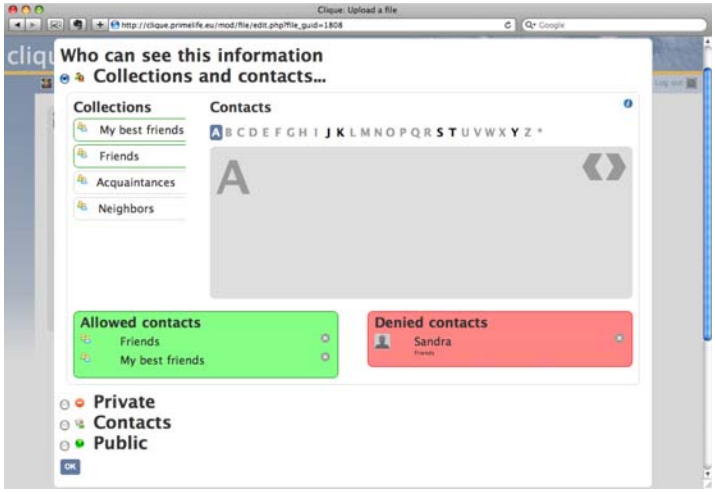


Fig. 2.4: Setting visibility rights to information items in Clique.

2.2.4 Scramble!: An Overview

Another demonstrator we have developed in the PrimeLife project to solve some of the issues surrounding privacy and security in self-presentation on social network sites (and also in other Web 2.0 environments), was an encryption tool called Scramble!. In previous years, several researchers have pointed to the need for access control through encryption in social network sites, like Facebook, MySpace or Twitter. Some of their ideas have been turned into tools such as Lockr[5] and FlyByNight [LB08]. However, these tools all have shortcomings.

For instance, Lockr uses trusted third-party storage for the hidden information, which means that the user does not have full control over his own data, but rather has to place trust in a (commercial) third-party to guarantee a safer use of social network sites. The other tool, FlyByNight, only works on Facebook, and relies on the servers of the social network itself for encryption key management. The decryption algorithm is implemented in JavaScript and retrieved from Facebook. Consequently,

[4] If a user decides to display the information to his 'default' collection, it is only one extra mouse click. If the user decides to share it with other collections and/or individuals, this still should not take more than a few seconds to accomplish.

[5] See http://www.lockr.org/

while FlyByNight is browser-independent and portable, its biggest disadvantage is that it is not secure against active attacks by the social network provider, Facebook. Both of these tools thus contain serious privacy risks.

Scramble! – the tool we built – provides a solution for the attacker model limitations of Lockr and FlyByNight. It relies primarily on the user side and has no dependencies on any specific social network site, as in the case of FlyByNight. Moreover, it does not use a third-party to store information, as is the case in the Lockr project. Also, what our access control mechanism enables, and what all other existing ones lack, is *selective access control*. We will explain what this means below. Scramble! has the following key goals:

- it enables users on social network sites to formulate which individuals have access to the content and personal information they place in, or attach to, their profile;
- all of the information (both content and personal data) that users place online is encrypted and will only be visible to those contacts and/or collections that have the appropriate access rights. Individuals and collections with no access rights, cannot see the information, and nor can the social network site's provider;
- to aim for ease-of-use in order to strike the difficult balance between usability and privacy for general users.

2.2.4.1 Selective Access Control in Scramble!

With Scramble!, we have aimed to use cryptographic techniques to enforce access control. In this prototype application, we use an OpenPGP[6] standard [rfc07] to keep social network users' data confidential. One nice feature of OpenPGP is that it supports encrypting to multiple recipients using hybrid encryption, by encrypting the content with a random secret, and the secret with all the public keys of the set of users. We assume that each user holds a public and a secret OpenPGP key pair.

For key distribution, we assume that users exchange their public keys when a friendship connection is established using an authenticated offline channel. Users can also make the public key available using the provider or any key server and distribute the fingerprint by the offline channel. In this way, users can verify the authenticity of the public key. Since Scramble! makes use of OpenPGP standard, it can build on the OpenPGP key management infrastructure, retrieving the key from an online key server by name or e-mail mapping.

As an example of the flow, let Alice and Bob be two users on a social network site. Bob accepts Alice as his friend. He then adds Alice's public key to his key ring, thereby including Alice in a circle of trust. Then, Bob can post encrypted messages that can only be accessed by a selective audience chosen from the Bob's circle of trust, which now includes Alice.

[6] OpenPGP is one of the world's most widely used encryption standards. For more information, see http://www.openpgp.org/

To realise selective access control on social network sites based on these principles, we have built a Firefox extension with several features. First, there is the fact that access control is generated through the use of an *encryption protocol* (as said, based on OpenPGP), which enables users to trust that their content and personal information is invisible to anyone who does not have the right access key. Note that this includes not only other members of the social network site, but also the social network site provider. Second, the user himself can *define the access rights* handed out to various members of his own social circle, either to individuals or to collections, or to both. The picture below shows two of the windows in which users can define access rights for particular items of content and for personal information.

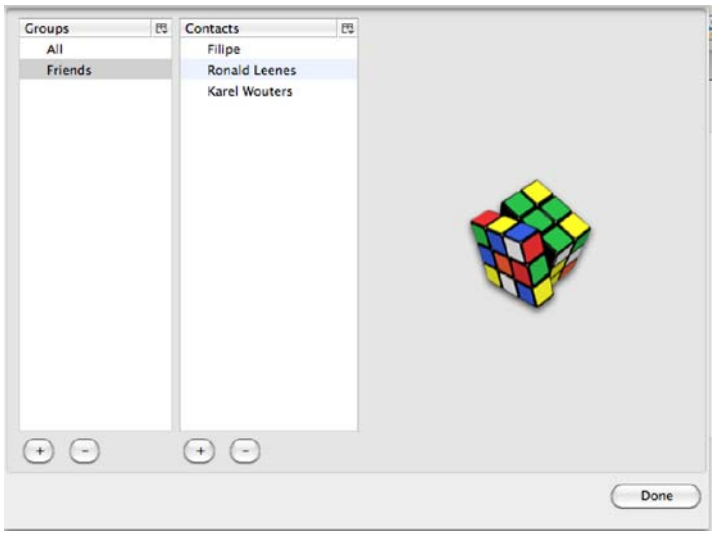


Fig. 2.5: The Scramble! address book, from which selective access rights can be managed.

Since Scramble! is a Firefox extension, it is not linked to a specific social network site, such as Facebook or MySpace, but works across platforms. We have done extensive testing with it in Facebook and MySpace, and also in our own social network site Clique. When a user has the plugin installed and switched on, each time he or she accesses or receives information posted by others, a check is run with regards to whether or not he or she has the proper access rights to read the information. If so, then the content is automatically decrypted and transparently displayed as normal text. Otherwise, if the user has the plugin installed and switched on, but does *not* have access rights to the information, the information is concealed or instead replaced by gobbledygook. Figure 2.6 shows what this looks like in Facebook.

Those who have not *installed* the plugin have no access to the information at all and instead see a so-called 'tiny URL' on their screen, a hyperlink referring to

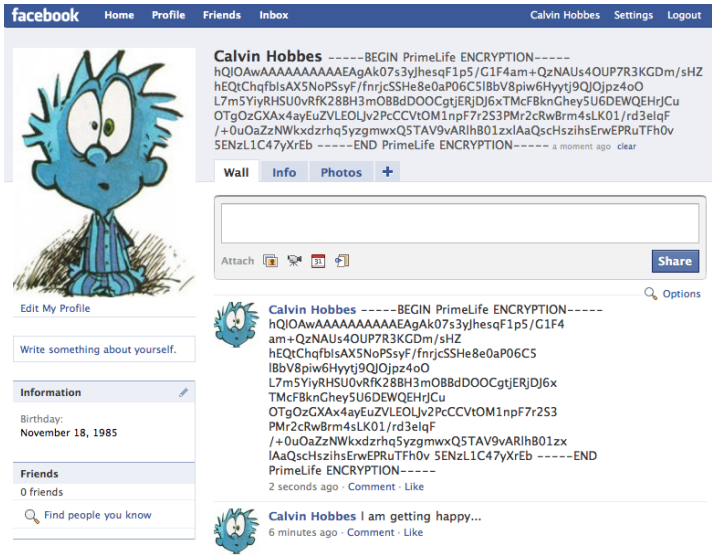


Fig. 2.6: Scramble! is switched on but the user does not have access rights.

an address where the encrypted text is stored instead of the decrypted information placed in the profile by the user. Figure 2.7 shows what this looks like in an earlier version of Clique.

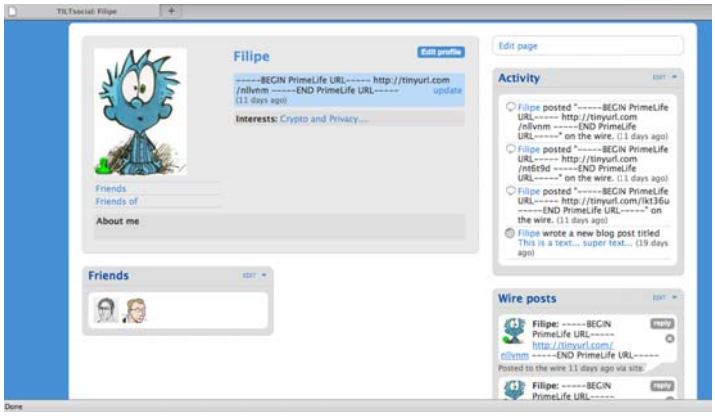


Fig. 2.7: Scramble! is not installed: access is denied and the ‘tiny URL’ is displayed.

2.2.4.2 Scramble! and Web 2.0

Since this encryption tool is built as a browser extension, it isn't merely independent of the various social network sites, but could also be used in other kinds of Web 2.0 environments, such as blogs, collaborative workspaces such as wikis, and forums. It could be used in any environment in which individuals fill in fields through which they exchange information. Using it is very simple. After installing the plug-in a user can select any kind of text in fill-in fields on Internet pages and simply choose 'Scramble!', after which the content will only be readable for those who have the right access key. Moreover, because the extension is integrated into the browser the encrypted content will be decrypted automatically for all authorised users, without their intervention. The exchange of keys runs in the background and requires no particular skills from the owner of the information, nor from those gaining access to it. Our extension is simple and aims at striking the difficult balance between usability and privacy for general users.

2.3 Privacy-Enhancing Selective Access Control for Forums

2.3.1 Objectives

User-generated content in forums may contain personal data in the sense of personal information, personal ideas, thoughts and personal feelings. In contrast to explicit profiles where, e. g., the date of birth is a specified data item saying "12 June 1979", the same personal data can be stated in a forum post which is tagged with the date of writing and says "I got two concert tickets at my 30th birthday yesterday!". In the latter case, it may be not that immediately obvious to the user that she has disclosed her date of birth on the Internet.

The disclosure of personal data in forums and other social software is critical from a privacy perspective, however from a social perspective, the disclosure is necessary since the exchange of information, both personal and non-personal, is the key feature of the application and the primary reason for people to use it. Hence, it is not our objective to prevent disclosure of personal data in forums. We rather want people to be aware of privacy and to enable them to more selectively specify to whom they disclose their data. Access control settings of currently available forums are once specified by the provider and cannot be changed by the particular user. Thus, the user can only decide to disclose information to the groups specified by the providers – in the worst case, this means disclosing to the public – or not to disclose anything at all. Since the first option is not preferable from privacy perspective and the second option is not preferable from social perspective, our objective is to develop a user-centred selective access control system for forums. Forum users should be able to protect their privacy through safeguarding their contextual integrity: data that is disclosed before an intended audience, should not spill over into other contexts and

hence possibly have damaging consequences. That is, a user who wants to share her happiness about her birthday present with some other users (e. g. other people going to the same concert) should be able to specify appropriate access control rules to her post in the forum. Besides the implementation of purely technical means, we further emphasise that it is necessary to sensitise users with respect to privacy in order to get a comprehensive solution. Therefore, we aim at raising awareness of the issue in users as another central goal in the direction of privacy-enhancing selective access control.

2.3.2 Introducing phpBB Forum Software and PRIME Framework

To demonstrate how an existing application can be extended with privacy-enhancing selective access control, we have chosen to build an extension for the popular forum software phpBB [php]. Thereby the main principles of the original system should be preserved. As in other forums, in phpBB, content is always structured in a specific way to make it easily accessible, easy to use, and searchable. In the following, we briefly explain the content structures of phpBB platform, which are illustrated in Figure 2.8.

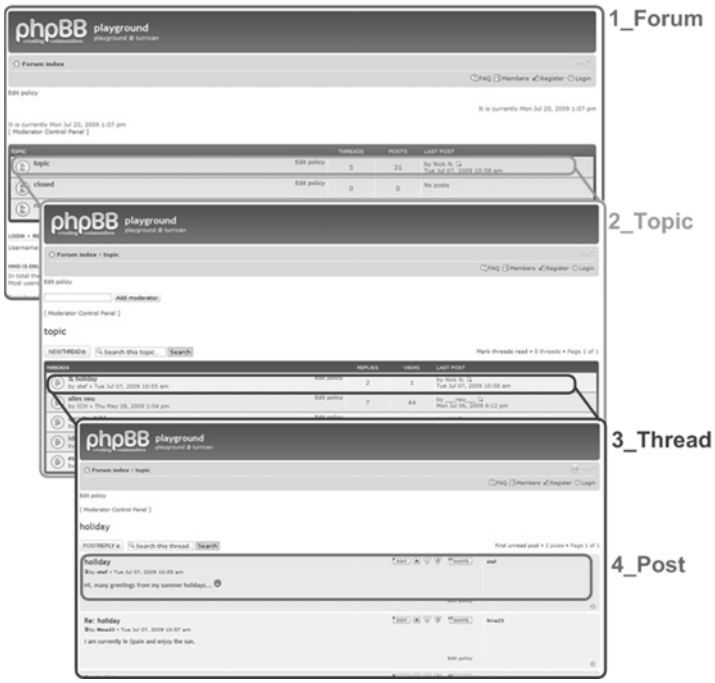


Fig. 2.8: Overview of the hierarchy of a phpBB forum

The top level resource is the forum itself, which is assigned a title and presented to the user when she first enters the platform. An administrator is responsible for managing all general issues of this forum. The forum is subdivided into topics that each address a different subject matter for discussion. For each topic, moderators are responsible for assuring compliance of the content with ethical quality and forum rules. Thus, they have the possibility to change subjects or content of posts, to lock or even to delete posts. Individual discussions focusing on particular aims are called threads. These are created with the submission of a starting post to which users can reply by submitting replying post.

PhpBB software is available with so-called "copyleft license" and is developed and supported by an open source community. This means, original phpBB source code is available to the public and fairly well documented. With respect to the technical realisation of our selective access control extension, we rely on privacy-enhancing mechanisms that were previously developed in the European project PRIME [PRI]. More precisely, we used *credentials* and *access control policies* from the PRIME framework.

2.3.3 Extending phpBB with Selective Access Control

The most common approaches to access control include the access control *list model*, the *role-based* and the *group-based* access control approaches. All three require a central instance that defines lists, roles, or groups based on user names, i.e., identifiers of user accounts (cf. [PBP10]). However, social and collaborative interaction in forums does not necessarily require an association of users by their names. Therefore, privacy-enhancing selective access control in forums requires mechanisms that are not based on the knowledge and existence of names or other particular identity information. Furthermore, it is important that users themselves can decide what they deem to be sensitive or intimate information, rather than what is evaluated as such by lawyers, computer specialists or other third parties [Ada99]. This is why we argue that users themselves need to be given control over the audience to whom they disclose data, and hence access control rules need to be set by the user, being the owner of a resource (e. g. a post), instead of by an administrative party. This implies that access control rules should be possible to specify not only for the whole forum or for topics, but also for threads and particular posts. We need to consider that forum platforms typically provide the roles "adminstrator" for addressing technical issues and "moderator" for content-related moderation of topics. Our approach should allow for keeping both roles. Hence, we can list the following specific requirements for privacy-enhancing selective access control in a forum whereby these are generalisable to further kinds of social software:

- Other persons, who should or should not be able to access the personal data are not necessarily known by the user.
- These other persons also have an interest to protect their privacy.

- No administrative party, but each user should be able to define and modify access rules to her contributions, i.e., personal information, expression of personal thoughts and feelings.
- User-controlled and privacy-respecting access control can be applied to different levels of content granularity (e. g. forum, topic, thread, post).
- An administrator of the forum should be able to address technical issues of the platform, but should not necessarily have access to content data.
- Moderators should be able to moderate particular topics.
- The owner of a resource is always able to have access on it.

To address these points in our prototype, we let the user define access control policies together with her contribution indicating the properties a reader has to possess and to prove. In order to protect the privacy also of readers, properties are presentable in an anonymous way and not linkable when repeatedly used. Therefore, we relied on the concept of *anonymous credentials* proposed by Chaum in 1985 [Cha85] and technically realised in the Identity Mixer (short: Idemix) system [CvH02]. The idea of access control based on anonymous credentials and access control policies is not new in general and was demonstrated in selected use cases for user - service provider - scenarios in the project PRIME ([ACK+09], [HBPP05]). We built on the results of PRIME, transferred the ideas to social software and demonstrated the practical feasibility of maintaining existing concepts of phpBB platform and integrating privacy-enhancing functionality provided by PRIME framework at the same time.

Using anonymous credentials, everyone can prove the possession of one or more properties (e. g. being older than 18, having more than 10 forum posts with a 5 star rating) without revealing the concrete value (e. g. being exactly 56 years old, having exactly 324 posts rated with 5 stars). In the prototype, credentials are also used to prove the possession of a particular role, which may be required by an access control policy. This implies that the process of creating a new resource includes that the originator of that resource receives the corresponding credential (`cred:Owner-`*`Thread-ID`* or `cred:Owner-`*`Post-ID`*) from the forum platform and stores it on the local device. The roles *administrator* and *moderator* are realised with help of the credential-based access control approach as well, i.e., the according credentials (`cred:Admin-Forum` and `cred:Moderator-`*`Topic-ID`*) are issued to the corresponding persons. Together with a new resource, default access control policies are created, which ensure that users who show the administrator credential or moderator credential get the required access granted to fulfill their roles. The owner of a resource possessing the owner credential always has access to that resource and can modify the access control policies to, e. g., allow other users with certain provable properties read access and maybe also write access to the resource.

In general, credentials are offered by particular trustworthy organisations, so-called *credential issuers*. Credential issuers need to be known to the public, so that everybody has a chance to get credentials certifying properties of the user. More details on the technical implementation of the prototype can be found in [WP110a, WP110b].

2.3.4 Scenario Revisited

Returning to the forum scenario from Sect. 2.1.2, the following alternative story illustrates how access control based on credentials and access control policies in a web forum works. Assume Hannes posts a message to the thread "Online Gambling" in a publicly accessible forum. The access control policy of the thread is derived from the parent topic, which is set to be open for reading and writing exclusively for people who have proven to be registered to an online gambling website. Hannes additionally restricts access to his post to allow only gamblers who are registered to their site for 3 months at least.

Table 2.1: Example of an access control policy

(1) Forum:	[(cred:Admin-Forum) OR (everybody*[default]*)] AND
(2) Topic:	[(cred:Moderator-GamesCorner) OR (everybody*[default]*)] AND
(3) Thread:	[(cred:Moderator-GamesCorner) OR (cred:Owner-OnlineGambling) OR (cred:memberOfGamblingSite)] AND
(4) Post:	[(cred:Moderator-GamesCorner) OR (cred:Owner-PostFromHannes) OR (cred:countMonth-memberOfGamblingSite $>$ 3)]

Whenever someone requests access to Hannes' post, the access control policy is evaluated according to the hierarchical order of content elements of the forum (cf. Table 2.1). In our example, step (1) ensures that authorised users are either an administrator of the forum or – since we have chosen a public forum for the example – any regular user. Step (2) specifies that users are allowed to read the topic "Games Corner" if they are a moderator of this topic or anybody else. The latter applies since the example does not specify any restriction on topic level either. Step (3) ensures that only users who are either moderator of the topic "Games Corner" or who are owner of the thread or who are member of a gambling website get read access to the thread "Online Gambling". Lastly, step (4) determines that only users who are either moderator of the topic "Games Corner", owner of the post, or member of a gambling website for at least 3 months can read the post created by Hannes. Note that read access to Hannes' post is only granted if the whole policy (steps 1 – 4) is evaluated to be "true". Similar to this example for *read access*, further policies can be defined in order to specify *add, edit* or *delete* rights of a resource. All users who add a post to a particular thread have the opportunity to further restrict access to their own contribution.

2.3.5 Privacy-Awareness Information

Having described the realisation of the privacy-enhancing selective access control extension so far, in the following we introduce a feature that supports users to be aware of their privacy in the forum. More precisely, we developed a phpBB modification (short: MOD) called "Personal Data" and integrated it into the forum prototype. The idea behind the Personal Data MOD is to provide additional privacy-related information in social software in order to raise users' privacy awareness, help them to better assess their potential audience and eventually enable them to make informed decisions whether to disclose personal data on the Internet. The perception of privacy in social settings depends on the anonymity or identifiability of the users on the one hand, and on the available audience, i. e., who may read and reuse the disclosed personal data, on the other hand. Considering that privacy is only a secondary task for users, presented privacy-awareness information should be easy and quick to understand and not hinder social interactions and communication as primary tasks in social software.

The Personal Data MOD contains two categories of privacy-related information:

Audience Hints about who may access user-generated content, e. g., number and/or properties of potential readers. This partly compensates for missing social and context cues in computer-mediated communication [Dör08] and reminds users especially not to blind out the mass of "silent" forum readers.

Identifiability Hints about potentially identifying data that is additionally available, e. g., IP address or location information known to providers. This shows that users are not completely anonymous on the Internet and in particular in phpBB forums, but that there are identifiers available.

In the prototype, the hint about the potential audience is coupled with the setting of the access control policies for read access. If no particular policy is specified for the corresponding forum element and the default policy of the upper-lying content element(s) states "allow everybody", then the Personal Data MOD indicates "all Internet users" as the potential audience for this post (Firgure 2.9). However, if an access control policy is set which restricts the potential audience, the MOD makes users aware of this fact as illustrated in Figure 2.10.

2.3.6 User Survey

Besides working on the implementation of the prototype for privacy-enhancing, selective access control, we wanted to evaluate whether our approach meets real forum users' needs. Therefore we conducted an online survey. The survey was available in German and consited of two parts: First, participants saw a realistic full-screen screenshot of the phpBB forum prototype with two posts in a discussion thread about leisure-time physical activity as shown in Figure 2.11.

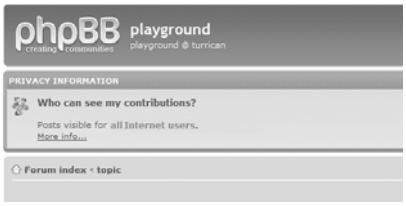


Fig. 2.9: Screenshot prototype: Privacy-awareness information about potential audience if access is not restricted.

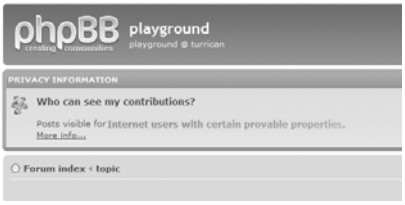
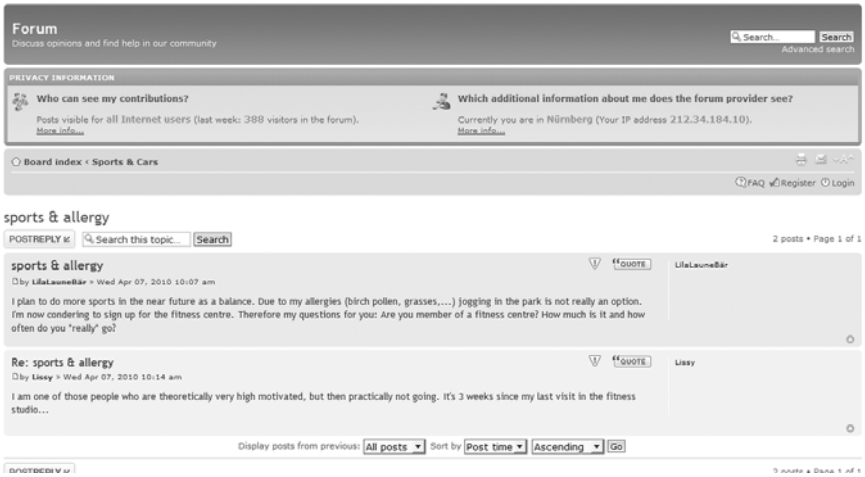


Fig. 2.10: Screenshot prototype: Privacy-awareness information about potential audience if access is restricted.

We instructed participants to imagine that they are the author of the first of the two contributions. An orange box on top contained either privacy-awareness hints or an advertisement. In the case that privacy-awareness hints were shown, participants saw either textual information about the potential audience and their individual current location, or numerical information about the exact number of visitors of the forum within the last week and their individual IP address, or a combination of both. All participants of the survey were randomly assigned to one of the four groups. For the second part of the survey, all participants were shown the same online questionnaire. The questionnaire contained questions about knowledge of technical- and privacy-related terms, use of the Internet in general and of forums in particular and questions related to audiences and access control. We also collected demographic data. A link to participate in the survey was distributed via blogs, mailing-lists and forums on the Internet. Due to this setup, we had a non-random sample as a basis for further analysis. After excluding answers from non-users of forums[7] and from participants who had not seriously answered the questionnaire, 313 valid responses remain. In the following, we report selected relevant results based on those 313 participants. More details about methodology, analysis and further results are provided in [PWG10].

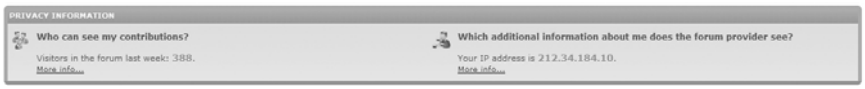
First, to test participants' knowledge and awareness of the potential audience, we asked them who actually has access to "their" forum post that they had seen previously. Second, since we were also interested in participants' ideas and requirements regarding access control, we further asked who they would *intend* to have access. Actually, the forum post that we showed to the participants was accessible for all people with access to the Internet, i. e., all registered and unregistered users, forum providers and Internet providers. The fact that the post from the example was completely public could be learnt from the privacy-awareness display with the textual information (shown for G_2 and G_3) and there was also a visual cue visible for participants of all survey groups indicating that the post can be viewed without being logged in, i. e. it is visible for everybody with Internet access.

[7] Participants who stated in the questionnaire that they have never even read in a forum are considered as non-users.

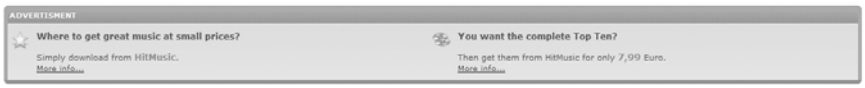


(a) Group G_3 (audience, location, number of visitors and IP)

(b) Group G_2 (audience and location)



(c) Group G_1 (number of visitors and IP)



(d) Group G_0 (advertisment)

Fig. 2.11: User interface for different survey groups (originally shown in German)

A comparison of the percentages of expected access vs intended access of different audience groups, listed in Table 2.2, reveals that nearly all participants know about and agree with the access to all post for registered members. Also nearly all participants know that the forum provider has access and three-quarters stated that the forum provider should have access. Our results further show that the majority of participants knows that also unregistered visitors can see the post, however only about one-third would *want* unregistered people to view their posts. Hence, there is a considerable difference between the percentage of participants who would let registered users read their posts and those who also would allow unregistered users access to their posts. This finding is interesting for two reasons: First, in most forums on the Internet, anybody can easily become a registered member by providing

Table 2.2: Expected vs intended access to forum posts by different given audience groups

Audience groups	G_0 n=78	G_1 n=74	G_2 n=86	G_3 n=75	all n=313
All registered users					
expected	96.15 %	97.30 %	95.35 %	97.33 %	96.49 %
intended	89.74 %	100.00 %	96.51 %	96.00 %	95.53 %
Unregistered users					
expected	69.23 %	70.27 %	70.93 %	78.67 %	72.20 %
intended	28.21 %	31.08 %	27.91 %	36.00 %	30.67 %
Forum provider					
expected	98.72 %	95.95 %	95.35 %	94.67 %	96.17 %
intended	66.67 %	75.68 %	75.58 %	70.67 %	72.20 %
Internet provider					
expected	47.44 %	47.30 %	52.33 %	50.67 %	49.52 %
intended	7.69 %	10.81 %	12.79 %	12.00 %	10.86 %

multiple choice questions with given answer categories

a fake e-mail address and choosing a password. This means that practically each Internet user could have access with no great effort, anyway and from this point of view there exists no essential difference between registered and unregistered users. Second, the result indicates that participants want to differentiate who can access their forum posts and that their requirements do not match with current access control settings which are defined by providers or administrators. Looking at the figures for the particular survey groups, we found no statistically significant differences between them (neither with the usual significance level of $p < 0.05$ nor with $p < 0.1$).

Besides deciding which of the four given audience groups is intended to have access to their forum posts, participants of the survey could specify other groups or share their thoughts about how access control should work in an additional free text field. Indeed, a dozen of the subjects took this opportunity to formulate ideas and said that they would like to authorise particular readers based on special properties or their relationship to them. A selection of comments, which underline real forum users' needs for selective privacy-enhancing access control, is presented below.

Selection of comments from participants to the question "Who would you intend to access your forum contributions?" (originally posted in German):

C1: "persons I have chosen"
C2: "authorised by me"
C3: "circle of people that I have defined"
C4: "members with at least 10 posts in the forum"
C5: "friends"
C6: "guests who I have invited"

These requirements can be addressed with the selective access control extension for phpBB forums. The extension enables users to define which properties someone has to possess – by showing either certified or self-issued credentials – for gaining access to users' contributions. It is also conceivable to have credentials that prove an existing relationship, e. g. *being friends in community X*, and using these credentials for specifying access rules. Thereby it is possible to realise relationship-based access control with the selective access control extension without being restricted to it. As argued previously, access control based only on relationships is not suitable for forums in general since this requires that the author of a contribution and the users she wants to give access have to know each other before. This assumption does not hold for web forums, where people with similar interests can meet and discuss without knowing each other in person.

2.4 Concluding Remarks

In this chapter, we have investigated privacy issues and issues surrounding the management and expression of identities in social software, with a focus on social networking sites and web forums. The main difference between the two example applications is that in the first case users already have a connection with each other whereas in the latter case potential interaction partners are not necessarily known to each other, e.g., by their user names. We presented appropriate concepts to address privacy-related issues for both types of social software.

First, in order to enhance users' privacy on social networking sites, our solution enables them to cluster their social contacts in their own 'collections' and we provide users with the possibility to create multiple 'faces', i.e., they can maintain multiple profile pages for their account. By defining which profile page should be displayed to the members of a specific collection, users are able to segregate their audiences and actively control who can access their personal data. In case the user does not trust the provider, she can further use *Scramble!* to encrypt all content and share decryption keys only with members of the intended audience. A precondition here is that users can address each other in order to exchange keys.

Second, we have presented the concept and realisation of a web forum prototype for privacy-enhancing selective access control. This solution enables active forum users to specify (a set of) properties which members of their potential audience need to possess. This means that even if the author and the audience are not known to each other, the author controls who can access her contributions to some extent. With *Personal Data MOD*, a feedback mechanism to support users' privacy awareness is integrated in the forum prototype. A user survey complements our work and has shown that the ideas behind the prototype meet real forum users' needs towards user-centred, selective access control.

If the developed selective access control features are used in a very restrictive way, social software users will experience a high level of privacy but a low amount of interactions. Vice versa, if the access control is handled very openly users could

lose much of their privacy. Certainly, it would be inappropriate to stick strict access control policies for every contribution in a forum or to encrypt each single piece of information on a social networking profile. However, having the user-centred selective access control at their disposal may encourage users to discuss issues, which they would not address in public forums, or to state unpopular and uncensored opinions to a specified audience. Neither the privacy-enhanced social networking site nor the web forum with selective access control will completely solve the conflict between sociability and privacy in social software. However, both applications empower users to find their individual balance on a case-by-cases basis.

Considering providers' point of view, it is important to note that privacy is a highly debated topic and providing social software with privacy-enhancing features can be a very good selling argument, especially with respect to people who refused to use social software so far because of privacy concerns.

2.5 Acknowledgements

Many thanks are due to Hagen Wahrig, Richard Wolsch and Joeri de Ruiter for their great work on the practical implementation of the concepts and ideas presented in this chapter.