Requirements and concepts for privacy-enhancing access control in social networks and collaborative workspaces

Editors:	Martin Pekárek (TILT)
	Stefanie Pötzsch (TUD)
Reviewers:	Uli Pinsdorf (EMIC)
	Erik Wästlund (KAU)

Identifier:	H1.2.5
Type:	Heartbeat
Class:	Public
Date:	July 2009
Status:	Final

Abstract

This heartbeat documents 17 use cases regarding common actions in Social Network Sites (9) and Collaborative Workspaces (8). These use cases, literature and a legal analysis of data disclosure in SNSs and CWs are used to elicit a set of high level mechanisms and requirements to be observed in the development of privacy enhancing features (e.g. access control) in Social Network Sites and Collaborative Workspace applications. The results described in this report are intended to serve as the basis for decision making and development of the PrimeLife WP 1.2 focal demonstrators.

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement n^{o} 216483 for the project PrimeLife.

Members of the PrimeLife Consortium

1.	IBM Research GmbH	IBM	Switzerland
2.	Unabhängiges Landeszentrum für Datenschutz	ULD	Germany
3.	Technische Universität Dresden	TUD	Germany
4.	Karlstads Universitet	KAU	Sweden
5.	Università degli Studi di Milano	UNIMI	Italy
6.	Johann Wolfgang Goethe - Universität Frankfurt am Main	GUF	Germany
7.	Stichting Katholieke Universiteit Brabant	TILT	Netherlands
8.	GEIE ERCIM	W3C	France
9.	Katholieke Universiteit Leuven	K.U.Leuven	Belgium
10.	Università degli Studi di Bergamo	UNIBG	Italy
11.	Giesecke & Devrient GmbH	GD	Germany
12.	Center for Usability Research & Engineering	CURE	Austria
13.	Europäisches Microsoft Innovations Center GmbH	EMIC	Germany
14.	SAP AG	SAP	Germany
15.	Brown University	UBR	USA

List of Contributors

Contributions from several PrimeLife partners are contained in this document. The following list presents the contributors for the chapters of this deliverable.

Chapter	Author(s)
Executive summary	Ronald Leenes (TILT)
Introduction	Martin Pekárek (TILT)
Scope: Social Network Sites and Collaborative Workspaces	Ronald Leenes (TILT), Stefanie Pötzsch (TUD)
Use Cases	Katrin Borcea-Pfitzmann (TUD), Stefanie Pötzsch, (TUD), Martin Pekárek (TILT), Maren Raguse (ULD), Karel Wouters (KUL)
Mechanisms	Carine Bournez (W3C), Dave Raggett (W3C), Martin Pekárek (TILT), Stefanie Pötzsch (TUD)
Issues	Ronald Leenes (TILT), Martin Pekárek (TILT)
Legal requirements	Aleksandra Kuczerawy (KUL), Maren Raguse (ULD)
Requirements overview	Martin Pekárek (TILT)
Conclusion	Martin Pekárek (TILT)
Lexicon of terms	Dave Raggett (W3C), Ronald Leenes (TILT)

This deliverable was rendered from HTML pages using Prince XML from YesLogic Pty Ltd. YesLogic has donated a license of Prince XML to W3C.

Executive summary

Heartbeat H 1.2.5 documents the results of an elaborate process to elicit requirements and mechanisms for privacy enhanced access control in social network sites (SNSs) and collaborative workspaces (CWs). The use cases, mechanisms and requirements discussed in this document form the basis for decision making regarding the wp 1.2 demonstrators to be developed within the PrimeLife project. Given the available resources within the project only a limited set of the use cases can be implemented. This document therefore extends beyond the wp 1.2 demonstrators.

SNSs and CWs inhibit a space that is spanned by three types of management: identity management (management of self), information management, and relationship management. SNSs primarily see to management of self and relationship management with information management being subordinate to these. CWs, on the other hand, primarily focus on information management. Both families of applications are members of the larger family of social software, were the sharing of information with like-minded spirits is a central feature. Since not every user of these systems belongs to this category, forms of access control to the various resources present is potentially required.

The document discusses common use cases for SNSs and CWs and shows how users disclose information on these social platforms and that the possibility to manage access to resources as well as managing one's identity is a necessity for privacy friendly 2.0 applications. The use cases show that users should be able to specify who, and under which conditions, has access to information about them or to the resources they provide. The scope of resources here is very broad. Basically it pertains to all user contributed content in Web 2.0 applications; users should be able to specify who can access their SNS profile, who gets to read their contributions to Web forums, who can view photo's they post online, etc. The use cases also show a need for Web 2.0 users to be able to specify under which partial identity they operate in a particular context or particular moment in time. A third important mechanism revealed by the use cases is a need for privacy awareness and transparency tools enabling the user to make informed choices about her behaviour (both regarding content to be disclosed and identity to be used).

The report also addresses aspects of the legal framework within which information disclosure in Web 2.0 applications takes place and the bearing this may have on the user interface of such applications. In particular the reports discusses the user as a data controller (next to the platform provider) when they disclose information about others (for instance on photo's or in discussions). In closed environments (such as a small group), the Directive (95/46/EC)'s household and private use exemption may be applicable, but in many cases the user will indeed be a proper data controller. This means that the user will have to acquire consent of those depicted or mentioned in contributions and that the data controller will have to provide information about themself and the purpose of data processing.

Finally, the report provides an overview of general issues that arise in SNSs and CWs. These issues can be grouped in broad categories: identity and relationship issues, surveillance issues, awareness (of risks) issues, and illicit use of content. The use cases and issues outlined reveal that elaborate access control mechanisms that go beyond what is currently available in the SNSs and CWs need to be developed. The report elaborates on a number of the key mechanisms that may help successful completion of the use cases. In particular it argues that rich access policies are required that allow for the specification of different kinds of access (e.g., identifier based, role based, group based, properties based). Also discussed are data handling policies, new federated authentication mechanisms, (partial) identity management,

anonymous and certified credentials, legal policy statements, content encryption and awareness and transparency mechanisms.

The use case, issues, legal analysis and requirements provided in this report will guide further research in wp 1.2 but is also valuable outside the scope of the PrimeLife project as it gives a comprehensive overview of relevant cases and issues.

Table Of Contents

Chapter 1

Introduction

This document constitutes the written result of the heartbeat with the full title: "Requirements and concepts for privacy-enhancing access control in social networks and collaborative workspaces". The title alone suggests that there are many alleys to be explored, and the current result underlines the broad scope that needs to be employed to effectively address privacy and identity management in social software.

In exploring the area under study, the first important observation is that the focus of the heartbeat is on two disparate types of social software. Both social networks - exemplified in social networking sites that are currently enjoying immense popularity - and collaborative workspaces are the research subjects. These two types of social software have many privacy-related aspects in common (see e.g. [Pekárek & Pötzsch 2009]), but differ in certain basic characteristics and their practical applications. Both types are considered in this document, and their diverging characteristics should not be left out of sight. The second observation is that access control is positioned as a primary means of privacy protection from the outset. Even stronger: the title already suggests that this is the way forward. Undoubtedly, improved means for users to manage privacy settings through access control potentially decrease the privacy risks users run when using these types of application, but more measures may be considered to serve this overarching goal. Therefore, in the document a number of different perspectives are considered that aim to explore the arising issues when using social software. It is investigated whether other means than access control could contribute to alleviating the concerns encountered.

Finally, the title starts with the terms "requirements" and "concepts". It is envisioned that the output of this current research effort can be used as input for the next step in the research, being the development and construction of prototypes for social networks and collaborative workspaces. Ideally, a list of requirements would be available in the last chapter of this document, that could be handed over to a number of software engineers who would be able to use it as step-by-step building instructions. In reality, this goal remains elusive due to the complex nature of the issues that we attempt to address, and the lagging experience with the prospective software environment(s) in which the proposed prototypes will eventually be realised. The iterative nature of requirements engineering is being acknowledged, judging from the PrimeLife Description of Work, which states that "The requirements will incrementally be revised following the prototypes and their evaluation." [DoW 2008].

Nevertheless, this document is expected to offer a good starting point for the subsequent development effort.

Chapter 2 starts with a short introduction to the two types of social software that are the object of the requirements elicitation effort, in which the scope is set for the next chapters exploring several angles to generate a number of requirements. The first angle explored is through the description of a number of use cases in chapter 3. Herein, short stories on the actual prospective use of proposed software solutions highlight particular pitfalls users may encounter. The alleviation of these pitfalls translate into mechanisms that need to be implemented in order to enable these use cases. The next chapter (4) titled Issues takes recent literature as a starting point in describing the problems encountered in the use of social software. Many of these issues can immediately be complemented with a tangible requirement necessary to resolve the issue. It is worthwhile to notice that the encountered issues in the use of social software are much broader than mere access control issues, indicating that potential solutions should also be positioned in a wider setting.

Chapter 5 titled Mechanisms draws conclusions from the previous chapters, and provides a condensed and categorised overview of the different means that can be employed to implement privacy-enhanced features in social networks and collaborative workspaces. Also, this chapter expands on specific mechanisms that merit more attention because of their particular (technologically) innovative character. The next chapter (6) underscores the fact that requirements can be derived from many sources, of which existing legislation is instrumental. Therefore, an entire chapter is devoted to legal requirements, in which also some particularities of social software are considered from a legal angle. Chapter 7, Requirements overview, summarises all requirements that have been addressed in the document so far, and categorises them into several (types of) mechanisms, thus linking this chapter with chapter 5 on mechanisms. A chapter with conclusions and outlooks and a reference overview wind up the document. In the annex, one can find a glossary, that was drafted during the development of this heartbeat document, and which may provide the less experienced reader with background information on terms used in conjunction with privacy-enhanced social software.

Chapter 2

Scope: Social Network Sites and Collaborative Workspaces

This heartbeat discusses use cases, mechanisms and high level requirements concerning Social Networking Sites/Services and Collaborative Workspaces. A detailed analysis of these instances of social software can be found in PrimeLife Heartbeat 1.2.2 “Privacy and Access Control in Social Software”. Here, we limit ourselves to outlining the primary features and the relation between the two types of social software.

Social software can be described as software in which three principal forms of management occurs: management of self, relationship management and information management (see figure 1). Social Network Software/Services focus on presentation of self, relationships and communities. It is focused on the individual, and users can create additional content (private messages, listed groups, the “wall” or “pin board”) - usually related to their profiles - to present themselves within a group of people. Collaborative workspaces focus on content and the process of jointly creating content. The key functionality of collaborative workspaces is to support collaborative editing and creating of contents (c.f. information management in Figure 1). The co-authors in a collaborative workspace form a social network, but this social network is not the essence of the collaborative workspace: the focal point is the jointly created content. The main value of a social network site lies in the network itself even if a collaborative plattform is integrated into the social network site, e.g., to enable members of a group to create shared content.

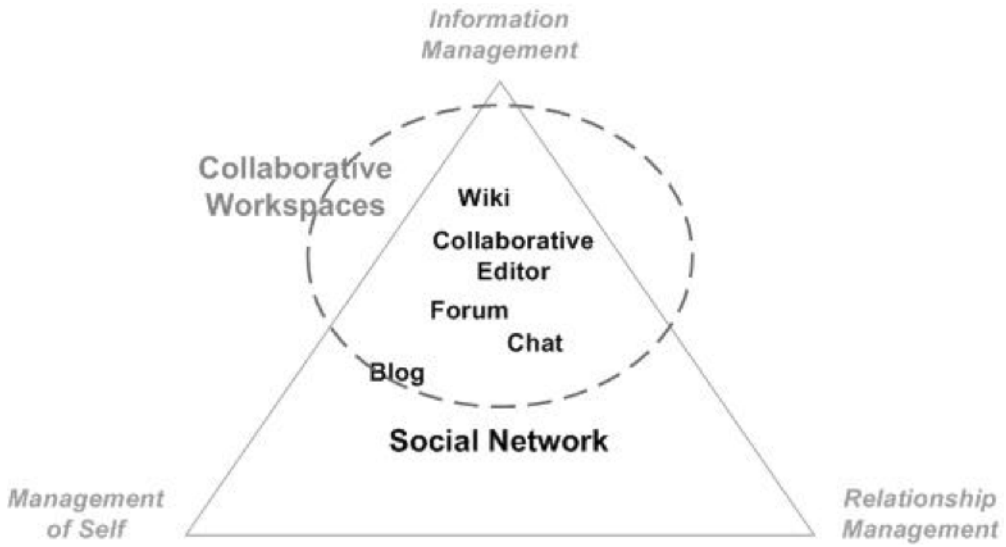

Figure 1: Functional Triangle of Social Software according to (Richter and Koch, 2007)

2.1 Social Network Sites

SNSs have three common features:

1. identity construction. Social network sites offer a very direct tool for what Goffman [Goffman 1959] calls "impression management": the profile page.
2. relationships. Social network sites offers communication channels for the users to make new friends and deepen connections with current ones.
3. community. Social network allow users to represent a social position: to be recognized as a valued member of one's various communities. Connectedness is social currency (social capital).

A typical SNS 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. Most offer multiple tools for users to search out and add potential contacts. Apart from the fixed fields for entering relatively static (personal) data, most sites also offer areas for ongoing communication (comments) that resemble 'writing on the wall'.When the pre-defined privacy settings are used, everyone can see (half of) the conversation between a profile owner and other users. This is where most of the action is.

Many SNSs also provide facilities for embedding applications in a profile page. These applications can pull data from other sources to the profile, or push information of the profile to other profiles or service providers. A much debated application is Facebook Beacon which notifies your 'friends' of purchases (movie tickets, video rentals, books etc) you made from participating entities. As an aside, it is important to realize that users have different perceptions of what they are doing on the networks. Considering three kinds of users ('Myspace is My Space (I claim privacy in a public space)', 'This is my recorded life of which I'm proud (Harry Truman show)', 'None of this is real (Fakester Manifesto)') illustrates that assuming that others play according to your rules may create problems.

In SNSs, the following personal data can exist

- first, the profiles of users (e.g. name, photo, contact data, date of birth),
- second, the connections between profiles,
- third, contributions of users (e.g. in group discussions, a posting on the wall of someone else).

2.2 Collaborative Workspaces

Collaborative workspaces (CWs) are infrastructures and platforms that enable users to work together, e.g. gathering information or creating contents in a collaborative manner or simply sharing data between each other. Applications of collaborative workspaces include knowledge management in an electronic environment, idea generation by applying computer-supported creativity techniques, or informal discussions of everyday life, amongst others. The focus of a collaborative workspace is on content. The very basic idea is to share resources such as texts, sounds, pictures, movies, and combinations of them. Users of the collaborative workspaces are allowed to access, display, move, remove, edit, and create resources in accordance with access control rules. Technical systems for establishing collaborative workspaces can be grouped into the following categories according to their functional differences:

- Wiki Systems,
- Collaborative Real-time Editors,
- Internet Forums,
- Chats,
- Weblogs,
- Comprehensive Groupware Systems.

More detailed information about these applications is available in Heartbeat 1.2.2 [Kuczerawy et al. 2008].

In CWs, the following personal data can exist

- first, the contributions of users (e.g. posting in a forum, message in a chat),
- second, the meta-data of the communication (e.g. time stamp when a contribution is made, availability of the user, list of all topics to which the user has contributed),
- third, member profiles, if any availabe.

Chapter 3

Use Cases

3.1 Introduction

This chapter presents a variety of use cases from social networks and collaborative workspaces. We put the focus on illustrating how privacy and access control should be realised in such applications and use the PrimeLife Personas in the descriptions of the use cases. From the use cases a number of mechanisms and, in turn, requirements - both abstract and more concrete ones - are derived.

Every use case comes with an initial inventory of mechanisms that are applicable to that particular use case. A number of use cases make a direct link between the identified mechanisms and the requirement that can be derived from it. This is the first step towards the inventory of a list of relevant requirements for CWs and SNS. At the end of the chapter, a summary is presented of all identified mechanisms. These mechanisms will contribute to the overall overview generated in chapter 7. Some of the use cases also present a number of open questions/ alternatives. These are added to the use cases to demonstrate issues that are to be considered in a later stage of the project, when tasks based on the use cases will be used for the evaluation of the prototypes from an end user's perspective.

3.2 Choice of use cases

When drafting use cases, one has virtually unlimited degrees of freedom. It is important, however, to ensure that on the one hand the number of use cases is manageable, but that on the other hand, all relevant aspects of the subject under study are covered.

For the use cases on *social network sites* (SNSs), we have considered the lifecycle of the use of SNSs. Therefore, the most frequent interactions with SNSs have been formatted into a use case, where the existence of a SNS, a number of profiles and connections between them are considered to be already implemented. A use case describing the creation of an account and the establishment of connections was deemed to be trivial.

SNS use case 1 and 2 describe the process of posting information to one's own profile and to someone else's profile respectively, highlighting the access rights to profile pages from the perspective of the contributor. The next two use cases describe how information available on SNS profiles can be accessed and/or used (use case 3), and how the profile owner is informed about the access to and use of the information (use case 4). This way, the first four use cases cover the basic information access activities occurring on SNSs.

Use case 5 introduces mobile SNS applications, the rising stars of the SNS firmament, and therefore indispensable in an overview of relevant SNS use cases. The next two (no. 6 and 7), shift the centre of attention from access management to privacy aspects. Use case 6 describes how a user can join a group anonymously, and use case no. 7 forms its counterpart, namely discussing how a group can allow anonymous users to become members in a certain group. SNS use case no. 8 describes the situation in which someone would like to leave an SNS, thereby deleting all the information generated over the lifetime use of the system. The final SNS use case is no. 9, introducing a particular setting (intra-company), in which the confidentiality of communication between SNS members is discussed.

For the use cases about selective access control in *collaborative workspaces* we aimed to include a variety of scenarios to illustrate the broad range of possible requirements about access control to users' data and views from a general, a technical and a legal perspective on this topic.

Use case no. 1 illustrates the necessity not only for simple access control policies, such like "resource is only accessible for registered members of the forum", but also for combined access control policies, e.g. "resource is only accessible for users, who have (((golden member card) AND (number of posting > 200)) OR (friend of owner of the workspace))". Use case no. 2 shows that we need to consider access control not only for currently available contents, but also for history files that are available to the public. The next use case (no. 3) illustrates the situation of access control based on dynamic properties of users, i.e. properties which vary over time. Use case no. 4 describes that access control should not only be applicable to single resource, but allows users to set the same rule for a couple of resources at once.

Use cases 5 and 6 are especially interesting from an legal point of view. Use case no. 5 shows how employees can be surveilled by their employer if the latter has a role as provider of the internal application for collaborative workspaces in a company. The access of the provider to user data and meta-data should be considered. Use case 6 explains possible problems that develop if providers have completely no access to users' data. Use case no. 7 discusses the management of (partial) identities in CWs, and the final use case (no. 8) introduces a number of selective access controls managed by the user.

3.3 Use Cases: Social Networking Sites

In the following sections we present a collection of different use cases describing several issues with regard to privacy and access control in social networking sites.

3.3.1 UC_sns1 - Post content to own profile

Goal:

- Illustrate the need for mechanisms to post content to one's own SNS profile

- Illustrate the need to define who can access this information

Preconditions:

- The profile owner already created a profile to which additional information can be posted
- The profile owner has connections with a number of other profile owners
- The profile owner has defined a number of lists among his connections

Scenario(s):

- Frank selects some photographs from his camera that he wants to upload to his profile page on the SNS "Seniorweb". He snapped them at the yearly Seniorweb picnic, a group outing where likeminded people can meet in person. He would like to share these pictures with one particular personal list of friends, namely the list titled "Picnic Lovers", that he already defined as one of several lists. These lists and their members are already included in his profile. After logging into the SNS, Frank uploads the photos to his profile, and selects "Picnic Lovers" from his lists as the only list that can access the photos. He does not want all his contacts to see these pictures: his love of picnics is something he wants to keep to himself. Frank has defined that all members of "Picnic Lovers" get a message that he has uploaded new information for them to view.

Success Conditions:

- Content is posted to the profile page of the user
- Content is accessible by certain (lists of) connections
- Everyone who has access to the information gets a message that new content is available

Failure Conditions:

- Connections other than the defined lists can access the uploaded content
- Connections other than the defined lists get a message indicating that new content is available

Mechanisms:

- Authentication, e.g. through a membership of access control list, when logging in.
- Define personal lists, that include a number of persons chosen by the profile owner. The mechanism should support different levels, e.g. several lists next to each other, overlapping lists, sublists. In contrast to groups where members of the SNS can choose whether they want to join, lists contain a (sub)set of connections of a user. This personal lists are part of the user's profile and are solely adminstered by him.
- Define content classes for data that can be "tagged" directly as being viewable only by selected lists. Frank may label his contribution with the content class "Leisure Time" for instance. He previously defined that content tagged as "Leisure Time" is only accessable to friends from the list "Picnic Lovers".
- Encryption: encrypting content and distributing the key to entities who should have access.

3.3.2 UC_sns2 - Post content to another profile

Goal:

- Illustrate the need for mechanisms to post content to someone else's profile
- Illustrate the need for the profile owner to be in control of what gets published on his own profile

Preconditions:

- The profile owner already created a profile to which additional information can be posted
- The profile owner has connections with a number of other profile owners

Scenario(s):

- Hannes is connected to Inga on a leisure SNS. They went out with a group of friends past weekend, and had a lot of fun. On Monday morning, Hannes wants to leave a message on Inga's profile page telling her how much he enjoyed everything. Therefore, he accesses Inga from his list of friends, selects the option to leave a note, writes it, and sends it to Inga for publication. Inga decided that she wants to review all messages left on her profile page before publication, after she suffered from less genial posted messages in the past. Inga gets notified that someone has left a message to be published on her profile page. She logs onto the SNS (if she hadn't done so yet), reviews the message, and decides whether she wants to publish it. If so, the message gets published. Inga has indicated that everyone whom she is connected to, gets an update when a new message appears on her profile, which consequently happens. If she does not want to publish the message it gets deleted. Alternatively, the choice of not publishing may also result in data that is not shared at all, but remains available for the profile owner. Hannes as the creator of the message gets a notification after Inga has decided whether to publish it.

Success Conditions:

- A message gets published on someone else's profile page
- The profile owner decides whether the new message is allowed
- Other connections get informed of the newly uploaded content

Failure Conditions:

- Messages get posted without consent of the profile owner

Additional Questions and Remarks:

- A further option to deal with the publishing of the message in Inga's profile is to allow only members from a personally defined list of connections to see the message, e.g. Inga's list "GirlfriensWhoNeedToKnowAboutMyDatingSituation".
    - This use case presupposes a direct link between the SNS user, content that is present on the profile site of the user, and the management of access rights to that content by the user. It is also possible to split the storage of the content (e.g. by means of a photo hosting site), and the access management to that content (e.g. by keeping this feature in the SNS). In such a constellation, it would be possible to check whether a visitor to the content

should be allowed access, based on the rights that have been granted to the particular visitor (e.g. by redirecting the call for access to the SNS access lists managed by the SNS user). This process could even occur without identification of the content owner, thus raising the level of privacy of the content provider. The mechanism is elaborated in section "Privacy-enhancement by new authentication mechanisms" of the chapter "Mechanisms".

- Related to the last observation, when creating a mashup, authentication of the visitor might be forwarded to the mashed-up component. In Google Sites, both scenarios exist: if you include a GCalendar, the visitor does not get to see the content, unless the calendar is shared with him. If you include a Picasa slideshow, any user that has access to the Google Site can view the shared pictures.

Mechanisms:

- Authentication, e.g. through a membership of access control list, when logging in.
- Authorisation/rights management: granting and revoking read/write rights per (group of) connections
- New authentication mechanisms (separating content, user groups, and access credentials)
- Define content classes. Hannes may label his contribution with a content class.
- Mechanism: Encryption, with the difference from UC_sns1 that encrypted content, posted to someone's profile, will have to be shared with that person (key), and that the profile owner can detect/correct who else is granted access.

3.3.3 UC_sns3 - Control access to and use of SNS content

Goal:

- Demonstrate the need to differentiate access to and use of SNS content between different parties:
  - (Different categories of) other SNS members
  - The SNS provider
  - Third parties (including ones using APIs such as mashups).

Preconditions:

- Content is posted on the profile

Scenario(s):

- Joshua has posted several new songs of his band on his SNS profile page, and wants to share these songs with some of his connections. He granted his connections in the list "Music lovers" access to the information. Frank, who is one of Joshua's connection who is listed in "Music lovers", can therefore download the latest material. Joshua is not ready yet to release his information to other defined lists of connections or other parties. These parties include automated programs (applications), that crawl the SNS searching for music files. When a program looking for this file type wants to access these on Joshua's profile, it should not gain access.

- Although Joshua would allow his friends that he listed in "Music Lovers" to enjoy his latest songs, he does now want them to forward the songs top other people who do not belong to the "Music Lovers" list.

Success Conditions:

- The same piece of information should be accessible to a share of users (e.g. (lists of) connections), but not to another share of users (e.g. applications)
- A piece of content that gets forwarded from an authorised list member to someone who is not on the list, should not be usable/viewable.

Failure Conditions:

- Some information is available to every type of information searcher
- Some information is usable by any user

Mechanisms:

- Access control, based on the type of the party who wants to access.
- Credentials. Only communication partners that have the right credentials (e.g. given to them when assigned to the list "Music lovers") can access/decode the information. Other parties cannot access/decode, or even find the information.
- Data handling policies (DHP), that travel along with the data when they get downloaded/shared with connections over the network, thereby denying access to the data to people who do not have the right credentials.
- Policies, enforced by a local secure software component (Window Media Player - alike).
- Traitor tracing schemes: to detect 'illegal' copies, (e.g, add a watermark for each downloaded copy). Informing the user that this happens also has a deterring effect. Note the analog hole: anything digital can be converted to analog form which makes it usable for humans. After that, it may be possible to copy it and thus circumventing a protective measures against copying (e.g. depending on the robustness of the watermarking algorithm that is used for the downloaded copy).

3.3.4 UC_sns4 - Report on access to and use of SNS content

Goal:

- Generate an overview of accessed profile information (logging), differentiated per user, such as other SNS members, the SNS provider and third parties (including APIs)

Preconditions:

- A profile page exists
- Content has been posted to the profile page

Scenario(s):

- Eugene has a complete profile page, including lots of uploaded information, on an SNS. In the course of a week, numerous people visit his profile page, both the publicly available information as well as the information that is only available for certain subsets of his connection. The content that is available on his profile site is

also separated in a publicly available part (consisting of photographs), and a private section. Eugene, being a hacker, has a section dedicated to the weaknesses of Internet Explorer 7, a web browser. The section consists of case descriptions and software to exploit various weaknesses in IE7. He is very interested who views this information.

- Eugene wants to have an overview who views what information on his profile. He wants to be able to differentiate between the following groups:
    - Connections (in general or single connections)
    - General public (not connected with Eugene)
    - The SNS provider
    - Automated programs (e.g. through mashup API)
- The overview can be created:
    - on a regular basis (daily/weekly/monthly)
    - in real time (to be used as an alarm when something/someone is accessing the information

Success Conditions:

- The requested information overviews are created

Failure Conditions:

- No information can be given concerning the access and use of information on a particular profile, whether it concerns profile information or content downloads.
- No distinction can be made between the information requesters (connections, SNS provider, etc.)

Additional Questions and Remarks:

- Is a mechanisms possible that hides the information a) that Eugene is logging access to b) what file and c) when he is checking the log from the provider?

Mechanisms:

- Logging, perhaps based on access control mechanism.
- Access control for the logging information (identical to the one introduced in UC_sns3)

3.3.5 UC_sns5 - Integration of mobile SNS applications

Goal:

- Illustrate the integration of location data in an SNS

Preconditions:

- A profile exists

Scenario(s):

- Ines has subscribed to an SNS, that involves location based features. This particular feature takes the current position from the mobile device of Ines, and transfers this information to her profile page on the SNS. Her connections can now see where she

currently is. The actual location information is conveyed by means of a map of the area where Ines currently resides. The availability of this information can be subject to several criteria:

- The location information is available to everyone who visits the profile page of Ines: everyone gets the same location information.
- Different lists of Ines' connections get different levels of detail. For instance, her close friends get the most exact location possible (within metres), whereas other lists get general information on her location (e.g. within kilometers), just indicating whether she is in town or not.

Success Conditions:

- The user can easily (de)activate his visibility for certain designated user groups (other connections, lists of connections, the SNS provider and third party programs).

Failure Conditions:

- The location information is distributed without the consent of the user.
- The location information is distributed in the wrong level of detail. More detailed information is more problematic than less detailed information.

Additional Questions and Remarks:

- Is it necessary for other users to have a certain application implemented on their SNS profile page in order to see Ines' location information? This would help the application provider to build a customer base because of the viral effects of application distribution (everyone tells everyone that they need this application in order to see where they are).
- An alternative implementation would be that the application would only be implemented on the mobile device of the user, preferably as a plugin of a mobile version of an already existing "regular" SNS. This would bring interactivity between roaming SNS users closer (e.g. sound alerts when one of your friends is near you).
- Is is possible to allow the user to change visibility settings either by visiting the SNS web site or also by switching it on and off from the mobile device without access to the web site?
- Should it be possible for the user to fake his location data?

Mechanism:

- Authentication. The application (plugin) should be sure that the REAL user is being identified using a REAL location in order to prevent (a) a user to fake his identity, or (b) a user could fake his location (see the Failure condition). Digital signatures may be used.

3.3.6 UC_sns6 - Joining groups anonymously

Goal:

- Illustrating how to join a group anonymously

Preconditions:

- A group with a certain dedicated topic of interest exists in a wider SNS.

- A user with a profile exists.

Scenario(s):

- Frank is thinking about joining a group on Seniorweb dedicated to the problem of arthritis. He thinks he may be suffering from it, but he is not really sure. This is the reason why he would like to join this group, as he thinks that the informal discussions between group members may give him more information whether his particular condition is arthritis or something else. To reach his goal, he searches the "Groups section" of Seniorweb using keywords like "arthritis", "stiffness", "painful joints", etc. His search results in a list of groups that match his search criteria. The top one is called "Old Men Online", and he decides to join it. Hereto, he clicks the "Join" button on the interface, after which he enters a pseudonym. Frank has explicitely decided that he wants to join the group anonymously: there is no need for anyone to know that he might be suffering from anything! However, he would like to share some aspects of his identity (e.g. age and city of residence) in order to make the interaction with the group more effective.

Success Conditions:

- The separate partial identity of Frank in his role as a member of "Old Men Online" cannot be associated to other parts of his presence within the same SNS. This should apply to other SNS users, applications, and the SNS provider.
- Frank wants to build on and extend the identity he has already created within the SNS. In other words, he wants to reuse parts of the information he already entered, and does no want to build a new, pseudonymous profile from scratch.

Failure Conditions:

- Frank's identity can be deduced from his activities within "Old Men Online".

Additional Questions and Remarks:

- Will Frank get a warning from the SNS when he is going to disclose his city "Supersmalltown" and there are only three members in the SNS from that place, where Frank is the only one above the age of 50? -> Awareness: Dynamic warning based on identifiability
- The same scenario may be developed describing Frank joining an SNS specifically dedicated to a certain illness as a new, outside member. This would make the issue in separating different contexts easier, since Frank would only have one context which he would have to manage in this setting: the context as a potential patient. It was decided to use the concept of a group within a wider, generic SNS, since this limits the number of different accounts (with their associated login credentials) Frank would have to manage. Also, it points out the challenge of context separation within one SNS.

Mechanism:

- Partial identities, because this would allow Frank to stay within the same SNS, without having to learn and populate a new SNS. Anonymous profiles is probably not a good mechanism, since he would like to share his (partial) profile with other patients, and therefore effectively not stay completely anonymous.

- Alternatively, the partial identity mechanism could be extended into a global (partial) identity management mechanism, in line with the mechanism introduced in UC_cw7. Such a system would support the management of partial identities to be employed in different SNSs, or separately manage partial identities used in one particular SNS.

3.3.7 UC_sns7 - Admitting anonymous group members

Goal:

- Illustrating how group owners admit new anonymous members

Preconditions:

- A group with a certain dedicated topic of interest exists in a wider SNS
- A group manager exists
- A prospective member with a profile exists

Scenario(s):

- Ines is running a special interest group of patients suffering from multiple sclerosis (MS), a serious disease affecting the central nervous system. The group allows patients to discuss their disease, share their experiences, and find mutual support. In principle, anyone can join the group, but Ines wants to limit the membership to actual patients. The reason is that she is afraid that people may join the group who have less honourable goals. For example, it happened in the past that someone joined who was pretending to be a patient, but turned out to be employed by an insurance company whose sole aim it was to discover as much personal information as possible from the group. The objective of the insurance company was to find out who was actually a (potential) patient, enabling them to deny them insurance if they were to apply for it. To counter this risk, Ines advises everyone to use a pseudonymous partial identity during the registration process.
- Ines only wants genuine patients to be able to join. Therefore, she asks for some proof during the registration process. She has opted for a digitally signed statement from a certified doctor, stating that the particular patient who shows the statement is genuinely diagnosed with MS. The statement can only be used by one patient, thus eliminating the risk that someone registers using someone else's statement. A neat feature is, that the statement does not identify the patient, although the patient using a pseudonym when registering is the only one for whom the statement is valid, and can therefore be authenticated as a valid potential group member. To further minimise identifiability, the exact identity of the doctor is also hidden: the only thing that is sure is that he/she carries the qualification to diagnose patients with MS.
- In order to distribute the power of controlling the access to the group a vote by all members of the group is possible. Only if *m* out of all *n* group members vote for the new member applicant s/he is allowed to join the group.

Success Conditions:

- People can join the group only if they are patients.
- New group members cannot be identified, nor can a connection be established to their online profile in the wider SNS.

Failure Conditions:

- User identities can be uncovered.
- People pretending to be patients gain access to the group.

Mechanism:

- Access control based on (anonymous) credentials: a credential given by a third party (e.g. a certified medical doctor) should allow access to the site.
- Partial identity: this would allow to build on the already existing profile/experience/ lay out that you have in an SNS, but assure anonymity when interacting with the special interest group.
- Alternatively, the partial identity mechanism could be extended into a global (partial) identity management mechanism, in line with the mechanism introduced in UC_cw7 (and UC_sns6 above). In this use case, it would allow the use of different patrial identities within the confines of one SNS.
- Anonymising networks (e.g. TOR).

3.3.8 UC_sns8 - Deleting an SNS profile

Goal:

- Illustrating what happens if someone deletes an SNS profile

Preconditions:

- An existing profile with connections and uploaded content
- The profile owner has left comments/sent content to other profile pages

Scenario(s):

- Joshua has been active on a particular SNS for some time, that focuses on the treatment of some serious mental disorder from which he was suffering, Recently, Joshua has undergone treatment and has emerged cured (i.e., his disorder is said to be in remission): he feels like a different person nowadays. To underscore his new take on life and eradicate all existing information that could link him with his cured disease, he decides to quit the SNS and delete all the information that he has contributed to the SNS during his membership period. After hitting the "Close my account"-button, the following information should be deleted:
    - His profile.
    - All the content uploaded to his profile, both by himself and by others.
    - All connections between Joshua's profile and his friends.
    - All communications that has taken place in the past.
    - All comments that Joshua left on profile pages of other members.

Success Conditions:

- After deletion, no information that was generated by Joshua should remain on the SNS.

Failure Conditions:

- Information of Joshua remains to be found on the SNS.

Additional Questions and Remarks:

- Who is the owner of messages? Does communication belong to the sender, to the receiver or to both parties? Answers to these question influence the options how to decide about the access or deletion of data.
- What about quotes or rephrasing of data that Josha once has published in the SNS by others?
- What about meta-information, e.g. logs of Joshua's visits to other member's profiles? -> conflict with UC_sns4

Mechanism:

- Sticky policies, applying to (a) content, (b) connections, (c) communication. For the last part, (c) communication, it is necessary to treat communication occurrences as content. This implies that each piece of interaction between users (e.g. a chat conversation between two SNS members) is tagged with metadata, such as the IDs of the people participating, and a timestamp of the communication. This way, data on communication can be dealt with just like any other content, and could be deleted using the information stored as metadata.

3.3.9 UC_sns9 - Confidentiality of communication in companies

Goal:

- enable only lawful access to content of communication exchanged over a company SNS; log access to enable later judicial scrutiny

Preconditions:

- A profile page exists
- The SNS allows exchange of messages (that are not public like the profile's wall)

Scenario(s):

- Inga has a SNS profile page. The news agency she works for supports use of the company SNS in order to tie the employees together and allows exchange of private messages over the SNS. A time limit of 30 mins of daily use is set. Inga is very fond of using SNS but wants to be sure that her employer does not access the content of messages exchanged over the SNS: after all she thinks these are private messages.
- Inga wants to be sure that her employer has no general access to the messages exchanged.
- Inga is aware of the fact that access may be necessary for law enforcement authorities, but that her employer must respect the secrecy of telecommunication and must never access the content for own purposes.
- The messages should be encrypted; decryption should only be possible if the keys of the company's data protection officer, a member of the company's works council and the member of the legal department responsible for police requests are used jointly.
- Accessing a message's content is logged. Inga can access the log at any time.

Success Conditions:

- General access is prevented, only cooperation of all three representatives allows access

Failure Conditions:

- access is possible to a member of the SNS who is not a recipient of the message
- collusion to circumvent three-eyes-access is possible
- no logging of access or incorrect logging
- no access to logs by the SNS users

Additional Questions and Remarks:

- The confidentiality principle in this use case may not only apply to companies but any communication via a SNS in general.

Mechanisms:

- Encryption and decryption of communicated content between 2 parties (sender/ receiver).
- Decryption by a combination of three parties' keys, that are NOT sender or receiver.
- Encryption of the communication metadata, like time sent, length of message, etc.

3.4 Use Cases: Collaborative Workspaces

3.4.1 UC_cw1 - Complex Access Control Policies and Data Handling Policies

Goal:

- Illustrate necessity for combination of simple access control rules
- Illustrate fine-grained access control with regard to 'Access for whom?'

Preconditions:

- Forum that allows creation of threads and defintion of access control rules

Scenario:

- Inga is member of the management board of the 'Street Art Club'. In the club she and her club mates share their opinions about street art and showing photos of some work. For this purpose, they also have a forum online, where Inga starts a new thread 'Photos of Street Art'. She therefore uses the nickname 'IvI' since she does not want to be recognised easily as a member of the management board of the club but she wants her different contributions to the forum to be linkable.
- For the forum thread she only wants to allow users who provide any nickname and who are currently member of the 'Street Art Club' writing access. Further, she decides that also her friends 'Ines' and 'Florence' should both have reading access regardless of their membership in the club, however they have to prove that they are Ines or Florence, respectively.
- Since Inga does not want her nice photos to be linked, copied or re-used by others, she also defines a rule that the posted pictures from her can be viewed by all members who have access to the thread, however further usage is not possible.

Success Conditions:

- User is able to specify combined access control conditions for the forum thread and the rules are enforced automatically by the system (e.g. using *AND, OR*)

- Different proven or unproven properties can be specified (*certified credentials and self-issued credentials*)
- User can define data handling policies for particular contents

Failure Conditions:

- Use of pseudonyms is not possible
- Combination of simple access control rules is not possible
- Definition of data handling rules is not possible
- Rules can be specified but will not be enforced
- Creator of the thread herself is no longer able to access her thread / contents or edit the policies

Mechanisms:

- Pseudonym / Partial Identity
    - Requirements: Inga can choose a unique nickname
- Access Control Rules, Credentials (self-issued, certified)
    - Requirements: Inga should be able to specify different access control policies to the thread according to the type of access. Others can prove certain attributes (e.g. member of the club) to get access to the thread.
- Data Handling Rules
    - Requirements: Inga should be able to specify data policies for her published contents and these DHPs will be enforced.

3.4.2 UC_cw2 - Fine-grained Access Control for Different Areas

Goal:

- Illustrate fine-grained access control with regard to 'Access to what?'

Preconditions:

- Wiki that allows creation of wiki sites and definition of access control rules for every wiki site including history and discussion pages

Scenario:

- Hannes starts a new wiki page about 'Online Games'. Since he does not care about access control he uses the standard configuration, which means free reading and writing access for everyone. He invites Bob, who has also much knowledge about online games, and both start to collect first ideas about what is interesting to say about online games. Carol, who is also interested in online games, found the wiki site and starts to restructure and modify the content and comments on the previous work of Hannes and Bob. Dave, who works for 'Gamba' - a company that makes much money with online games - also visits the wiki site. He thinks that the games of Gamba need to be represented better and therefore he also edits the wiki site.
- After Hannes saw what has happened, he decides to set new access control rules, that allow only Bob and him access during the current phase of early development. When the two guys declare their wiki site about online games as 'ready for the public', Hannes again edits the access control rules, so that everbody has reading access on the wiki site and can add comments on the discussion page if he/she provides a nickname.

- However, Hannes does not want to make the previous versions (the so-called history) of the site also available to the public in order to hide the surreptitious advertising from Dave and the abundance of spelling mistakes that he and Bob produced during the development of the wiki site so far.

Success Conditions:

- User is able to specify access control rules seperately for versions of the wiki content, history and discussion page

Failure Conditions:

- User can only define access control for the wrong level of details, e.g. for the whole wiki site (including all older versions, discussions)
- Creator of the wiki site herself is no longer able to access all versions and discussion page / edit the policies

Mechanisms:

- Access Control Rules & Management
    - Requirements: A Standard Configuration for access control exists when a new resource is created. Hannes should be able to change the access control rules for the resource. Hannes should be able to have writing access to contributions from others (delete).
- Access Control Rules & Management
    - Requirements: Hannes should be able to change access control rules on a fine granularity for the resource (e.g. current, version, history, discussion page).

3.4.3 UC_cw3 - Access Control based on Dynamic Properties

Goal:

- Illustrate necessity for revoking of credentials
- Illustrate possible interplay between Forum and SNS

Preconditions:

- Forum that allows creation of threads and definition of access control rules for every thread
- Social network that allows for indication of "friendship" between members

Scenarios:

- Joshua first browses the forum and is just reading content of publicly accessible threads. When Joshua then wants to contribute some ideas to a thread about music bands, which was created by his friend Peter, he is asked to provide a proof of his friendship with Peter. Having this proof of friendship (e.g. a certificate of a relationship of type "friends" in a social network), Joshua is able to contribute to the thread about music bands. However, one day Joshua and Peter have a dispute over a girl and as a consequence Peter ends his friendship with Joshua in real life and in the social network. As a consequence thereof, Joshua is no longer able to get writing access to the thread in the forum created by Peter.

- Hannes currently plays 'Indiana Jones - the video game' in his spare time and he has created a thread in a gamer forum about this game, where he collects tricks how to finish particular levels or how to gain extra points and so on. Hannes wants also other users playing this game to read and contribute to this thread. However, he does not want to have spoilers from people who already reached a higher level in the game than he has. Since he cannot control whether the content that someone wants to post is serious information about a higher level, he decides to allow only people who can proof to have the same or a lower level than Hannes to post entries in the thread. Of course, if Hannes finished another level successfully, that should be considered for the access control rules automatically.
- Mariangela owns a wiki site about dogs and allows only people with a reputation value higher than '4.6' writing access to the site. In addition, Mariangela wants all contributors in advance to sign a legally binding privacy statement that they are not going to post any personal data such as names, addresses or telephone numbers of others (e.g. dog breeders, vets...).

Success Conditions:

- User is able to specify access control rules based on dynamic properties of others (resp. a dynamic group)
- User can specify access control rules based on dynamic properties of himself (others need to proof properties relative to his one)
- Revoking of credentials is possible, i.e. Joshua is denied access to the thread after the friendship is finished
- User is able to specify legal privacy rules for the contributions to her workspace (in compliance with the general terms of use of the application)
- All rules will be enforced

Failure Conditions:

- User cannot define access control rules based on dynamic properties of others
- No revocation of credentials, i.e. Joshua can access the thread after the friendship is finished
- The creator of the resource herself is no longer able to access the resource and to edit the policies
- Creators cannot define legally binding rules for the contributions to their workspaces
- Creators can define legal privacy rules which are not in compliance with the general terms of use

Additional Questions and Remarks:

- How legally binding would such a statement from Mariangela, a 17 years old girl, in fact be? This question will be treated in the context of chapter 6 on legal requirements.

Mechanisms:

- Access Control Rules
    - Requirements: Hannes should be able to define conditions (access control policy) for reading access to his thread. Hannes should be able to define conditions (access control policy) for writing access to his thread.
- Credentials

    - Requirements: Hannes should be able to specify mandatory attributes (credentials) and a value for comparison. That value for comparison can be changed continuously, and is updated automatically. Checking of the defined conditions is done automatically each time a user wants to have reading or writing access to the thread.
- Legal privacy statements
    - Requirements: Users can define legally binding privacy statements in compliance with the general terms of use of the application (if there are any) when creating a new workspace (*thread, wiki site*...)

3.4.4 UC_cw4 - Set Access Control Rules for a Number of Resources

Goal:

- Illustrate necessity to define access control policies for a (undefined) number of forum threads

Preconditions:

- Threads have some meta-data, e.g. creator, date of creation

Scenario:

- Hannes has created a number of threads in the gamer forum about online games and gambling. Now he realises that a colleague of him, Alice, is also browsing the forum. She seems to be looking for a computer game as a birthday present for her daughter. However, Hannes does not want her to know that he is such an eager online gamer. He realises that he has posted a lot of personal experiences and stories from his personal life in the forum. Unfortunately he cannot remember which nicknames he used in all the different threads and if he maybe has offered too much identifying personal details during some discussions. Therefore he decides to close every thread that was created by himself for access by others immediately and reduce the number of his postings that are available to the public.
- Ines created a few threads in the past that lead to a brainstorming and discussion about new ideas for marketing concepts for several insurance packages. The discussions were quite fruitful and Ines company wants to realise one of the concepts. In order to reduce the risk of attracting the interst of competing companies for the ideas in her threads, all threads created by Ines within the the period between June 2008 and January 2009 should no longer be accessible for anybody, except Ines and her colleagues in the insurance company.

Success Conditions:

- User is able to specify the same access control policies for a number of contents with specified properties (creation date, creator...) at once
- User can specify same access control policies for a number of contents that are existing and also that will be created in the future

Failure Conditions:

- User needs to specify access control policy for each content seperately
- Creator of the content herself is no longer able to access the content and edit the policies

Additonal Questions and Remarks:

- Should it be possible for the creator of a workspace to change access control settings to contributions that were collaboratively created by more than one author? Refering to the scenarios the question is, whether Hannes / Ines as creator of a thread should have the right to restrict access to this thread so that others were no longer able to access at least their own contributions?

Mechanisms:

- Awareness
    - Requirements: Hannes should be able to be aware of what information he has disclosed in the forum and to which audience.
- Access Control Rules & Management
    - Requirements: Hannes / Ines should be able to change access control rules. Changing of access control rules should be possible for a number of contents at once.

3.4.5 UC_cw5 - Unlinkability between CWs Users and their Civil Identities (Non-Profiling)

Goal:

- Illustrate necessity for some pseudonymity of users in order to prevent surveillance by providers of CWs

Preconditions:

- Provider of the wiki can relate nicknames of users to civil identities

Scenario(s):

- Hannes' company in Germany introduced a CWs application for all of their 400 salesmen in order to work jointly on the new corporate design and the new sales strategy for netbooks. Hannes is not very fond of the idea of receiving a login and having to add comments and making suggestions for marketing ideas in a wiki. Not only does he prefer discussing ideas face to face and is simply not experienced in using a collaborative workspace. He is also worried because his company has been affected severely by the current economic crisis and the management has announced to cut jobs. Hannes fears the CW may be used by the company to closely monitor the employees' quality and quantity of work. He spoke to friends recently who work in another retail store chain. Since a CW had been introduced in their company, inconvenient and unpopular colleagues got fired for flimsy reasons and the management is known to monitor all steps taken on the CW. Hannes would endorse the idea of working jointly in a CW if the users could remain anonymous to the employer.

Success Conditions:

- employee representatives must be included in setting up SNS/CW and in setting the access rights and purpose

- employer cannot in genral relate nicknames in the wiki to civil identites of their employees

Failure Conditions:

- employer controls role and access management
- employer can fully identify and track any steps taken by employees (in public SNS it is often possible to remain pseudonymous, and the service provider is usually not interested in uniquely identifying the user; to meet the service provider's business case it is sufficient to profile usage and preferences of the user)

Additional Questions and Remarks:

- Employee is subordinated due to employment relationship
- Fully monitoring employees' performance is unlawful (in Germany)
- Logging of CW use can be permissible if it is necessary for technical reasons
- Access to log files must again be logged to allow later scrutiny
- How can access to the log files be organised in a privacy-respecting way? (cf. proposed solution in UC_sns9)
- Assuming that the employers use pseudonyms. If someone has a very valuable idea in the wiki and wants to cover hiself with glory also under his civil identity, is there any possibility to proove undoubtfully the civil identity of the person considered without losing any privacy features?
- Scenario refers to German case law and its interpretation of [Art.29 WP 55] (see also Chapter 6).
- From a legal point of view, in Germany it is not allowed to observe employees in their workplace in general. Only if there is a concrete and reasonable suspicion that the interest of the employer to run his "business efficiently" is endangered and preferably an intermediating third party, e.g. the data protection officer of the company, is informed, exceptions to this rule are possible.

Mechanisms:

- Pseudonyms, Anonymous Communication
    - Requirements: Hannes (and all of his colleagues) can choose a nickname. The provider is not able to link nicknames with real identites (e.g. by using the IP as an identifier).

3.4.6 UC_cw6 - Legal Liability of the Provider

Goal:

- Illustrate conflict between full privacy for users and content created by them and the legal responsibility of the provider

Preconditions:

- Forum has a central provider and provides fine-grained access control mechanisms, that allow groups of user to deny the provider access to their threads and the content posted there
- Provider is located in Germany.

Scenario(s):

- Florence was accepted to access a thread about Babysitters in a forum. The members exchange their experiences with babysitters and warn others if someone is really unacceptable. Since they share a lot of personal data, especially some information about their kids, the thread is not open to the public and also not accessable for the provider. One day, Florence finds a racist entry and informs the provider about this posting. According to the German law, the provider has 24 hours to remove the entry considered in case the claim by Florence is true.

Success Conditions:

- Entries can be deleted by the provider within the given time frame in case and only if it contains unlawful content

Failure Conditions:

- Provider cannot check whether the claim about unlawful content is true or not
- Users can notify any posting as unlawful (even if it is not) just to violate the privacy of the posting

Additional Questions and Remarks:

- Messages that are in compliance with the law and the rules of the board, however not liked by a particular user, should not be deleted by the provider. Otherwise this would support some kind of censorship.
- Provider needs to be able to fulfill the requirements from legislation, i.e. delete unlawful content.
- Provider should not be able to abuse a potential "emergency"-access option to content that else is not accessible for him.
- What are the differences in legal regulations with regard to the responsibility of the provider among different countries (EU, worldwide)?

Mechanisms:

- Access Control Management
    - Requirements: Florence is informed what attributes (credentials) are requested in order to access the thread. Florence can get the proof that she has these attributes.
- Access Control Rules
    - Requirements: Access to the thread is denied to all people who cannot prove they have the requested attributes, access can also be denied for the provider.
- Notification Feature
    - Requirements: It is possible to notify the provider (data controller) about content that is not in compliance with the law.
- Deletion / blocking of particular content
    - Requirements: Provider (data controller) can check the particular content and delete unlawful paragraphs, (or at least mark the entry as deleted and keep it as evidence of the unlawful behaviour)

3.4.7 UC_cw7 - Management of (Partial) Identities

Goal:

- Illustrate the requirement of a global partial-identities management module for privacy-enhancing identity management (PE-IDM).

Preconditions:

- Forum that allows browsing, contributing and creating new threads
- Different SNS allowing creation of connections to other persons
- Wiki allowing for differentiating between different namespaces

Scenario(s):

- Ines is a person having very wide interests. In order to exchange her experiences as well as to receive new information regarding her interests, she makes intensive use of different networking applications. Thus, Ines together with her colleagues use a wiki to collaboratively work on content related to different projects in the company. Further, Ines is member of a business-related as well as of a rather personal SNS where she regularly visits her profile and connects to others with similar interests. Besides these applications, Ines uses also different forums addressing topics of her interests.
- Since one of Ines's many interests is protecting her privacy, she tends to present herself in these applications using different pseudonyms and partial identities. In fact, she even differentiates between different sub-topics and actions within one and the same applications (e.g. separate threads of a forum, different wiki pages addressing the different projects; browsing content, contributing content, creating new topics/threads) when partitioning her identity. At the same time however, she is also interested in being recognizable within certain contexts, e.g., contributions to a particular thread in a forum should be performed using one and the same pseudonym. Since, remembering that many different partial identities together with the contexts in which they were used is a nearly impossible task, Ines needs support in selecting the right partial identity or creating a new one according to the particular situation, respectively.

Success Conditions:

- User is enabled to partition her identity into individual partial identities
- User is able to specify the granularity of usage spaces (contexts) for which she represents herself with one partial identity, i.e., context dimensions may be the application (e.g., for SNS), a namespace or a topic (wiki/forum), a single contribution (wiki/forum).
- User is supported in selecting partial identity corresponding to the particular context (i.e., forum thread/topic, wiki namespace, SNS group).
- User can specify rules for which usage spaces which partial identity should be selected by the systems

Failure Conditions:

- User cannot partition her identity into different partial identities with the applications she uses
- User cannot self-determine the granularity of usage spaces for partial identities
- User is not supported in partial-identity selection
- User cannot specify rules for automatic mapping of usage spaces to specific partial identities

Mechanism:

- Partial Identities and Pseudonyms
- Context recognition and management
- Decision suggestions with regard to selection of partial identity
- User Interface
- Awareness

3.4.8 UC_cw8 - Awareness and Selective Access Control

Goal:

- Illustrate the interplay between awareness information and the use of fine-grained access control options that can be defined by the user

Preconditions:

- Forum provides awareness information with regard to privacy
- Forum provides options for users to define rules for access to their postings

Scenario(s):

- Hannes is user of a forum where several different topics can be discussed. In general, everybody is allowed to contribute there without having to register. All users are made aware of the fact that they are linked with an IP address, and thus e.g. when Hannes asked in a thread where to get a new computer game, nobody posted a link to an illegal download portal for instance. Further, the interface of the forum provides a hint that potentially everybody on the internet can have access to the contributions of the forum, if users have not specified selected rules for access. In the health category of the forum, Bob created therefore a thread where only men can discuss their weight problems, i.e. Bob has defined that women are not allowed to contribute or even to read the postings in this thread. Hannes, who is a bit overweight, wants to find a buddy for the fitness center around the corner. Therefore he describes his weight problem, his time constraints due to work and family and which fitness center he is member of. Since Hannes does not want everybody to know about these facts, he only allows others who are already member of the same fitness center to read his posting in order to find a buddy for training together and motivating each other.
- Inga reads in the category "local journalisms" in a forum. She can access this category only because she is an official journalist. Inga is interested in what news-readers think about their local journalists and wants to start a new thread. A hint on the forum tells her, that the new thread she is going to add to the forum will only be visible to journalists. Since this restriction does not match with the target group Inga has in mind and she aims for more publicity, she opens the thread in another category in the forum, that is open to the public and does not restrict this access rules for her thread.

Success Conditions:

- User is aware of the privacy level (with regard to identifiability, audience) provided by the application
- User can define the potential audience / interaction partners for his contributions
- Rules for access are enforced

Failure Conditions:

- No selective access control settings possible
- No support for the awareness of users regarding current access control settings
- User can only choose between a few "audiences" predefined by someone else (e.g. moderators, admins)
- Rules are not enforced

Additional Questions and Remarks:

- How usable / handy / convenient is a forum that allows access control on the levels of categories, threads, and even single postings?
- Does awareness information really make users to "want" to define access control to their contents?
- Is it possible to really implement such an access control system (with a number of policies that need to be evaluated) for a social application without decreasing performance to an unacceptable degree for its users?

Mechanisms

- Awareness
- Access Control Policies / Management

3.5 Summary of Privacy Enhancements in Access Control

Awareness and data control:

> It should be easy for a data controller to understand what data he/she controls, what is available to whom in which context. A choice of improved Access Control Policies, and in some cases of Data Handling Policies - that may travel along with the data as sticky policies -, is a first step to achieve a better data control in social networking sites and collaborative workspaces.

Transparency:

> The flow of information triggered by a given action accessing some data must be transparent to the user: what is logged, monitored, and/or sent to another party must be known before performing the action.

Enforcement of Data Handling Policies:

> Data Handling Policies attached as metadata (sticky policies) may act as a way to enforce digital rights set by the data owner or controller. Such a mechanism could be integrated into a system similar to digital signatures. Access control rules can be embedded as a Data Handling Policy (e.g. must not be shared with other parties, must not be viewed by a user under 18, etc.).

Anonymity protection:

> Access to given data must not jeopardize anonymity choices. A number of anonymous actions or communications can take place using anonymous credentials,

even in contexts where identifying data is currently used for access control purposes. In the context of Social Network Sites, some features are incompatible with fully anonymous profiles, of course, but as described in this document, some use cases actually require the anonymity feature.

Confidentiality:

Security of communications is a key feature for anonymity protection but also for ensuring the confidentiality of content.

Partial identities / Management of partial identities:

When users have several identities on the same or different sites or workspaces, there is a linkability risk through access to some information shared between those identities, including connections to other people. Partitioning of personal data into different subsets, so-called partial identities, helps to reduce linkability. An identity management supports the user in creating, managing and deleting her/his partial identities.

Deletion:

Users have a right to deletion of their profile or contributions (content that is personally identifying or not). It must be possible to know before posting any data which deletion policy will be applied and preferably choose a relevant policy, depending on who the data controller is.

Encryption:

The data within the platform may be better protected through encryption. This encryption may apply to several data sets, including raw data posted by the user and secondary data generated by the interactions of the users with the platform (e.g. communication patterns).

3.5.1 SNS Use Cases: overview of identified mechanisms

- Authentication, e.g. through a membership of access control list, when logging in (UC_sns1, 2).
    - In case of mobile SNSs, the application (plugin) should be sure that the REAL user is being identified using a REAL location. This issue should be considered with regard to the question to what extent users should (not) be allowed (a) to fake their identity, or (b) to fake their location. (UC_sns5)
- Definition of groups. The mechanism should support different levels, e.g. several groups next to each other, overlapping groups, subgroups (UC_sns1)
- Authorisation/rights management: granting and revoking read/write rights per (group of) connections (UC_sns2, 3, 4)
- Credentials. Only communication partners that have the right credentials (e.g. given to them when assigned to the group "Music lovers") can access/decode the information. Other parties cannot access/decode, or even find the information. (UC_sns3)
- Logging, perhaps based on access control mechanism (UC_sns4)
- Partial identities, because this would allow users to stay within the same SNS, without having to learn a new SNS, whilst playing different (unlinkable) roles on them (UC_sns6, 7)

- Credential based access control: a credential given by a third party (e.g. a certified medical doctor) should allow access to the site (UC_sns7)
- Data handling policies, applying to (a) content, (b) connections, (c) communication. (UC_sns8)
- Encryption and decryption (UC-sns9):
    - Of content communicated between 2 parties (sender/receiver).
    - Decryption by a combination of three parties that are NOT sender or receiver.
    - Encryption of the communication metadata, like time sent, length of message, etc.

3.5.2 CW Use Cases: overview of identified mechanisms

The CW use cases generates a number of mechanisms, that are patrially overlapping the mechanisms derived from the SNS use cases. Some legal and social requirements are also listed.

Technical

- Access Control Policies / Access Control Management (change access type, resources, conditions)
- Credentials (self-certified, certified by others)
- Anonymous communication
- Pseudonyms / Partial Identities
- Context recognition and management
- Decision suggestions with regard to selection of partial identities
- Deletion / Blocking
- Data Handling Policies / Sticky policies

Legal

- Legal privacy statements (natural language)

Social

- Awareness
- Notification Feature

Chapter 4

Issues

This chapter focuses on privacy and identity issues relating to the use of SNSs and CWs. The issues are compiled from various sources, including the PrimeLife heartbeat document H1.2.2 titled "Privacy and Access Control in Social Software" and a number of recent academic papers, that will be referenced in the respective sections. Together with the use cases in Chapter 3, the issues described in the following build a valuable basis for identifying a set of requirements for privacy-enhancements and privacy-respecting access control in SNS and CWs.

4.1 SNS issues and requirements

People have compelling social reasons to use SNSs, and those same social factors lead them to badly misunderstand the privacy risks involved. “Solutions” that treat SNSs as a rogue actor that must be restrained from sharing personal information miss the point that people use these networks *because* it lets them share personal information (see e.g., [Grimmelmann 2009] and [boyd 2007]).

Before diving into the requirements of privacy-enhanced SNSs, it is necessary to understand the character of the issues arising from the use of SNSs. As the following overview will show, there are different types of issues dealing with different aspects of (the use of) SNSs. The issues below are based on a number of sources, including [Grimmelmann 2009], [boyd 2007], [ENISA 2007]. In order to maintain structure of the encountered issues, they have been categorised in a number of subsections below. Some of the issues have been complemented with a requirement, because of the one-to-one relationship of the issue with a particular requirement. For other issues, the link between the issue itself and potential required solutions to meet the issue is not so straightforward. In those cases, an explicit requirement is not stated.

4.1.1 Identity and relationship

IS1 Social convergence

Our social roles are contextual and audience-specific—but when multiple audiences are present simultaneously, it may not be possible to keep up both performances at once

[Goffman 1959]. One of the primary issues is that the networks offer hardly any mechanisms for creating and maintaining relevant social contexts.

- RS1: The SNS should facilitate methods for creating and maintaining useful (social) contexts (e.g. personal lists of connections) within a user account (profile) and have proper access control to information according to those contexts.

IS2 Sociability paradox

By choosing to make their profile private, users are able to select who can see their content. This prevents unwanted others (parents, teachers, etc) from lurking, but it also means that peers cannot engage with them without being invited as Friends. To handle this, teens are often promiscuous whom they are willing to add as Friends on the site. A similar issue exists on dating sites where users want to be able to find similar souls without revealing too much of themselves before establishing a connection.

- RS2: The SNS should facilitate users with similar interests to connect without revealing personal data until after a link is established.

IS3 False sense of security

SNSs systematically deliver users signals suggesting an intimate, confidential, and safe setting. These signals support the creation of an atmosphere of confidentiality and intimacy that entices user to share more information than they might in other, more formal settings. Users are confusing Gesellschafts and Gemeinschafts [Tönnies 1965]: some (parts of the) networks are Gesellschafts, some are Gemeinschafts, and treating a Gesellschaft as a Gemeinschaft creates a false sense of security.

- RS3: Users should have control over social contexts and be able to create different kinds of context relating to distinctions such as Gemeischaft v. Gesellschaft.

IS4 Eagerness to connect

Social inclusion and a need to be considered popular are deeply ingrained in us. This is what SNSs exploit. Many users accept invitations to become friends from perfect strangers as shown by a study by a security vendor that some 60% of the users were willing to add a plastic frog as a contact, thereby leaking personal information to it [Sophos 2007]. At TILT we have found similar results in a study we conducted (with an empty profile).

- RS4: Users should be able to assess the proposed new contact prior to committing to a connection.

IS5 Unauthorised access

The best-known examples of unwanted disclosure on social network sites involve students acting their age and being called out for it by authority figures, such as the college student who lost the chance for a summer internship when the company's president saw that his Facebook profile lists "smokin' blunts" as an interest [New York Times 2006].

- RS5: The SNS should offer proper access control to the profile data.

IS6 Fading relationships

The intensity of relationships we maintain in everyday life fluctuates. One time close friends get out of touch and consequently they learn less and less of our current activities. In SNSs, everyone within a particular social group is attributed the same 'intensity', i.e. treated the same regarding to access to our information. This is in a sense not a bug, but a feature of SNSs: it provides users a simple way to get back into the social loop whenever they want. Yet on the other hand this faculty of instant revising of

relationships poses issues because it may be difficult for the individual to manage both manifest and latent relations. Demarcating active and passive relationships may facilitate privacy and identity management.

- RS6: The SNS should provide ways to move inactive relations to social groups more distant from the user (less access rights).

IS7 Instability of (social) norms

One of the most disruptive things a social network site can do is to change the ground rules of how personal information flows — and social network sites do this a lot. The norms regarding proper behaviour with respect to information a user can see are blurry and change over time and not clear to the reader.

- RS7: The SNS should offer mechanisms for the user to specify data handling policies to be respected by human readers and machines.

IS8 Simplistic models

Everyday relationships are often implicit. Social network sites require explicit representation of social facts. What aggravates this problem is that humans have problems to manage privacy using rigid ex ante rules. We think about privacy in terms of social rules and social roles, not in terms of access control lists and file permissions. The use cases described in the previous chapter are also of a fairly simplistic nature, but their aim is to allow for more nuances than currently possible in SNSs, and should be considered as an intermediate step in the continuous development towards SNSs that are more aligned with human social interactions.

- RS8: The SNS should offer models for relationships, policies, etc., that mimic everyday human social interactions.

IS9 It's not what it seems

The inferences made by applications such as Facebook's Beacon do not reflect the 'truth'. Not everything I buy or do online reflects me as I'd like to be seen; I occasionally buy articles for others, so my purchasing behaviour as observed by a Beacon affiliate may not correctly represent 'me'.

- RS9a: The SNS should provide users with tools to inspect (and correct) the automated inferences made on the basis of their behaviour in the network.
- RS9b: The SNS should provide possibilities to prevent automated observations, at least by provinding an opt-out option.

IS10 Persistence of identity

Users wishing to delete accounts from SNSs find that it is almost impossible to remove secondary information linked to their profile such as public comments on other profiles. Platform providers have an incentive to keep the profiles (even if they are dormant) for economic reasons.

- RS10: The SNS should offer users the option to terminate their SNS identity which should result in deletion of all data pertaining to this user in the SNS.

IS11 Profile non-portability

One of the reasons why current SNSs do not offer the users the privacy protection they deserve is that the SNS sphere is an imperfect market. There are severe lock-in effects due to the fact that the value of the network is in the network itself. Individual users harm their social capital if they move away from a network they have invested in. Their relations have to move as well.

- RS11a: The SNS should offer users means to export their profile and network (relations) to other SNSs.

- RS11b: A global identity management should be provided, that support users in maintaining relationships across a number of SNSs.

4.1.2 Lack of risk awareness

IS12 Implicit information leaks

Information is leaked implicitly through network data. If one attends Barnett College, many of your Facebook contacts probably attend Barnett College too. Even if you don't list a trait on your profile, it may be possible to infer it statistically by looking at the values others in the social network list. Researchers using a simple algorithm on LiveJournal were able to predict users' age and nationality with good confidence in many cases simply by observing the age and nationality of their contacts.

- RS12: The SNS should provide mechanisms that allow the user to see what implicit information leaks may occur (transparency tools).

IS13 Living on the edge

[Edwards & Brown 2009] flirt with the idea that default "privacy settings be set at the most privacy-friendly setting when a profile is first set up," only to recognize that "this is not a desirable start state for social networking." If Facebook profiles started off hidden by default, the next thing each user would do after creating it would be to turn off the invisibility. Social needs induce users to jump over technological hurdles. We have to take into account that studies show that a proper sense of risk is only completed when people reach the age of about 25 [Reyna and Farley 2006]. Throwing information about potential risks at teenagers only has limited effects.

- RS13: The SNS should provide information about risks associated to certain behaviour in an empathy encouraging or empathy understanding way.

4.1.3 Surveillance

IS14 Surveillance

Awareness that one is being watched can be connected to "anxiety and discomfort . . . self-censorship and inhibition," even "social control." is one of the longer term issues. As one stalker puts it in Grimmelmann: "With close friends, it is always OK to comment on their profiles; they expect it and might even be upset if you don't. With distant acquaintances, it is almost never OK. It's those in the middle that are tricky; it's OK to bring up their profiles only if there is a reasonable explanation for why you were looking at it in the first place." [Grimmelmann 2009]

- RS14: The SNS should offer mechanisms for the user to see who has accessed their data.

IS15 Advanced monitoring

Face recognition: user-provided digital images are a very popular part of profiles on SNSs. The photograph is, in effect, a digital identifier for the user, enabling linking across profiles, e.g. a fully identified Bebo profile and a pseudo-anonymous dating profile.

Content-based Image Retrieval (CBIR) is an emerging technology which can match features, such as identifying aspects of a room (e.g. a painting) in very large databases, increasing the possibilities for locating users.

Linkability from image metadata: many SNSs now allow users to tag images with metadata, such as links to SNS profiles (even if they are not the owner/controller of

that profile), or even e-mail addresses. This leads to greater possibilities for unwanted linkage to personal data.

- RS15: The SNS should prevent the use of profile information for surveillance purposes

IS16 Permeability

Digital dossier aggregation: profiles on online SNSs can be downloaded and stored by third parties, creating a digital dossier of personal data.

- RS16: The SNS should prevent the possibility of unauthorised download of profile information.

4.1.4 Curious providers

IS17 Panoptic providers

The platform provider has a reasonably comprehensive snapshot both of who the user is and of who they know. This information is used for targeted advertising and other profiling uses. Also humans use the profile data. If some accounts in the blogosphere are to be believed, Facebook has trouble controlling its own employees, who treat access to profile and user-activity information as a "job perk" [Douglas 2007].

- RS17: The infrastructure should make it impossible for the SNS provider (and its employees) to have access to the data of the users.

IS18 Secondary data collection

As well as data knowingly disclosed in a profile, SN members disclose personal information using the network itself: e.g. length of connections, other users' profiles visited and messages sent. SNSs provide a central repository accessible to a single provider. The high value of SNSs suggests that such data is being used to considerable financial gain.

- RS18: The infrastructure should make it impossible for the SNS provider (and its employees) to have access to the collected secondary data of the users.

IS18a Data ownership

In general, the question remains who owns information uploaded to an SNS. Differences between legal systems come to the fore when discussing this item: US based SNSs will generally be able to claim that all personal information, once released, becomes the possession of the SNS provider, where European companies will have to revert to a licensing model, in which the SNS provider is granted the right to use the information provided for other (commercial) purposes. In all cases, the Terms of Use will specify to what extent information ownership is transferred to the SNS. The issue remains that the SNS user must be made aware of any transfers of data ownership when uploading content to the SNS. Moreover, this provision is also valid for secondary data generated whilst interacting with the SNS.

- RS18a: The user must be made aware who owns data uploaded to the SNS, and who owns information generated through the use of an SNS.

4.1.5 (Risk of) illicit use

IS19 The user as data controller

Users post information (text, photos, videos) involving or about others both on their own profile pages, and that of other users. It is likely that the legal status of those disclosures is that the profile owner that publishes the data is to be regarded a data controller, meaning that they have to comply with the data protection directive provisions,

including purpose specification and legitimate ground for processing (which includes asking permission of the involved data subjects). This is hardly ever done. Since the role of data controller is virtually never put into practice, many people appearing on unfavourable pictures want to take action themselves. Examples of measures these people may take are requesting the uploader of the concerned content to remove it from the public view, or to remove identiftying features from it (e.g. tags containing names or mail addresses).

- RS19: The SNS should offer proper mechanisms to assist users in getting consent of those involved in the content they publish.
- RS20: The SNS should provide mechanisms for users to retract their consent to publishing data pertaining to them and have data removed.

IS20 Denigration

Since an SNS user's identity is social—it inheres in the impressions she gives and gives off to others—she runs the risk that someone else will mutilate it. If so, then the dignitary side of her privacy interest has been harmed.

- RS21: The SNS should provide users the means to make their own code of conduct or house rules for their 'friends'.
- RS22: The SNS should provide a code of conduct for its users.

IS21 SNS spam

Unsolicited messages propagated using SNSs. This is a growing phenomenon with several SNS-specific features.

- RS23: The SNS should offer mechanisms to manage/limit the distribution of unsolicited messages.

IS22 SNs aggregators

'SNS portals' integrate several SNSs which multiply vulnerabilities by giving read/write access to several SNS accounts using a single weak authentication. An examples of an SNS aggregator is 2009.

IS23 Spear phishing using SNSs and SN-specific phishing

Highly targeted phishing attacks, facilitated by the self-created 'profiles' easily accessible on SNSs. SNSs are also vulnerable to social engineering techniques which exploit low entry thresholds to trust networks and to scripting attacks which allow the automated injection of phishing links.

IS24 Profile-squatting and reputation slander through ID theft

Fake profiles are created in the name of well-known personalities or brands or within a particular network, such as a school class, in order to slander people or profit from their reputation.

- RS24: The SNS should require proof of identity before allowing someone to publish their own profile.

IS24a Prosecution of SNS users based on uploaded content

When proof of identity is made compulsory in order to meet the previous issue, the opportunity to voice opinions anonymously is drastically reduced. Freedom of expression may require a certain level of anonymity, at least to such an extent that contributors should not fear to be prosecuted. This leads of a requirement that diametrically opposite to the previous requirement.

- RS24a: The SNSs should provide a certain level of anonymity to its members.

IS25 Stalking

Cyberstalking is threatening behaviour in which a perpetrator repeatedly contacts a victim by electronic means such as e-mail, Instant Messenger and messaging on SNSs. Statistics suggest that stalking using SNSs is increasing.

IS26 Bullying

SNSs can offer an array of tools which facilitate cyberbullying (i.e. repeated and purposeful acts of harm such as harassment, humiliation and secret sharing).

IS27 Corporate espionage

Social engineering attacks using SNSs are a growing and often underrated risk to corporate IT infrastructure.

4.2 CW issues and requirements

SNSs focus on identities of the participants and the social networks they construct. In contrast, collaborative workspaces concentrate more on the contents of the contributions of the individuals participating in the CW than on the identities of the participants. Nevertheless, CWs come with their own set of issues that are similar to the ones listed in the previous sections, but differ because of the change of focus. The limited number of issues particular to CWs did not merit a subclassification.

IC1 Awareness of potential audience

Collaborative workspaces are available and easily accessible on the Internet. This is preferable from a social point of view in the sense that everybody can participate and communicate with many other users. From a privacy perspective this means that all personal data that can be included in the user's contribution (e.g., personal ideas and experiences described in a forum posting) are easily accessible by anybody. We argue that users of CWs are not always aware of the potential audience to which they are disclosing their personal stories. Users think about the active members of the community, but forget about the potential broad audience of "silent readers". Making users aware of the broad potential audience supports the realisation of the right to control to whom personal data is disclosed (cf. [Directive 95/46/EC]).

- RC1: CWs should provide features for the awareness of users about the potential audience of their contributions.

IC2 Accessibility of contributions

Even if users would be aware of the potential audience, in currently available collaborative workspaces they have barely any options to self-determine access to their contributions. Instead, e.g. the moderator of a forum or of a certain topic specifies the access policies. Thus, the only chance the users have is not to contribute to the collaborative content. This, however, is not desirable since user participation is essential in forums.

- RC2: CWs should provide options for users to define access control rules to their user-generated content in a privacy-respecting way.

IC3 No user control over contributions

In currently available collaborative workspaces, it is usually up to the provider (incl. technical administrators, moderators) to decide how the user generated content is used (e.g., contextualised advertisements).

- RC3: CWs should allow users to control secondary use of their contributions.

IC4 Deletion of personal data

A thoughtless posting once created in a CW may remain on the Internet for many years and can be copied and retold several times.

- RC4a: CWs should provide options for users to remove all copies of their contributions (which is very hard or even impossible to realise in practice.)
- RC4b: CWs should provide options for users to specify a time period after that their contribution is deleted or marked as out-dated.

IC5 Social engineering attacks

Many forums do not require any proof of identity in order to become a member of the forum. This is good from a privacy perspective since it allows users to keep some anonymity. On the other hand, it is easily possible to create a false identity, i.e., to pretend to be someone else, in order to spy on other members of the forum either in public threads or via private messages.

- RC5: CWs should provide a privacy-friendly solution to prevent the abuse of other's identities (e.g., trusted third party that certifies the identity of users).

IC6 False sense of privacy

Not having to provide any proof of identity gives people a feeling of high privacy in the sense of anonymity. Many of them don't know that providers or authorities are able to identify them anyway, at least under special circumstances (e.g., requested by law, creation of anonymous profiles for marketing purposes,…).

- RC6: CWs should support the privacy awareness of user by informing them about their actual level of privacy (e.g., identifiablity of the user from the perspective of service providers).

IC7 Social Embarrassment

With the opportunity to create a false identity and a feeling of high privacy, adversaries are enabled to participate in collaborations in an inappropriate way, e.g. offending other users, post unlawful content, etc. and in this way embarrass the person whose civil identity is abused.

- A possible solution may include RC5 and RC6.

IC8 Surveillance of users

Many users tend to use the CW over a longer period in their life. Throughout their contributions they disclose a lot of personal thoughts, wishes, experiences and probably even information about their family, friends, and colleagues. Tracking all contributions of particular members over a given period of time will give a potential adversary a comprehensive view about their life, interests, health, their job, their family and friends, their beliefs and so on. Thus, someone may build a more realistic impression of a person through surveillance of contributions than an explicitly created profile would otherwise offer. This issue gets worse when considering that users tend to re-use identities in different applications. This allows for unwanted linkability not only of activities (i.e., the user's usage patterns of web applications), but also of contributed content to these applications by the users.

- RC8: CWs should provide features for creating, managing and deleting different partial identities in order to reduce linkability of all actions of the same user.

Chapter 5

Mechanisms

Mechanisms function as the linking pin between the use cases and the actual requirements. In some cases it is possible to make a direct connection between a description in a use case and a (technical) requirement that must be met in a functional solution in order to enable the use case. The majority of use cases, however, express a high level of ambiguity which explains why the intermediate step of mechanisms may prove to be quite effective. Moreover, the identified mechanisms provide a focal point that allows the concentration of disparate issues into a limited number of mechanisms. Finally, the overview of mechanisms delimit the amount of possible requirements and therefore the scope of an implemented prototype.

This chapter starts with scoping the topic of Mechanisms within the wider context of PrimeLife. The subsequent section reminds us of the central role of access control in privacy enhancement, which is the leading theme within the current work package. The remainder of the chapter deals with a number of identified mechanisms that can be employed to provide privacy-enhancing access control in social networks and collaborative workspaces.

5.1 Scope

The primary scope of this work is privacy enhancement through improved access control mechanisms and policies. In the PrimeLife project, Activity 5 work packages cover the policy language level requirements, in particular expressivity of access control policies in a future policy language. The following requirements will not go into details about policy language for privacy-respecting access control since this is already gathered in PrimeLife Activity 5. Some of the features mentioned in the Use Cases chapter involve trust and reputation mechanisms. This document does not cover these mechanisms since PrimeLife work package 1.1 is focused on them.

The contribution of this heartbeat document is mainly in the field of privacy-enhancements for social networks and collaborative workspaces by developing requirements for privacy-respecting and user-controlled access control mechanisms. Further, mechanisms for supporting awareness of these features among users of both types of applications is also considered.

5.2 Overview about Mechanisms

5.2.1 Access Control Policies

The following definition is in the PrimeLife heartbeat document H5.1.1: *An access control policy (ACP) protects access to an object by specifying which subjects should be granted which type of access to it. The object being protected can be a piece of data like a file, a database record, or a webpage, but it can also be a more abstract functionality like a service or a remote procedure call*. Several privacy-enhancing features can be added when designing access control mechanisms in SNSs or CWs, where the objects include profile information and contributions as well as privacy preferences themselves.

Access based on identifier

Commonly used identifiers in SNSs and CWs are user names. Enabling privacy in some use cases rely on anonymization of the user name. In SNSs, the user name is very often the real name of the person, which prevents some anonymous actions and communications. An anonymous identifier enables the ability to combine an anonymous partial identity with identifying partial identities.

Access based on role

Many CWs already set up different classes of roles for access control. However, transparency and usability can be improved so as to give the user a better view over 'who controls what'. In SNSs, some community-based scenarios can also take advantage of the definition of roles in addition to groups (see below).

Access based on groups

A group is a collection of individuals, i.e. of identifiers. The group itself has a meaning for the person defining the group and/or for the individuals joining the group. Individuals can have a role inside a group, e.g. chair, administrator, user. Access control can vary for different roles in a given group. Technically, a group can be used as a basis to collectively give or remove access to a resource.

Access based on properties

Attributes of the subject and properties of the object can be used to define access control rules. Attributes of the subject can be proven by the way of credentials, that enable anonymity and possibly involve trust mechanisms with a third party. Properties of the object (resource) often modify rules (e.g. content must not be viewed by users under 18) and trigger a requirement on the subject's properties. A reputation mechanism may add a reputation property to a subject.

Access based on context

Context include time (e.g. date when user joined a group), events (e.g. acknowledgement of permission to access), location and sometimes jurisdiction. Other user-independent context properties can also modify the application of access control rules (processor load, etc.)

An Access Control List (ACL) is a list of rules that can combine identifiers, groups and roles. ACLs can be combined themselves to determine the access control rule for a given resource. For example, in a resource accessible to group X, a data controller can set an ACL restricting write-access to persons having the role of administrator and who are also members of a group Y. In that case, non-administrators in group X would be denied write-access, as well as

members of group Y that are not in group X. Other rules (see below) can also be combined. ACLs that feature complex logical operators are one type of ACPs.

An Access Control engine for a privacy-enhanced SNS or CW framework should be able to process and enforce the access control rules deriving from these different features. On the client-side, a UI to define the corresponding advanced access control policies is required whenever the user should have the possibility to specify these for his/her data.

5.2.2 Data Handling Policies

The following definition is in the PrimeLife heartbeat document H5.1.1: *A data handling policy (DHP) is a set of rules stating how a piece of sensitive data should be treated. The data handling policy specifies, amongst other things, for what purposes the data can be used (e.g. research, marketing), to which third parties the data can be disclosed (e.g. all, nobody, only auditors), how long the data can be stored, etc. server-side data handling policies are sometimes referred to as obligations, client-side data handling policies are often called preferences*. In the context of social networks and collaborative workspaces, server-side DHPs include, in addition to server obligations, policies about the data controller and the deletion of information, not only personal data but also contributions that are not identifying but may be linkable. DHPs could be considered as client-side policies since in most cases the resource that has the policy associated to it is set by a client (user) when uploading the data onto the SNS or CW. Mechanisms required for data handling policies are:

1. a UI or similar client-side feature to define the policy and attach it to the data (as metadata)
2. a system to package and transmit the metadata and data together (e.g. an endpoint for a web service building and sending a SOAP message)
3. an enforcement system that reads the metadata and applies the DHP (e.g. require credentials to access the data itself).

While there is a variety of existing technologies to achieve steps 1 and 2, the achievement of step 3 is more complex and needs more research work.

5.2.3 Privacy-enhancement through new authentication mechanisms

New mechanisms for authority delegation are being deployed on a variety of web sites. For example, the OAuth protocol [OAuth 2009], built over HTTP, allows a user to grant access to a protected resource by a third party (consumer) through a given service provider. Prior agreement must have occured out-of-band about policies, including revocation of access. The basic idea is the delegation of authentication through a consumer that will be able to get access to a given resource at the service provider without giving any personal data from the user to the provider.

An example scenario is authorizing a photo sharing site to access a social network site's information about the user (e.g. photos that the user has uploaded into her SNS profile): The photo sharing site learns (from the user, or through a referral) about the URL of the user's SNS profile. The user is redirected to the SN site, where he can determine what information (if any) is given to photo sharing site users (consumers), and how long that authorization should last. The authorization is passed back to the photo sharing site, which can now process photo sharing information further. The user can revoke the authorization without collaboration from the photo sharing site. Anyone visiting the photo sharing site does not get information about the user's SNS profile at all. This kind of mechanism can be applied

whenever a user wants to access information without revealing his/her identity, i.e. every use case where the person is not getting access to his/her own data, but data from another source.

5.2.4 Identity management

Websites have traditionally managed identity in terms of a user name that uniquely identifies the user/account and an associated password. When faced with having to deal with user names and passwords for many different websites, it is human nature to use the same name and password. This not only reduces security, it also makes it easier to link accesses across websites.

More recently, a trend has emerged for websites to require the use of an active email address in place of a user name. This is easier for users, since they don't have to remember what user name they defined for this site. It also provides a mechanism for dealing with forgotten passwords, and as part of the account setup process, when an email, sent to the user, contains information needed to activate the account. The disadvantage is that email addresses are globally unique identifiers which make it easier to track users, with adverse effects on their privacy.

Single sign-on systems allow users to sign on once with an identity provider rather than once for each website they visit. This offers increased usability. One such system is OpenID where users identify themselves with a URI [OpenID 2009]. The relying website is then able to use this URI to obtain credentials about the user, including personal data. URIs make it easier to track users across websites, and the identity provider needs to be trusted by both relying websites and end-users.

A refinement of this approach is for users to disclose the URI for their identity provider rather than for themselves. This makes it easy for users to manage different identities for different websites, but still relies on trust in the identity provider. Users can even choose to use anonymous credentials that make it harder to link successive visits to the same website.

Privacy and Open Identification Providers

Recent work in decentralized identification providers, such as the OpenID protocol, must be taken into account in new SNSs and CWs. The OpenID protocol provides a framework for certain assertions about a user's association with a URI. It does not provide an independent cryptographic proof to the relying party that the user has indeed executed a certain protocol with the OpenID Provider. The establishment of trust between the relying party and the OpenID provider is out of the protocol scope. In deployments, the requisite policies range from accepting identities from any OpenID provider, through OpenID provider blacklists, to approaches where few (or only one) previously known OpenID providers are trusted. Privacy concerns focus on the ability of the user's OpenID provider to link user transactions with different relying parties. It should also be noted that OpenID can be used to pass along personal information; how the release of this information is authorized is up to the individual OpenID Provider's choice. Criticisms of OpenID center around certain aspects of the protocol design, and on risks that a malicious relying party might be able to successfully impersonate the user's OpenID provider.

The relative simplicity of many core aspects of OpenID - while easing deployment - will also be a challenge, as it might render the integration of advanced privacy enhancing technologies in the context of this protocol more difficult.

Partial identities

Many SNS and CW users have more than one profile on a given site in order to circumvent current limitations in the privacy features of those sites. There would be a clear benefit if a client-side application that manages various partial identities for a user would exist (cf. 2009). The client-side identity mangement should ensure that unlinkability of information can be checked and privacy-related risks could be revealed to the user. A trusted third-party could also serve as an identity provider and partial identity manager. However in that case other questions arise: trust would be a major issue, of course, but also secure and anonymous communications. A benefit would be the means to utilize and manage partial identities from different computers, e.g. when dropping into an Internet Cafe or using a mobile device instead of a desktop computer (see also [Spitz et al. 2008]). A further consideration is avoiding loss of data when the user's computer breaks down (or is stolen) since many people aren't very thorough when it comes to regularly backing up their data.

5.2.5 Use of credentials

Credential mechanism

A credential is a statement attributing a property to an identity, e.g. 'Alice is at least 18 years old'. The significance of the credential depends on the trustworthiness of the entity making the statement. Credentials may provide a mechanism to verify their authenticity and integrity, i.e. to detect forged or modified credentials. Credentials can cover an open-ended set of properties, e.g. age, occupation, gender, reputation, skill level in a game and so on. More complex credentials can be used to express what kinds of statements the subject identity can make.

Different technologies can provide credentials, built on software or/and hardware solutions. Privacy is not necessarily present in the credential-based mechanisms, some systems use personal data, even biometric data.

Anonymous credentials

Anonymous credentials can be used to for revealing properties of an individual without revealing the identity of that individual, e.g. to attest that X is a member of the group "employees" without revealing who X is. Anonymous credentials can't be linked across sessions. This is distinct from the use of an anonymous identity, where the same identity is used for multiple sessions, e.g. where a user of a collaborative website provides a pseudonym in place of their civil name.

5.2.6 Legal policy statements

A data controller should be able to add legal privacy statements in a Social Network or Collaborative Workspace. Such a legal privacy statement can be defined for a restricted context that the data controller defines, such as a group (see use cases UC_sns6 and UC_sns7). This mechanism brings attention on three essential requirements:

- ease of definition of such legal statements by a user without particular legal knowledge,

- ability to check that legal statement are not contradicting other statements in application, such as the terms of use of the SNS or CW,
- enforcement of the legal statement.

A first prototype of this kind of mechanism could support the presentation of verifiable and as much as possible technically enforceable simple policies along with corresponding legal statements to the data controller. Legal requirements will be covered extensively in chapter 6.

5.2.7 Encryption of content and communications

Although it is not common for web users to encrypt the data that they publish on a website, it may be the most trivial mechanism to protect data from unwanted access, even from the web service providers or the Internet service providers. Cryptographic software can be also used in the access control mechanism, in such a way that securing access control and the following transmission of data may be achieved within an integrated architecture. This implies that the encryption of content and communication is an approach that can be very effective in securing the privacy of social software users. When it is implemented in an all-encompassing way, it may provide a viable approach to limit the access of service providers/ISP to data stored and exchanged on the application.

The drawback this approach is that encrypted data is not searchable. Thus, it would be useful to rely on more enhanced crypto schemes. PrimeLife Activity 2 does research in this field.

From the perspective of Mechanisms (the subject of this chapter), the statement suffices that the availability of encryption of content and communication is desirable. The next step would be to draw up specified requirements concerning the way these mechanisms should be implemented, thereby quickly delving into technical intricacies. This is therefore not proposed, and the introduction of the need for encryption in the sense as it is described here, will not be further elaborated.

5.2.8 Awareness and transparency

In order to apply privacy-enhancing access control features effectively, users of collaborative workspaces and social networks need to know and understand what personal data they disclose to whom. Therefore the concept of privacy awareness and transparency tools is part of PrimeLife work package 2.2. Privacy awareness is defined as a user's perception, cognition and attention on whether others receive or have received personal data, which personal data others receive or have received in detail, who receives or has received personal data, and how these personal data is or might be processed and used. Transparency of (personal) data flows contributes to privacy awareness of users. Technological means to provide transparency - so-called transparency tools - can give information on intended collection and storage of personal data (ex ante) or enable the user to access stored data (ex post) or even allow for counterprofiling in order to "guess" how user's data matches relevant group profiles.

Chapter 6

Legal Requirements

6.1 Introduction

A list of legal requirements was originally prepared for the Prime project, where they can be found in full detail. The presented list of legal requirements is based on the set of Directives: general Data Protection Directive 95/46/EC [Directive 95/46/EC], the Directive 2002/58, commonly known as ePrivacy Directive [Directive 2002/58/EC], the Directive 2000/31/EC on Electronic Commerce and the Directive 1999/93/EC on Electronic Signatures [Directive 1999/93/EC].

Based on the legal requirements of the PRIME project [PRIME 2008], the section below will introduce three categories, which can be distinguished when addressing privacy issues in electronic environments. These requirements are applicable to all dealings with personally identifiable information, and are therefore relevant for SNSs and CWs. Due to the fact that these types of applications are relatively new, case law has only been developed to a limited extent. However, any SNSs or CWs must respect the provisions outlined in the discussed directives. Subsequent sections will address a number of specific instances of legal regulation applying to SNSs and CWs. First, the issue of the user as a data controller is discussed. The fact that members of SNSs and CWs have certain obligations as outlined in current legislation justifies a separate discussion on this topic. Next, the particular setting of the use of SNSs and CWs within corporate surroundings is discussed. This debate focuses on the tension between the expected right to privacy of employees and the justified interests of the employer. Finally, a section will be devoted to some aspects of the human computer interface (HCI) in SNS and CW applications, with special attention for the relevant legal requirements.

6.2 Types of legal requirements

The first set of requirements is based on the principles on processing of personal data. This process must be fair and lawful, abiding the law in each step of the process. Users must unambiguously consent to the processing of their personal data for a specified and legitimate purpose, in which only the minimum of information is used that is necessary to deliver the service agreed upon. Other principles that have to be met consider the data quality, and the

fact that the data should be stored for a limited period that is only long enough to provide the agreed service. When stored or transferred, the data should be secure and kept confidential, and the responsible national Data Protection Authority should be informed of the data processing taking place. Finally, the data subjects should have means to ensure that the their personal information is processed in accordance with the provisions outlined in the law.

- RL1: The application shall collect and process personal data in a fair and lawful way.
- RL2: Legitimate processing. The application shall base the processing of personal data on a legitimate ground (e.g. consent of the user required, unless one of the other grounds applies).
- RL3: Principle of finality / purpose limitation. The application shall use the personal data only for the specified and legitimate purposes.
- RL4: Principle of data minimisation. The application shall collect and process only the data that are adequate, relevant and not excessive for the specified purposes.
- RL5: Principle of data quality. The application shall use accurate and up to date information.
- RL6: Principle of conservation. The application shall keep personal data only for the necessary purposes, for which the data were collected.
- RL7: Principle of security. The application shall ensure the secure storage and transmission of personal data.
- RL8: Principle of notification to the Supervisory Authority. The data controller shall inform the national Data Protection Authority of the collection and processing of personal data.

Whereas the first set of requirements focused on the processing of personal data, the second set outlines the rights of the data subject. Providing the data subjects with those rights is intended to guarantee that they remain the ultimate controllers of their personal data. The starting point is that the data subject should be informed of who is going to do what and for what purpose to the collected information, thus also creating a possibility for a right to object to the proposed processing. A right of access also exists, enabling the data subject to rectify, erase or block certain parts of the data in cases where its processing does not comply with the requirements of the data protection directive (DPD). Finally, the data subject has a right not to be subjected to an automated decision and the right to seek legal relief, which may lead to compensation in case of damages.

- RL9: Right to information. The application shall ensure the data subject is informed before the processing of his data
- RL10: Right to object. The application shall allow the data subject to object to the processing of his personal data.
- RL11: Right of access. The application shall enable the data subject to get information regarding the processing of his data.
- RL12: Right to rectify, erase or block. The application shall allow the data subject to rectify, erase or block his data.
- RL13: Right not to be a subject to an automated decision. The application shall avoid taking automated decisions.
- RL14: Right to seek legal relief. The data subject has the right to seek legal relief for any breach of his data protection rights.

The third set of requirements is specifically aimed at electronic communications systems or applications. It poses limitations on the use of traffic data, and the processing of location data for the provision of Location Based Services. Automatic data collection procedures (e.g. on

websites) and unsolicited commercial communications (better known as spam) are also regulated, and form another category of legal requirements.

- RL15: Processing of traffic data. The application shall process personal data only to the extent needed for the purpose of the transmission of a communication.
- RL16: Processing of location data for the provision of a Location Based Service. The application shall only process location data when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service.
- RL17: Principle of confidentiality. The application shall ensure the confidentiality for communications.
- RL18: Automatic data collection procedures. The application shall inform the data subject regarding the processing of their personal data, even in the course of automatic data collection procedures.
- RL19: Unsolicited commercial communications (spam). The application shall protect the user against unsolicited commercial communication.

As mentioned in the introduction, all the different types of requirements listed in this section limit the degrees of freedom available in the design and use of SNSs and CWs. It is difficult, however, to translate the legal principles underpinning the different directives into very specific requirements against which technical designs can be matched. Nevertheless, any proposed application (use) must acknowledge these principles, and the legal requirements must therefore be be treated on par with the requirements elicited in the other parts of this document.

6.3 The user as a data controller

The notion of *data controller* is defined in the Data Protection Directive (art.2(d) DPD) as every individual or entity who determines the purposes and means of the processing of the data.

Processing of personal data refers to any operation performed on personal data such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction (art.2(b) DPD). A definition that wide covers basically every possible action that could be performed with regard to personal data, also in social networking sites.

In social networking sites, the provider of the service, who is processing personal data, is considered to be a controller (For a more thorough analysis see [Kuczerawy et al. 2008]). He is defining the technical side of the service, enabling its all functionalities and through that, determining the purposes and means of data processing (see [Wong and Savirimuthu 2008]). It is not possible to perform any activity on social network that has not been designed by the provider of the service. But is he the sole controller of the data?

It should be noted that the Data protection Directive provides an exemption from the general rule in case when the processing is performed for personal use (art.3(2)(b) DPD). In the European Court of Justice [ECJ] case of Lindquist (see [C-101/01]) it was decided that the act of referring, on an internet page, to a person and identifying that person by name or by other means, for example by providing the phone number, information regarding their working conditions or hobbies, is not covered by this exception. The ECJ ruled that 'personal use' must be understood as relating solely to activities carried out in the course of private or family

life of individuals, like holding of records of addresses (as mentioned in recital 12 of the Directive). According to the ECJ, it is not the case when the processing of the data consists in publication on the Internet which makes data accessible to an indefinite number of people. In effect of such a decision, Mrs. Lindquist was found to be processing data of her colleagues and thus she was a data controller in this scenario. Following that decision it could be argued that unrestricted use of SNS does not fall under the exception of Article 3(2)(b) DPD.

It is important to remember that social networks are used to share information, but not only about the user of a particular profile. Users of SNS upload information about themselves, but also about their friends, colleagues, family, etc. The position of an individual engaged in such activity will be interpreted differently according to the data he's processing. In case it is data referring to him, there is no problem. Everybody is free to give information about themselves if they wish so. Of course awareness of how much information is actually given and potential threats involved are issues that present a major problem, but this is not the topic of the discussion. In order to assess the position of the user as a data controller, and the need of compliance with the Data Protection Regulation the distinction has to be made between the data that is being processed. In other words, the subject of data has to be defined. It could be either the user of the profile, or somebody else. Things get complicated when the data given away in the social network site are of other people, very often not consenting to such action or even not aware of it.

- RL20: Subject of the data that is processed needs to be defined.

One has to bear in mind that the provider, although he makes the processing possible from the technical point of view, is most of the time not the one who is making the actual decision about putting somebody's data on the SNS. In such situations, it should be said that a joint controllership is occurring. The status of data controller is shared between the entities participating in the decision about data processing ([Response to Art.29] opinion 8). The entities are: the party allowing for the processing from the technical point of view and the party making the actual decision to publish the data. It means that, according to the circumstances, the person of data controller may change, moreover several data controllers could appear. Everything depends on the situation and the entity performing a particular action.

- RL21: Joint Controllership. Status of being the data controller can be shared between entities involved in the decision to process personal data.

It should be noted that there is a possibility that the same entity will act in more than one role simultaneously. However, this will only be true for separate activities and data of different data subjects. To illustrate this: a user of a social network service would be a data subject – for his own data, and at the same time, a data controller – for somebody else's data. That is, of course, if he is the one processing personal data and deciding on the purposes and means of such processing. To establish that, the level of the actual decision making power on the purposes and means has to be examined. Only in case such power can be attributed to a certain entity, that entity can be considered as data controller.

- RL22: The same entity can have more than one legal roles at the same time, e.g. being a data subject and being a data controller.

For the user, the power of deciding on the means, from the technical point of view, is limited. There is, usually, a possibility to adjust some settings but the manner in which the processing is conducted is beyond his control [Van Alsenoy et al. 2009]. This is a non-negotiable aspect that is designed by the service provider. In another words, it is a commercial intermediary

providing the service whom the technical functionality depends on (see [Wong and Savirimuthu 2008]). On the other hand, the decision-making power of the user refers to a choice whether he wants to provide certain information and which application he decides to use. For that reason, the roles of the entities in data processing should be distinguished with regard to a specific processing operation. The difference should be made between the decision-making power referring to the overall structure of an application, its security features, generic purpose etc., and the decision-making power over the input of specific personal data. If both decisions are made by the same entity, there will be a single controller. However, if these decisions are taken by different entities, there will be a situation of multiple controllers. One of them could easily be the user of SNS, e.g., when he puts pictures of his friends on his profile and tags the pictures with the names of his friends. As he's the one deciding about this action, he will be a controller of that data, but together with the service provider who made the function of uploading pictures technically available.

It should be emphasized that although the user will be in a position of data controller for processing data of his friends, it does not mean that he will be in such position for other activities performed within SNS. Such generalization should be avoided. Social networking sites consist of many different actions that should be separated. For each of these activities, the controllership should be established separately through an examination of participating entities.

- RL23: It should be avoided to generalize the controllership over personal data that users have.

In conclusion it should be said that the user of the SNS puts himself in a position where he can be qualified as the data controller but only of those processing operations for which he really determines the purpose and means. Consequently, the user can be attributed the controllership with regard to the information he decides to provide and processing operations he initiates.

6.4 Confidentiality of communication in the work environment

Specific provisions addressing protection of privacy of employees at work should be looked for in national legislations. However, the general approach on the European level originates from European Convention for the Protection of Human Rights and Fundamental Freedoms [EU Convention 1950]. In the article 8, it is stated that:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Although the article does not explicitly refer to privacy in the workplace, the case-law of the European Court of Justice proves that it should be understood so. According to the Court's interpretation in 'Halford v. the United Kingdom' (judgment of 25 June 1997, Reports of Judgments and Decisions 1997 III), and 'Amann v. Switzerland' (case no. 27798/95, § 43, ECHR 2000 II), telephone calls from business premises are prima facie covered by the

notions of “private life” and “correspondence” for the purposes of Article 8 § 1. As explained by the Court, it is a logical consequence that e-mails sent from work gain similarly protection under Article 8. The same applies to information derived from the monitoring of personal internet usage. In the case 'Copland v the United Kingdom' (judgment of 3 of April 2007, no. 62617/00, 2007, ECHR 253) it was decided that while the applicant had been given no warning that her calls would be liable to monitoring, she had a reasonable expectation as to the privacy of calls made from her work telephone. The ECJ stated that the same expectation should apply in relation to the applicant's e-mail and internet usage.

Furthermore, the Court found that the collection and storage of personal information relating to the applicant's telephone, as well as to her e-mail and internet usage, without her knowledge, resulted in a violation of her right to respect for her private life and correspondence within the meaning of Article 8. In effect, it should be said that the correspondence of employees can be controlled by their employers, but only as long as it is done with respect to their private life and correspondence.

- RL24: Employers should respect private life of employees when their workplace correspondence is controlled.

The presented interpretation of art. 8 by the ECJ delineates its approach to communication privacy at work. It has to be taken into account by the national courts when they interpret specific national provisions. For example in Poland there is no specific regulation addressing the issue in detail apart from one article of the Labour Codex which says that the employer has to respect the dignity of his employees, for example their right to confidentiality of correspondence. It is considered that the employers may control the professional inbox of their workers to know if they use the company’s equipment accordingly to its purpose. However, they have no right to check the content of private emails found in such business mailbox.

In Germany the Federal Labour Court (Bundesarbeitsgericht - BAG) has ruled several times on communication privacy at work. It stated that general surveillance of employees at work is not permissible and that surveillance requires a concrete suspicion of illegal behaviour and no other means of clarification being available (BAG, 14.3.2003, Az. 2 AZR 51/02). Regarding video surveillance at work the BAG ruled (BAG, 29.6.2004, Az 1 ABR 21/03) that this measure constitutes a severe infringement of the right to one’s own image, the right of confidentiality of the spoken word, and the right of informational self-determination. Only in case of an overriding legitimate interest of the employer can video surveillance be lawful. An example for such an overriding interest would be again a concrete suspicion of a behaviour punishable by law (theft, sabotage, industrial espionage).

Having said that, it should be mentioned that Art. 29 WP has discussed the problem and issued several opinions addressing it. It provided guidance and described the acceptable limits of workers' surveillance by the employer. It allows ensuring employers’ rights without violating those of the employees. According to the Art. 29 WP working document WP55 on the surveillance of electronic communications in the workplace:

Workers do not abandon their right to privacy and data protection every morning at the doors of the workplace. They do have a legitimate expectation of a certain degree of privacy in the workplace as they develop a significant part of their relationships with other human beings within the workplace. However, this right must be balanced with other legitimate rights and interests of the employer, in particular the employer's right to run his business efficiently to a certain extent, and above all, the right to protect himself from the liability or the harm that workers' actions may create [Art.29 WP 55].

In general, the existing case law on Article 8 provides three principles. The first one says that workers can have a legitimate expectation of privacy at the workplace. Such expectation should not be overridden by the fact that workers use communication devices or any other business facilities that belong to the employer. At the same time, the workers' legitimate expectation of privacy might be reduced by the provision of proper information by the employer. The second states that the general principle of secrecy of correspondence covers communications at the workplace. Moreover, it includes electronic e-mail and attached files. The third principle announces that respect for private life also includes to some degree the right to establish and develop relationships with other human beings. As such relationships, to a great extent, take place at the workplace, it puts limits to employer's legitimate need for surveillance measures ([Art.29 WP 55], p9).

- RL25: Employees can have proper expections about their privacy at workplaces.
- RL26: Employees should be informed if privacy might be reduced.

As for applicability of the Data Protection Directive, Opinion 8/2001 of the Art. 29 WP made it clear that it applies to the processing of personal data in the employment context the same way as in any other context ([Art.29 Opinion 8] (WP48), p13). Monitoring of email should be done with respect to the data processing principles like necessity, finality, legitimacy, proportionality, accuracy, retention of the data, and security ([Art.29 WP 55], p13-19, and [Art.29 Opinion 8] (WP48), p3). The special weight is put on the transparency principle, which in this case means that that the employer has to provide his employees with "a readily accessible, clear and accurate statement of his policy" regarding e-mail and Internet monitoring. Such statement should inform workers about:

1. E-mail/Internet policy of the company with a detailed description of the extent to which communication facilities of the company may be used for personal/private communications by the employees (e.g. limitation on time and duration of use).
2. Reasons and purposes for which surveillance, if any, is being carried out.
3. The details of surveillance measures taken, i.e. who? what? how? when?
4. Details of any enforcement procedures describing how and when workers will be notified of breaches of internal policies and be given the chance to respond to any such claims against them.

([Art.29 WP 55], p14)

On the basis of the DPD legitimization for e-mail monitoring can be found in Article 7(f), that is, where processing is necessary for the purposes of the legitimate interest pursued by the controller or by the third party or parties to whom the data are disclosed. Nevertheless, it should be emphasized that such legitimization cannot override fundamental rights and freedoms of the worker. For that reason case analysis is required. Moreover, it will be difficult to justify email monitoring in case the employee is given an e-mail account for purely personal use or is allowed access to web-mail account (it would be accepted in case of a criminal activity of a worker). In this situation it is not in the legitimate interests of the employer to have access to such data.

- RL27: Monitoring of e-mail communication requires case analysis and should not override fundamental rights of the employees.

6.5 Conclusion

In conclusion it should be said that although communication monitoring of the employees is allowed, it can be done only on condition that the fundamental rights of the workers are complied with. All the data processing requirements provided by the Data Protection Directive apply the same way as in any other context. The guidance provided by the Art. 29 WP allow employers to fulfill those requirements and free themselves from possible liability.

6.6 HCI Perspective on Legal Requirements

In PrimeLife several activities look at different aspects of social network services and collaborative workspaces. Work in Activity 4 on Human Computer Interaction (HCI) looks at design aspects of social networks and collaborative workspaces which facilitate adequate transparency for users to exercise and understand their privacy rights.

6.6.1 Art. 3 – household exemption

The main question currently being discussed in PrimeLife Activity 4 is whether users that process other users' data in virtual communities should or must have a privacy policy and how such policies should look like. This is of importance for both task 4.2.3 on Transparency tools for virtual community users, as the data track is also storing negotiated policies for data released to communication partners, as well as for task 4.3.2 on policy negotiations in virtual communities. The first question arising in this context is whether Art. 3 EU Directive 95/46/EC (so called household exemption) can be applied with the consequence that the other articles of the Directive do not hold? In other words: Is personal data processing by other individuals in virtual communities a data processing for purely private purposes? The household exemption applies only if the users have restricted access to their profile to self-selected friends (Draft Opinion on SNS [Art. 29 Draft 2009]) If the user allows access to his profile by groups he does not know or control the scope of, publishing data on his or her profile equals publishing it on the entire web (for example in facebook the network of a user's hometown may in some cases have several million members, for example the New York network). In this case, the processing can no longer be regarded to take place for purely personal or household activities. From a practical perspective, this conclusion requires technical tools to assist the user and to clarify the "status" of his profile and the data processing initiated therein. The SNS provider should provide general information about when the household exemption applies and when it does not and should also inform the user of what consequences this has (that is, if the user is regarded a data controller he has to comply with the obligations of Directive 95/46/EC). Additionally, each time a user wants to join a network in which the user does not control the number of members and allow access to his profile to all network or group members or when he sets his access control settings to "access to all SNS users" ,the SNS provider should inform the user of the changing legal obligations. Such information could for example be given by means of a pop-up window.

6.6.2 Art. 10 and 11 and the content of privacy policies

If we assume that an individual processing data of another individual in a virtual community is a data controller, how far can Art. 10 really be applied? This is important to know, as Art. 10 defines the content of privacy policies. If Art. 10 applies fully, then it means that if an individual Alice is processing data about another individual, Bob, then Alice has to inform Bob about her identity when she requests personal data from him. On the other hand, Alice

has also privacy interests to stay anonymous or pseudonymous within transactions. Therefore, for instance, in eBay both seller and buyer can act pseudonymously. How can we solve these conflicting interests of Bob of being informed of the identity of a data controller and of Alice of being not identified?

Art. 10 does not apply to all kinds of data processing as defined in Art. 2(b). According to Art. 2(b) processing of personal data shall mean any operation or set of operations which is performed upon personal data, such as collection, recording, organizing, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction. This provision applies only in cases where personal data is collected from the data subject. If this provision should have been applicable to all forms of data processing the term "processing" would have been used. The use cases regulated in Art. 10 are probably not the typical SNS use cases: Art. 10 applies in cases where a transaction or the conclusion of a contract is conducted online and the data subject provides information him- or herself. In SNS the profile owner publishes (not collects) data about third parties without their prompt knowledge or contribution. Art. 10 may however apply in cases where e.g. a SNS user takes a photo - taking a photo means data collection; data collection can be defined as the purpose-bound acquisition of data on the data subject - with the intention to publish it in his SNS profile (and no household exemption applying to that profile). In this case Art. 10 applies fully. Art 10 differentiates between two kinds of information the data controller has to give to the data subject. Under all circumstances (no exemption is regulated), the data controller has to give the following (minimum) information (unless the data subject already has this information):

- identity of controller and representative,
- purpose of processing.

In addition, "further information" must be given only in so far as such further information is "necessary". Further information comprises:

- recipients or categories of recipients of the data
- whether replies to the questions are obligatory or voluntary, as well as the consequence of a failure to reply,
- the existence of a right of access to and the right to rectify the data concerning the data subject.

Giving this additional information is considered "necessary" if the person whose data is to be collected needs this information to rightly and comprehensively assess the consequences of his or her contribution to the data collection and to make a decision aware of the legal position. Germany decided to include the general obligation to provide information about recipients or categories of recipients into Art. 4 (3) 3. Federal Data Protection Act. However, we have to look into whether Art. 11 and the therein regulated information obligations may be applicable (with very similar consequences as if Art. 10 were applicable).

Art. 11 applies in cases where the data have not been obtained from the data subject. In these cases the data subject shall be informed at a later point in time (not upon collection): when the data relating to him his recorded or when a disclosure to third parties is envisaged. Thus, Art. 11 is applicable when a SNS user is about to enter (and subsequently record and publish to third parties) data about the data subject in his profile that he did not collect from the data subject himself (again: if the household exemption applies, the entire provisions of the directive and thus also Art. 11 is not applicable).

Unlike in Art 10 there exists and exemption from the obligation to inform the data subject under Art. 11. In Art. 11 (2) it is stated that the information obligation shall not apply where […] the provision of such information proves impossible or would involve disproportionate effort. Regarding the "disproportionate effort" exemption not the overall effort matters that providing information would ensue. The disproportionality has to be assessed taking into account the data subject's legitimate interest to receive the information as well as the effort to provide this information. Considering the fact that in the context of SNS Art. 11 applies only where access to the profile is not limited to self-selected friends, the data recorded in such profiles and disclosed to (an unlimited number of) third parties may be very sensitive and at the same time accessible to a vast and uncontrolled number of individuals. On the other hand, implementing an information tool seems possible for SNS providers who have to offer this mechanism to their profile users who want to publish data about other individuals.

6.6.3 Data of third parties

In virtual communities, communications between users contain personal data of those users. If we implement the data track at one users side (Alice's side) and store all personal data releases to other users (e.g., to Bob), these transaction records stored at Alice computer do not only contain Alice personal data but also Bob's personal data. How far can this be a problem?

If these communications occur between a limited number of users, the household exemption does apply (this is email-like communication, not posting (=publishing) information on a profile's wall.

6.6.4 User rights

In task 4.3.2, online functions for implementing user rights to access their data will be implemented. If a services side stores records that contain data about relations of more than two persons, how far do one have the right to access those data that not only refer to oneself but also to others?

Article 12 explains the scope of access rights of the data subject. The data subject has the right to demand information about "data relating to him" from the data controller. The information to be provided comprises: categories of data as well as the purpose of processing and the recipients of data as well as information about the data itself in an easy understandable manner. If the data controller stores information about the network of a user (whom he put on his buddy list or whom he exchanged communication with), this information must be given to the data subject upon request.

The question remains whether an individual will have the right to access personal data referring to him/her that another individual is processing. The answer to that question is affirmative, if the other individual is a data controller and the household exemption does not apply.

Chapter 7

Requirements Overview

7.1 Introduction

The goal of this chapter is to collect the requirements that have already been explicitly identified in the previous chapters, and structure these by means of the mechanisms that also have been distinguished. The ideal situation would be that the overview of requirements can be handed over as a list of instructions for technical designers of the ideal future SNS and CW. In practice, however, the list of requirements is an approximation at best, and new requirements will evolve as the use of SNSs and CWs becomes more broadly accepted, and new application areas are discovered.

Therefore, the following approach has been adopted. The main structure of the requirements is provided by the overview of mechanisms, that is constructed based on the mechanisms identified in the chapter on use cases, and the more elaborate investigation of chapter 5, Mechanisms. Within this framework, all explicit requirements that are listed in chapter 4, Issues, are gathered under the relevant mechanism. This leads to an overview in which some mechanisms are worked out into a large number of specific requirements, whereas the result for other mechanisms may be more limited. Since the development of particular new requirements is an ongoing process, the offered structure allows placing new requirements under the relevant mechanisms, thus building on an ever larger repository of requirements, that is - by definition - never complete.

Selective access control as a means for privacy enhancement chiefly builds on technical features, which is reflected in the technical focus of many requirements. It should not be overlooked that many requirements with regard to privacy are rooted in legislation. Therefore, a separate chapter is devoted to the legal requirements to SNSs and CWs that can be derived from applicable European legislation. Any privacy-enhanced SNS or CW must meet both the technical and the legal requirements in order to be acceptable.

7.2 Overview

Chapter 5 provided an overview of all mechanisms that should be considered to enable selective access control as a means for enhanced privacy in social networks and collaborative workspaces. These mechanisms will be used as a structure in which the more detailed requirements are allocated. Besides the requirements that have been elicited in the past chapters (starting with RS or RC), new requirements (R) complementing them will also be listed in this overview. They will also be distinguished with a unique identifier.

7.2.1 Access Control

Several privacy-enhancing features can be added when designing access control mechanisms in SNSs or CWs, where the objects include profile information and contributions as well as privacy preferences themselves. Access can be based on numerous features, including the object identifier, its role, certain properties of the data object, or the context in which access is requested, amongst others.

The collected requirements which pertain to this mechanism are the following.

- RS2: The SNS should facilitate users with similar interests to connect without revealing personal data until after a link is established.
- RS4: Users should be able to assess the proposed new contact prior to committing to a connection.
- RS5: The SNS should offer proper access control to the profile data.
- RS15: The SNS should prevent the use of profile information for surveillance purposes
- RS16: The SNS should prevent the possibility of unauthorised download of profile information.
- RS17: The infrastructure should make it impossible for the SNS provider (and its employees) to have access to the data of the users.
- RS18: The infrastructure should make it impossible for the SNS provider (and its employees) to have access to the collected secondary data of the users.
- RC2: CWs should provide options for users to define access control rules to their user-generated content in a privacy-respecting way.
- RC3: CWs should allow users to control secondary use of their contributions.

Additional requirements that need to be considered for user-controlled access control.

- R30: an access control engine for a privacy-enhanced SNS or CW framework should be able to process and enforce the access control rules deriving from different features.
- R31: on the client-side, a user interface supporting the definition of the corresponding advanced access control policies (see R30) is required whenever the user should have the possibility to specify these for his/her data.

7.2.2 Data Handling Policies

The requirements surrounding control of access to certain personal information was the main theme of the previous subsection. When access is granted to a certain piece of information, the next set of requirements deals with the way the data is treated when it is being accessed.

- RS7: The SNS should offer mechanisms for the user to specify data handling policies to be respected by human readers and machines.
- RC3: CWs should allow users to control secondary use of their contributions.

- RC4b: CWs should provide options for users to specify a time period after that their contribution is deleted or marked as out-dated.

Additional requirements concerning data handling policies, that are more geared towards technical implementation.

- R40: a UI or similar client-side feature to define the policy and attach it to the data (as metadata)
- R41: a system to package and transmit the metadata and data together (e.g. an endpoint for a web service building and sending a SOAP message)
- R42: an enforcement system that reads the metadata and applies the DHP (e.g. require credentials to access the data itself).

7.2.3 Identity and relationship management

Considering the central role of personally identifiable information within this work package, the number of requirements dealing with identity management is not surprising.

- RS1: The SNS should facilitate methods for creating and maintaining useful (social) groups within a user account (profile) and have proper access control to information in those groups.
- RS3: Users should have control over social contexts and be able to create different kinds of context relating to distinctions such as Gemeischaft v. Gesellschaft.
- RS6: The SNS should provide ways to move inactive relations to social groups more distant from the user (less access rights).
- RS8: The SNS should offer models for relationships, policies, etc., that mimic everyday human social interactions.
- RS9: The SNS should provide users with tools to inspect (and correct) the automated inferences made on the basis of their behaviour in the network.
- RS10: The SNS should offer users the option to terminate their SNS identity which should result in deletion of all data pertaining to this user in the SNS.
- RS11: The SNS should offer users means to export their profile and network (relations) to other SNSs.
- RS23: The SNS should offer mechanisms to manage/limit the distribution of unsolicited messages.
- RS24: The SNS should require proof of identity before allowing someone to publish their own profile.
- RS24a: The SNSs should provide a certain level of anonymity to its members.
- RC5: CWs should provide a privacy-friendly solution to prevent the abuse of other's identities (e.g., trusted third party that certifies the identity of users).
- RC8: CWs should provide features for creating, managing and deleting different partial identities in order to reduce linkability of all actions of the same user.

7.2.4 Use of credentials

Credentials are used to ascertain the right of certain requesters of access to personal information. Requirements relating to credentials are the following:

- RC2: CWs should provide options for users to define access control rules to their user-generated content in a privacy-respecting way.
- RC5: CWs should provide a privacy-friendly solution to prevent the abuse of other's identities (e.g., trusted third party that certifies the identity of users).

7.2.5 Encryption of content and communications

Encryption is used to safeguard personal information from unauthorised views, both when stored and when transmitted. The number of requirements reflect the different perspectives from which data can be shielded using encryption, being third parties, or even the provider offering the social network or collaborative workspace as a service running on its IT platform.

- RC3: CWs should allow users to control secondary use of their contributions.

7.2.6 Legal requirements

Existing legislation limits the freedom the different parties in SNSs and CWs have to structure the access and processing of personally identifiable information. Quite some requirements can be derived from this perspective, and the challenge will be to implement these requirements in such a way that some degree of automation is feasible. Chapter 6 focuses specifically on the relevant legal requirements. In the chapter on Issues, a number of requirements was already formulated.

- RL1: The application shall collect and process personal data in a fair and lawful way.
- RL2: Legitimate processing. The application shall base the processing of personal data on a legitimate ground (e.g. consent of the user required, unless one of the other grounds applies).
- RL3: Principle of finality / purpose limitation. The application shall use the personal data only for the specified and legitimate purposes.
- RL4: Principle of data minimisation. The application shall collect and process only the data that are adequate, relevant and not excessive for the specified purposes.
- RL5: Principle of data quality. The application shall use accurate and up to date information.
- RL6: Principle of conservation. The application shall keep personal data only for the necessary purposes, for which the data were collected.
- RL7: Principle of security. The application shall ensure the secure storage and transmission of personal data.
- RL8: Principle of notification to the Supervisory Authority. The data controller shall inform the national Data Protection Authority of the collection and processing of personal data.
- RL9: Right to information. The application shall ensure the data subject is informed before the processing of his data
- RL10: Right to object. The application shall allow the data subject to object to the processing of his personal data.
- RL11: Right of access. The application shall enable the data subject to get information regarding the processing of his data.
- RL12: Right to rectify, erase or block. The application shall allow the data subject to rectify, erase or block his data.
- RL13: Right not to be a subject to an automated decision. The application shall avoid taking automated decisions.
- RL14: Right to seek legal relief. The data subject has the right to seek legal relief for any breach of his data protection rights.
- RL15: Processing of traffic data. The application shall process personal data only to the extent needed for the purpose of the transmission of a communication.
- RL16: Processing of location data for the provision of a Location Based Service. The application shall only process location data when they are made anonymous, or with

the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service.

- RL17: Principle of confidentiality. The application shall ensure the confidentiality for communications.
- RL18: Automatic data collection procedures. The application shall inform the data subject regarding the processing of their personal data, even in the course of automatic data collection procedures.
- RL19: Unsolicited commercial communications (spam). The application shall protect the user against unsolicited commercial communication.
- RL20: Subject of the data that is processed needs to be defined.
- RL21: Joint Controllership. Status of being the data controller can be shared between entities involved in the decision to process personal data.
- RL22: The same entity can have more than one legal roles at the same time, e.g. being a data subject and being a data controller.
- RL23: It should be avoided to generalize the controllership over personal data that users have.
- RL24: Employers should respect private life of employees when their workplace correspondence is controlled.
- RL25: Employees can have proper expections about their privacy at workplaces.
- RL26: Employees should be informed if privacy might be reduced.
- RL27: Monitoring of e-mail communication requires case analysis and should not override fundamental rights of the employees.

Additional requirements on SNS and CWs with regard to legal rules.

- RL28: The platform should offer proper mechanisms to assist users in getting consent of those involved in the content they publish.
- RL29: The platform should provide mechanisms for users to retract their consent to publishing data pertaining to them and have data removed.
- RL30: The platform should provide users the means to make their own code of conduct or house rules for their ‘friends’.
- RL31: The platform should provide a code of conduct for its users.

7.2.7 Awareness and Transparency

No matter how many technical measures are implemented to meet the demands of selective access control in SNSs and CWs, all is lost if users are not aware of the way their personal information may be used, or what the consequences are of their decisions regarding their information dissemination behaviour. The following list of requirements addresses this final perspective on relevant requirements.

- RS12: The SNS should provide mechanisms that allow the user to see what implicit information leaks may occur (transparency tools).
- RS13: The SNS should provide information about risks associated to certain behaviour in an empathy encouraging or empathy understanding way.
- RS14: The SNS should offer mechanisms for the user to see who has accessed their data.
- RS18a: The user must be made aware who owns data uploaded to the SNS, and who owns information generated through the use of an SNS.
- RC1: CWs should provide features for the awareness of users about the potential audience of their contributions.

- RC6: CWs should support the privacy awareness of user by informing them about their actual level of privacy (e.g., identifiablity of the user from the perspective of service providers)

Chapter 8

Conclusion

This document investigated the requirements and concepts for privacy-enhancing access control in social networks and collaborative workspaces. Several approaches were used to unearth relevant requirements, starting with the description of a wide range of use cases for both social network sites (SNSs) and collaborative workspaces (CWs). These delivered a first assessment of relevant mechanisms that should be available if the social software under investigation is to function in a privacy-enabled way. The chapter on issues used another angle to elicit relevant requirements: based in recent literature many issues were addressed, where it was interesting to note that these reached much farther than the expected problems surrounding deficient access control mechanisms. Social consequences of the (un)intended use of social software were identified as issues in their own right, and alleviating these types of problems is not so straightforward, not least because there are some inherent conflicting interests in the daily use of these technologies.

A large number of legal requirements can be derived from current privacy and data protection regulation, that is applicable to electronic data processing solutions in the broadest sense. These regulations also apply to SNSs and CWs, but at the moment the legal provisions have not been translated into a level of granularity that is detailed enough to link with certain mechanims on a one-to-one basis, let alone that they are specific enough to incorporate in unambiguous instruction for system development. Finally, based on the input generated through the previous chapters, a number of mechanisms was derived that cover different means to decrease the privacy risks associated with the use of social software. Thanks to the more encompassing initial investigation, mechanisms are proposed that go beyond mere access control technologies. The created mechanism overview was expanded upon, amongst others through a deeper investigation of available technologies that may support the objective of improved privacy and identity management in social networks. The requirement overview used the categorisation over the different mechanisms as a structure in which the individual detailed requirements were put. This structure also makes it easier to assess the type and character of any additional requirements that may be developed in the future.

One of the conclusions that can be derived from the work done in this heartbeat is that requirements to privacy-enhanced social networks and collaborative workspaces diverge widely in their application areas. Not only technically focused requirements pertaining to intricate implementation details emerge, but also requirements with regard to raising

awareness amongst unsuspected users are mentioned. Notwithstanding the wide diversity of these types of requirements, they are all relevant for the success of future privacy-enhanced solutions. Another conclusion is, that a number of areas require further in-depth research in order to make the requirements more specific and thus more tangible for application in live (prototype) environments. The legal requirements are a prime example of this.

8.1 Outlook

An iterative approach is indispensable when it comes to the development of innovative solutions, and this truth certainly applies to future privacy-enhanced social networks and collaborative workspaces. The output of this document will be used to support design decisions of the next PrimeLife heartbeat H1.2.6, which consists of the development of prototypes of an SNS and one for CWs that have incorporated privacy features. It is only after some initial work on the prototypes will have been done that some practical issues will feed back into the requirements overview. Development and implementation of required features will undoubtedly teach us impossibilities or new possibilities that have not been considered in a previous phase. A further wave of additional requirements will be generated when the developed prototypes will be used as platform for actual user interaction. It is only at this stage that feedback will become available on the way end users actually use the provided system features, which may lead to radical new insights and - consequently - drastic adaptations of the requirements overview generated to date.

Another expected development is that many requirements that have been identified and documented in this report, will undergo a further specification based on their applicability in practice. This will definitely be true for the legal requirements, since these have to be made specific for the systems and associated communication of persoanl information to which they have to be applied. It is only through a confrontation with actual circumstances that the practical effective implementation of the legal requiremenst can be taken a step further.

Finally, the next phase will open possibilities to outline more specific technical requirements as well. During work on this document a number of technical avenues have already been explored, but the results better fit as exploratory parts in the next heartbeat document. These technical requirements will come to the fore when they can be explicitly linked to certain technical design decisions, and this is the reason why they have been largely transfered to the next heartbeat in which all requirements and concepts developed in this heartbeat will come to life.

Appendix 9

Glossary

In the discussion on requirements and concepts for privacy-enhancing access control in social networks and collaborative workspaces, many terms are used that could benefit from some further explanation. This lexicon of terms contains many of the concepts used in the main document, and can be consulted when needed.

Access control

The means to restrict access to resources or services based upon policies defined by the owner. For example, limiting access to a photo to people who are members of a named group defined by the owner. Different access control policies can be set for different operations, e.g. reading and writing. Access control can apply to metadata like group definitions, e.g. to prevent group members from seeing who the other members are.

Access control is based upon facts known to the entity evaluating the policy or which can be determined by asking trusted parties. One issue is whether the domain of facts is open or closed, i.e.if a fact is not known to be true, can it be assumed to be false. The closed world assumption may be a good fit when a profile owner is responsible for the properties attributed to his or her connections. In other words, the value of access control policies depends on the quality of the information upon which they act.

Access control policies may be changed to reflect changes in relationships between people, e.g. when you fall out with someone and decide to withdraw their read or write access to your profile.

Authentication

Establishing your identity to an SNS, e.g. by providing your identity and associated password. To avoid the risk of people accessing your profile when you have gone for a coffee, etc. the website may require you to re-authenticate yourself after a period of inactivity.

Strong authentication may involve the use of a hardware device (e.g. a SIM card) that can prove its presence in response to a challenge, or biometric techniques such as voice authentication, iris or finger print scans, and face recognition.

Websites may authenticate themselves to users as a defence against phishing, e.g. by showing you a photo that you uploaded and which is only accessible to you. Research has shown that digital certificates attesting to the identity of a website are unreliable, and offer poor usability.

Calendar

Information describing someone's planned activities over time periods of hours, days, months and years. Such information may be exposed to other people with the appropriate access rights. The information may also form part of access control policies, e.g. hide my location from my work colleagues out of normal working hours or when I am on vacation. A calendar may be composed of information from other people/groups, e.g. national vacation days and sporting events.

Captcha

A challenge-response mechanism used to distinguish people from software agents, e.g. on the basis of identifying text in an image or performing some task that requires competence at commonsense. This is sometimes referred to as a reverse Turing test. The term is short for "Completely Automated Public Turing test to tell Computers and Humans Apart". Multiple captchas may be needed to avoid discriminating against people with different disabilities.

Collaborative Workspaces

Collaborative Workspaces (CWs) are infrastructures and platforms that enable users to work together, e.g. gathering information or creating contents in a collaborative manner or simply sharing data between each other. Applications of collaborative workspaces include knowledge management in an electronic environment, idea generation by applying computer-supported creativity techniques, or informal discussions of everyday life, amongst others. E.g.: Wiki systems, Forums.

Credential

A statement attributing a property to an identity, e.g. that Alice is at least 18 years old. The significance of the credential depends on the trustworthiness of the entity making the statement. Credentials may provide a mechanism to verify their authenticity and integrity, i.e. to detect forged or modified credentials.

Credentials can cover an open ended set of properties, e.g. your age, your occupation, your gender, your reputation, your skill level in a game and so on. More complex credentials can be used to express what kinds of statements the subject identity can make.

Credentials can be used for anonymous identities, e.g. to attest that X is a member of the group "employees" without revealing which employee X is. This can be used to prevent a website from relating nicknames of users to their civil identities. Access control policies should be able to distinguish whether someone is using an anonymous identity.

Credentials may be signed by a trusted third party or even self-signed. The latter can be used to distingish between statements made by the identified person from statements made by others.

Access control policies may require trust in the reliability of a credential provider to supply credentials upon request, e.g. if you want to provide access to friends but not

colleagues, and the credential that someone is a colleague is held back, then access will be granted incorrectly.

This isn't a problem for groups maintained by a profile owner as the owner will know which of his or her friends are colleagues. It becomes more complicated when people want to access resources using partial or anonymous identities where they limit the amount of information they are prepared to disclose about themselves. This can be managed through policy languages that describe who can be can be relied on to provide accurate information about a subject even if the subject's identity is withheld.

The logical distinction between not saying something that you know to be true, and saying something that you know to be false doesn't really matter, as neither case will arise for a trusted speaker.

Users may want to restrict the personally identifying information they disclose to a website, including their list of connections. A trusted third party could be employed to apply access control policies without the need to disclose users' personal data to the website. This would require a new breed of SNS/CW with more sophisticated business models where privacy providers are a new breed of intermediaries.

Download

Read access to a resource. This may be associated with data handling policies, e.g. you can view a clip within the browser, but you are not licensed to save a local copy.

Groups

Groups can be defined as an explicit set of named identities, or implicitly as the set of identities bearing a given credential. One implicit group is "everyone", i.e. anyone accessing the SNS. Members of the SNS can choose whether they want to join a group.

Groups, joining/leaving

The group owner may allow people to subscribe themselves to a group and to leave a group under their own volition. Alternatively, a mechanism may be provided to invite people into a group, e.g. by sending them a notification with an appropriate credential. Access control policies should be able to distinguish between open and closed groups, as you should exercise caution in what resources you make available to open groups as you have no control over the group membership.

Group members and group owners may choose to receive notifications when people join or leave groups.

Users should be able to determine what information they disclose about themselves for the purpose of joining a group. This can be done via credentials. Such information may be hidden from other group members. It shouldn't be necessary to construct an explicit partial identity when doing so.

Entrance to a group may be dependent on presenting appropriate credentials, e.g. that you are a suffering from a particular illness, as attested by a doctor, but without disclosing either your or the doctor's identity. Digital certificates provide one mechanism for achieving this. Zero-knowledge proofs may provide another mechanism.

Identity

This is a name by which a user is uniquely identified by an SNS. The identifier is often an email address and may be associated with a non-unique alias, e.g. Alice. Software agents that can access the SNS also have identities.

Identity, anonymous vs partial

Someone may wish to join a group without disclosing their identity. One approach is to sign up with a pseudonym that is visible to other group members, e.g. on messages posted to the group. The pseudonym may be associated with a partial identity with its own profile. In principle, the same user may have multiple partial identities on the same SNS.

Anonymous access goes one step further by avoiding any record of the (partial) identity for group accesses. Access control policies should be able to distinguish anonymous access from other access, e.g. to limit write access to non-anonymous users.

Users should be able to determine what information they disclose to other group members about their identity, e.g. you could disclose your age and city of residence without providing any further information.

Lists

Named set of people forming a set of social connections to the list owner, e.g. a number of friends named "Picnic Lovers". This lists are part of the user's profile and are solely adminstered by him, i.e. others cannot decide whether they want to be on a particulat list.

Location

Handset location may be determined by the mobile network, e.g. based on time difference of arrival at network antennae. Alternatively, handsets may use A-GPS and upload location data to the SNS, e.g. using a widget application that is launched when the phone is switched on. The network based method takes advantage of capabilities deployed to meet regulations from the EU Directive E112 2003 [Directive E112], and illustrates the role of software agents as sources of information.

Access control policies should be able to limit the accuracy and frequency of update used to report location to different users or software agents. Policies should also be sensitive to the owner's current status, e.g. in/out of working hours, on vacation or at a confidential meeting. This can be based on access to the owner's calendar, or to presence information provided by the owner.

An open question is whether there needs to be a mechanism to allow or disallow users from providing fake location data. This would seem to depend on the context. Private individuals going about their business are one thing, where it could be argued that individuals should be free to give whatever location they want, while calls to the emergency services are another, see [Directive E112] which requires mobile phone networks to provide emergency services with whatever information they have about the location from which a mobile call was made.

Accurate location data may also be important for logistical purposes e.g. a company monitoring the location of its delivery vans, and for security purposes such as the location of police cars in case they run into trouble and assistance needs to be sent.

Logs

Records of accesses to a profile. These logs are only accessible to the profile owner. The records describes who accessed what resources and differentiate between known connections (Alice's friends), the general public, and software agents (of which the SNS provider is a special case). Access control policies may require the use of a captcha mechanism to preclude or distinguish access by software agents.

Log analyses may be provided on a regular basis as determined by the profile owner's preferences or on request. Real-time notifications may be provided e.g. for access control violations, assuming the profile owner has designated an appropriate notification mechanism, e.g. instant messenger.

Message

This can be a passage of text or multimedia content that posted to a profile or group and placed into a message queue. See moderation for a consideration of how messages are handled.

Moderation

A mechanism for reviewing messages and determining whether to publish them, to delete them or to mark them as spam. Your profile preferences determine whether you need to approve messages before they are published. In principle, you could set a policy that controls how incoming messages are handled based upon who posted them and other factors. For instance, messages from people in your friends group are published immediately, but messages from other people require moderation.

Notification

A means to alert users to events such as a new message appearing on a friend's profile. Notifications could be provided in a number of different ways, e.g. on your profile page, as emails, as SMS text messages to your phone, or through instant messaging services.

Persona, digital

The digital persona is a model of an individual's public personality based on data and maintained by transactions, and intended for use as a proxy for the individual.

Persona, imposed

An imposed persona is the part of the digital persona (see definition) that is controlled by the individual. The imposed persona corresponds with the individual's profile (see definition) as maintained on a web page. [Clarke 1994].

Persona, projected

The projected persona is the (gestalt) impression of an individual created by other(s). In the context of SNS/CW a projected persona is used to describe the profile maintained by platform providers about individual users on the basis of their imposed persona and data concerning the user's actions and their relationship's actions as well as other information that can be associated to the imposed persona (usually unknown to the person concerned). This corresponds to the notion of profiling in relation to data mining etc, as performed by web based service providers such as Google.

Policies, reputation based

An access control mechanism that limits access based on someone's reputation score.

Policies, time based

An access control policy could limit access to people who have been members of a given group for a given period of time, or who joined the group before a give date. Policy

languages should support expressions such as before or after a given date, or during a given interval.

Presence

This is information describing the status of an identity that is generally used as part of instant messaging services. It may include information on whether the person behind the identity is available to chat with, or simply offline. Presence information may include a geographical location. The level of detail provided may vary according to the recipient's access rights.

Privacy preferences, client-side management of

This approach relies on a browser extension for managing Alice's privacy preferences and storing them locally on her computer. The architecture is outlined in the Social Network Demonstrator where a Firefox browser extension manages privacy options in local storage. Content created by Alice and deemed to be secret is encrypted before submission to the social networking site (SNS). The policies for access control to that content are also included in the web page using a digital signature to ensure integrity. When Bob wants to look at this content, he is required to have installed the same browser extension. The extension reads the page and associated policy on the fly, verifies its integrity and enforces the policy. If the policy allows Bob to view the content, the extension decrypts it and presents it.

This approach has the benefit that users keeps all of their privacy preferences locally, but that is also a weakness, e.g. should the computer breakdown or become unavailable, e.g. due to damage or theft. In practice, many users find it difficult to backup their computers, with a consequent risk of permanent loss of data. A further drawback is that users won't be able to upload or view private content should they find themselves without their computer. For instance, when they want to access the site from an Internet Cafe or from a mobile device rather than their desktop computer (or vice versa). Finally, the approach restricts users to browsers that support the extension and imposes the burden on friends to install that extension.

Privacy preferences, server-side management of

In this approach users trust a privacy provider to look after their privacy preferences and to enforce the associated policies. Users can use the web browser of their choice and there is no need to install a browser extension. Users are required to authenticate themselves with the privacy provider which then communicates directly with the website (e.g. an SNS). The approach allows for single-sign on with participating websites, and can be combined with support for micropayments, as a further incentive to these websites.

This avoids the drawbacks of the client-side approach, and enables access at any time, from anywhere, and on any device, but puts users at risk if their user name and password fall into the wrong hands. That can be safeguarded through the use of stronger authentication, e.g. through a hardware device that can prove its presence through a response to a challenge, or through the use of biometric techniques. Alice's data is at risk should the privacy provider go out of business, and it should be possible for Alice to transfer to another provider in that eventuality.

Privacy providers are in a position to profile user actions, but would be subject to privacy policies, and the full weight of regulatory measures and market forces, should they breach those policies. A further issue is that the approach will only work with the active cooperation of participating websites.

Profile

A web page with information provided by the profile's owner. The profile also includes meta-data such as personal preferences, group definitions and access control policies, with the means for the profile owner to determine who can access this information.

Profile, deactivating vs deleting

The SNS may distinguish between deactivating and deleting a profile. For example, are messages posted to other profiles/groups deleted when the profile owner decides to close his account with the SNS? Are there any requirements imposed by national security legislation? The SNS terms of use policy should make this clear.

The data that should be deleted includes:

- The profile and associated personal preferences and policies.
- All content uploaded to the profile by the owner and others.
- All group definitions defined by the owner for this profile.
- All records of communications that have taken place in the past.
- All messages that the owner posted to other profiles/groups.

This essentially requires the data to be tagged with the owner's identity to enable the SNS provider to find and delete the data.

Profile preferences

These are defined by the profile owner, and include access control policies, and personal preferences for the appearence and function of the profile.

Reputation

A numeric or enumerated score indicating the reputation of an identity. The SNS/CW will typically operate a process that automatically determines the reputation based on a number of considerations, e.g. the number of posts, and rankings provided by people viewing theses posts. Reputation can be used by rules for filtering posts (e.g. to discard low scoring posts), and for access control policies, e.g. restricting write access to people with high reputation.

Resources

Text and media clips, e.g. photos, songs, and video. This may also include metadata such as group definitions and personal preferences, as well as messages posted to the profile by the owner or other people.

Resources, encrypted

Resources may be uploaded and held in an encrypted form to prevent unauthorized access (including by the SNS provider). This assumes a mechanism whereby only legitimate users may gain access to the corresponding decryption key. This could be as simple as a shared secret password (e.g. as for PDF files).

Encryption may be used for messages, e.g. when an employee posts messages to the profiles of other employees, and wants to avoid a manager from being able review these messages.

Law enforcement agencies may be able to require access to encrypted resources. One mechanism for this may require the use of keys from multiple people in different positions as a safeguard against abuse. Key escrow mechanisms are

available, but the question remains whether they adequate and whether their use is logged effectively to satisfy legal rights of end users?

Resource id

A means to identify a given resource as a basis for access control. This is equivalent to a unique tag that is guaranteed to only apply to a single resource.

Session

A sequence of interactions between a person or agent and a web application that take place during a limited period of time. Note that a user can be involved in multiple overlapping sessions with different websites. A particular case is where the user signs onto an SNS using a federated identity service where one session is with the SNS and another is with the identity service.

Sign-off

The process of signing off from a session. This terminates the session. Sign-off may be initiated automatically after a period of inactivity.

Sign-on

The process of signing onto a session with a web site or service. This starts the session. The user will typically be asked for a credential, e.g. a password, or a credential supplied by an identity provider, which could even be as simple as a cookie set by the website during the previous session with that site.

The session may require users to confirm their presence at regular intervals or after periods of inactivity, as a means to defend against other people masquerading as the user.

Social Network Sites

Social Network Sites (SNSs), e.g.: LinkedIn, Facebook, have three common features:

1. identity construction. Social network sites offer a very direct tool for what Goffman [Goffman 1959] calls “impression management”: the profile page.
2. relationships. Social network sites offers communication channels for the users to make new friends and deepen connections with current ones.
3. community. Social network allow users to represent a social position: to be recognized as a valued member of one’s various communities. Connectedness is social currency (social capital).

Tags

Words used to tag resources to enable selection by tag, or for use in access control policies to restrict access to resources with a given tag.

Transferring to another SNS/CW

It should be possible to transfer an identity and profile from one site to another with the option to delete the identity and profile on the originating site.

Upload

Mechanism for transferring resources into a website/SNS

URI

A Uniform Resource Identifier (URI) identifies a resource (e.g. Webpage) on the Internet.

Versioning

A website for a wiki may provide access to previous versions of pages. Access control policies should be able to restrict access to previous versions based upon the identity of the person who is seeking access, e.g. the wiki owner(s) may limit such access to a set of trusted colleagues.

References

[Art. 29 Draft 2009]
Draft Opinion of Art. 29 Working Party on SNS, Version 29.1.2009, p. 6.

[Art.29 Opinion 8]
Article 29 Working Party, Opinion 8/2001: Opinion on the processing of personal data in the employment context, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2001/wp48en.pdf, accessed 13 May 2009.

[Art.29 WP55]
Article 29 Working Party, Working document on the surveillance of electronic communications in the workplace, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp55_en.pdf, accessed 13 May 2009.

[C-101/01]
Official Journal of the European Union, Judgement of European Court of Justice, case C-101/01, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2004:007:0003:0004:EN:PDF, accessed 13 May 2009.

[CardSpace 2009]
http://msdn.microsoft.com/de-de/netframework/aa663320(en-us).aspx, accessed 19 June 2009.

[Clarke 1994]
Clarke, R., "The Digital Persona and its Application to Data Surveillance", *The Information Society 10*, 2, http://www.rogerclarke.com/DV/DigPersona.html, June 1994.

[Directive 1999/93/EC]
Directive 1999/93/EC on a Community framework for electronic signatures, Official Journal L No. 13, 19.01.2000, p. 12, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:HTML, accessed 13 May 2009.

[Directive 2002/58/EC]
Directive 2002/58/EC on Privacy and Electronic Communications, http://eur-lex.europa.eu/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf, accessed 13 May 2009.

[Directive 95/46/EC]
Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf, accessed 13 May 2009.

[Directive E112]
Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0022:EN:HTML., accessed 3 July 2009.

[DoW 2008]
PrimeLife: Description of Work, internal document, version 4 as of February 18, 2008.

[Douglas 2007]
Douglas, N., *Facebook Employees Know What Profiles You Look At*, VALLEYWAG (Oct. 27, 2007), http://valleywag.com/tech/scoop/facebook-employees-know-what-profiles-you-look-at-315901.php, accessed 3 July 2009.

[EU Convention 1950]
European Convention for the Protection of Human Rights and Fundamental Freedoms, Rome 4.11.1950, http://conventions.coe.int/treaty/en/Treaties/Html/005.htm, accessed 13 May 2009.

[Edwards & Brown 2009]
Edwards, Lilian and Brown, Ian: Data Control and Social Networking: Irreconcilable Ideas? *Harboring data: Information Security, Law and the Corporation*, (ed. A. Matwyshyn), Stanford University Press, http://ssrn.com/abstract=1148732, accessed 13 May 2009.
[FriendFeed 2009]
FriendFeed is the easiest way to share online, http://friendfeed.com, accessed 8 May 2009.
[Goffman 1959]
Goffman, E.: The Presentation of Self in Everyday Life, Doubleday Anchor Books, Garden City, New York, 1959.
[Grimmelmann 2009]
Grimmelmann, James Taylor Lewis: Facebook and the Social Dynamics of Privacy, *Iowa Law Review*, Vol. 95, No. 4, May 2009, http://ssrn.com/abstract=1262822.
[Kuczerawy et al. 2008]
Kuczerawy A., Pekárek M., Pötzsch S., Roosendaal A.: Privacy and Access Control in Social Software, *PrimeLife Heartbeat 1.2.2*, November 2008.
[New York Times 2006]
For Some, Online Persona Undermines a Résumé, http://www.nytimes.com/2006/06/11/us/11recruit.html?pagewanted=all, accessed 7 May 2009.
[OAuth 2009]
http://oauth.net, accessed 19 June 2006.
[OpenID 2009]
http://openid.net, accessed 19 June 2006.
[PRIME 2008]
PRIME Project: Requirements for Privacy Enhancing Tools, 3rd version, chapter 3, https://www.prime-project.eu/prime_products/reports/reqs/pub_del_D1.1.d_final.pdf, March 2008.
[Pekarek and Pötzsch 2009]
Pekárek M., Pötzsch S.: Comparison of Privacy Issues in Collaborative Workspaces and Social Networks, *Identity in the Information Society*, special issue on Social Web and Identity, Springer Netherlands, to appear 2009.
[Response to Art.29]
Response to the Article 29 Working Party Opinion On Data Protection Issues Related to Search Engines, 8 September 2008, http://64.233.179.110/blog_resources/google_ogb_article29_response.pdf, accessed 13 May 2009.
[Reyna and Farley 2006]
Reyna, V.F, Farley, F.: Risk and Rationality in Adolescent Decision Making. Implications for Theory, Practice, and Public Policy, *7:1 Psychological Science in the Public Interest 2*, 2006
[Sophos 2007]
Sophos Facebook ID probe shows 41% of users happy to reveal all to potential identity thieves, http://www.sophos.com/pressoffice/news/articles/2007/08/facebook.html, accessed 7 May 2009.
[Spitz et al. 2008]
Spitz St., Hinz W., Bergfeld M.-M.: Infrastructures for Trusted Content, *PrimeLife Deliverable 6.2.1*, August 2008.
[Tönnies 1965]
Tönnies, F.: Einführung in die Soziologie, Ferdinand Enke Verlag, Stuttgart, 1965.
[Van Alsenoy et al. 2009]
Van Alsenoy B., Ballet J., Kuczerawy A.: Social networks and web 2.0: are users also bound by data protection regulations?, forthcoming.
[Wong and Savirimuthu 2008]
Wong R. and Savirimuthu J.: All or Nothing: This is the Question? The Application of Art. 3(2) Data Protection Directive 95/46/EC to the Internet, *John Marshall Journal of Computer*

& Information Law, Vol. 25 No. 2, 2008, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1003025, accessed 13 May 2009.

[boyd 2007]

boyd, danah: Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life *MacArthur Foundation Series on Digital Learning – Youth, Identity, and Digital Media Volume* (ed. David Buckingham), MIT Press, http://www.danah.org/papers/WhyYouthHeart.pdf, 2007.