Privacy Enabled Communities

Editors:	Bibi van den Berg, (TILT)
	Ronald Leenes, (TILT)
Reviewers:	Dave Raggett, (W3C)
	Leif-Erik Holtz, (ULD)
Identifier:	D1.2.1
Type:	Deliverable
Version:	Final
Class:	Public
Date:	March 15, 2010

Abstract

In this deliverable we present an analysis of the ways in which individuals use two types of web 2.0 environments, collaborative workspaces and social network sites, to construct and express identities, to manage relationships and to cooperate in the creation and dissemination of content. We investigate which privacy issues may arise in relation to these activities and provide a number of possible solutions for these issues. We also present the three demonstrators we have built to contribute to solving some of the issues with regard to privacy and identity management in collaborative workspaces and social network sites. Deliverable 1.2.2, which accompanies this one, provides a detailed and technical description of these three 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° 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

This deliverable has been jointly authored by multiple PrimeLife partner organisations. The following list presents the contributors for the individual parts of this deliverable.

Chapter	Author(s)
Executive Summary	Ronald Leenes (TILT)
Chapter 1: Introduction	Bibi van den Berg (TILT)
Chapter 2: Identity and sociality in web 2.0	Bibi van den Berg (TILT) Ronald Leenes (TILT) Stefanie Pötzsch (TU Dresden) Martin Pekárek (TILT)
Chapter 3: Privacy: A complicated yet valuable concept	Bibi van den Berg (TILT)
Chapter 4: Privacy in collaborative workspaces	Stefanie Pötzsch (TU Dresden) Bibi van den Berg (TILT)
Chapter 5: Privacy in social network sites	Bibi van den Berg (TILT) Martin Pekárek (TILT) Ronald Leenes (TILT) Arnold Roosendaal (TILT)
Chapter 6: Legal aspects of social network sites and collaborative workspaces	Aleksandra Kuczerawy (KU Leuven) Bibi van den Berg (TILT) Ronald Leenes (TILT)
Chapter 7: Towards a privacy-enhanced web 2.0	Bibi van den Berg (TILT) Katrin Borcea-Pfitzmann (TU Dresden) Stefanie Pötzsch (TU Dresden) Filipe Beato (KU Leuven)
Chapter 8: Legal issues in Scramble!	Sandra Olislaegers (TILT) Ronald Leenes (TILT) Bibi van den Berg (TILT)
Chapter 9: Conclusions	Bibi van den Berg (TILT)

Executive Summary

This deliverable presents the theoretical and analytical work with respect to privacy and social communities in online worlds carried out in PrimeLife Work Package 1.2 in 2008 and 2009. This deliverable (D 1.2.1) should be considered in conjunction with D 1.2.2, entitled '*Privacy-enabled Communities Demonstrator*' which describes the demonstrators that were developed in the same period.

The document consists of 9 chapters. *Chapter 2 – Identity and sociality in web 2.0* explores the notion of web 2.0. Its key characteristics and expressions are discussed in light of three general goals of web 2.0 applications as distinguished by Richter and Koch (2007): information management, management of the self (or identity management), and relationship management. These three goals are embodied in collaborative workspaces such as forums and wikis on the one hand, which revolve predominantly around information management, and social network sites on the other, which revolve around both the management of the self and relationship management. Both of these new web 2.0 domains, as well as their similarities and differences are discussed. Social network sites and collaborative workspaces are the technology platforms on which the current deliverable focuses. More specifically, we have limited our attention to the truly *social* web 2.0 applications, because this is the realm where most of the privacy issues arise within WP 1.2's focus. Hence more individually oriented web 2.0 applications, such as blogs, are only marginally addressed in this deliverable. Some of the analyses and findings, however, do also apply to these self-management technologies. Besides a discussion of web 2.0, this chapter explores our conception of identity, which is based on an interactionist perspective – identities are constructed and expressed in and through *interactions* between people. We argue that the internet has been used extensively as a platform for self-expression, experimentation and exploration from its earliest days onwards. Identity and identity management also play an important role in social network sites and collaborative workspaces.

Chapter 3 – Privacy: A complicated yet valuable concept provides a conceptual analysis of the notion of privacy. In the twentieth century privacy has become a topic of much debate, and a lot of different perspectives on and interpretations of this notion have emerged. The chapter provides an overview of some of its most common definitions and interpretations and sketches our own stance with respect to privacy: we align ourselves primarily with Helen Nissenbaum's interpretation of privacy as 'contextual integrity' (Nissenbaum, 1998, 2004, 2010). In the second part of this chapter we clarify why privacy is an especially relevant topic of debate in a world of modern technology by categorizing a number of the privacy issues that may arise in relation to technology use. These include, for instance, the collection and manipulation of (personal) information on a massive scale, the indefinite storage of information and the possibility of undermining other people's reputation in web 2.0. We conclude the chapter by providing a model that was developed by Bennett and Raab (2006) to come to a better understanding of the causes of privacy problems.

Chapters 4 and 5 discuss the focal web 2.0 domains in more detail with an emphasis on the specific privacy issues in each of them. *Chapter 4 – Privacy in collaborative workspaces* provides an analysis of possible privacy threats that may arise for users and participants in collaborative workspaces. Three possible privacy attackers are distinguished: (1) third parties, (2) other users of the same collaborative workspace, and (3) the providers of these workspaces. As an illustration privacy issues in two major types of collaborative workspaces, Wikipedia and the phpBB forum are discussed. The second part of the chapter provides a number of general requirements for (a next generation of) collaborative workspaces to make them more privacy-friendly for users participating in them. The chapter concludes with a focus on one type privacy-enhancement: access control. Mechanisms of access control enable users to decide who has access to the content

they share in collaborative workspaces. We explain the different approaches to building and administering mechanisms for access control and propose our own alternative, which is elaborated upon in the phpBB.de demonstrator (discussed in chapter 7).

Chapter 5 – Privacy in social network sites provides an analysis of privacy issues in social network sites such as Facebook, MySpace, LinkedIn and Friendster. We argue that these issues arise on three levels: (1) between users, (2) because of actions (or lack thereof) by the provider of the social network site, and (3) because of actions (or lack thereof) by third parties. Each of these levels is discussed in detail and, similar to the previous chapter, a set of requirements for (a next generation of) social network sites to make them more privacy-friendly is presented. These requirements provide the foundation for the Clique demonstrator (see chapter 7).

Chapter 6 – *Legal aspects of social network sites and collaborative workspaces* provides an analysis of the European legal frameworks and directives that are relevant to the two focal web 2.0 technologies of this deliverable, i.e. social network sites and collaborative workspaces. These are the general Data Protection Directive 95/46/EC; the e-Privacy Directive 2002/58/EC; the Data Retention Directive 2006/24/EC; e-Commerce Directive 2000/31/EC, and the Copyright Directive 2001/29/EC. The legal issues relating to our primary web 2.0 applications, predominantly with respect to privacy, are explored. Attention is also paid to legal issues relating to, for instance, copyright and e-commerce. While we discuss both social network sites and collaborative workspaces as relevant technologies for legal inspection in this chapter, in some sections the focus is on social network sites alone. The reason for this is that we have found that, due to their complexity and the high degree of explicit sharing of personal information, social network sites are more prone to create legal issues than collaborative workspaces. However, since legal issues may also arise in collaborative workspaces, we have chosen to discuss both technologies in the overall structure of this chapter.

Chapter 7 – Towards a privacy-enhanced web 2.0 introduces three demonstrators built within Work Package 1.2 to provide pointers for solving some of the issues with respect to privacy and identity management that were discussed in the previous chapters of this deliverable. Specifically, we introduce (1) a phpBB extension that we have built for users of phpBB forum software, which enables them to have fine-grained access control over the content they post in the forum; (2) a social network site demonstrator called Clique, in which we present a number of mechanisms for so-called 'audience segregation' and the preservation of 'contextual integrity' (these terms will be explained in detail in Chapters 5 and 3 respectively); and (3) Scramble!, a browser add-on that can encrypt any information shared by users in forms or fields, so that it becomes unreadable for anyone other than the intended audience.

Chapter 8 – Legal aspects of Scramble! discusses the legal aspects regarding the release of the Firefox plug-in Scramble! to the public at large. The chapter discusses the legal issues from the perspective of Scramble! being used in conjunction with US based social network site Facebook. It discusses crypto regulation both in the EU and the US, potential export restrictions and whether Scramble! encrypted data is protected against legal decryption orders. The conclusions seem to be different for the different EU member states. The chapter also discusses Scramble! in light of Facebook's Terms of Service. One conclusion is that there are various provisions that Facebook could employ to effectively ban the use of Scramble! or the scrambled content.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

This deliverable presents the theoretical and analytical work we have conducted within Work Package 1.2 of the PrimeLife project in 2008 and 2009 with respect to privacy and social communities in online worlds. It is accompanied by a second deliverable, entitled '*Privacy-enabled Communities Demonstrator*' (D1.2.2) in which the demonstrators, i.e. the practical applications and tools we have developed in light of the findings presented in this deliverable, will be discussed.

1.1 Privacy and web 2.0

In recent years a wide variety of web applications, environments and forums have emerged that together have loosely become known as 'web 2.0'. One often quoted definition of web 2.0, formulated by web 2.0 guru Tim O'Neill in 2005, is that it refers to a "*set of economic, social, and technological trends, that collectively form the basis of the next generation of the Internet – a more mature, distinct medium characterized by user participation, openness, and network effects*" (Tim O'Neill, cited in Mergel *et al.*, 2009: 3-4). The loose formulation of this definition points to one of the key difficulties in grappling with this new phenomenon: there is a variety of characterisations and descriptions of web 2.0 in the literature on the subject, and a range of technological, economic and social developments are included in the discussion of this next generation of the internet (cf. Aguiton and Cardon, 2007; Heng *et al.*, 2007; Lastowka, 2008; Mabillot, 2007; Mergel *et al.*, 2009; O'Reilly, 2007). However, there are four characteristics that can be distilled from almost all of them. We will discuss them briefly here and return to a more in-depth discussion in Chapter 2.

First of all, in contrast to older internet applications and sites (now collectively called 'web 1.0') the *end user* has come to play a central role in web 2.0. While users were mostly passive consumers of information and entertainment services in web 1.0 a wide range of new possibilities has emerged that enable them to interact and share their own knowledge and information (stories, pictures, music, movie clips and so on and so forth) with other people. Blogs, YouTube movies, wikis, file-sharing and consumer reviews are examples of this trend. Users are no longer merely consumers, but can now also become producers of information and entertainment services. In web

2.0 they are therefore regularly called ‘prosumers’ (Tapscott, 2009: 208; Toffler, 1980), a contraction of the words ‘producer’ and ‘consumer’.

Second, web 2.0 is characterised by a high degree of *sociality* – this is why web 2.0 is sometimes also called ‘the social web’. Again, whereas web 1.0 revolved largely around the passive and solitary consumption of information and entertainment, web 2.0 is not just about sharing knowledge and information, but also about engaging in interactions with other people, for instance based on a shared interest (as is the case in most internet forums), but also through social network sites, in which users can present a profile page of themselves and engage in contact with both known and unknown others within the same network.

Third, the combination of the first two characteristics (active end users and social interaction) entails that in many web 2.0 environments the production and dissemination of information and entertainment services has a highly *co-operative* character. Participation is one of the key aspects of web 2.0. Prosumers create information together in joint projects, for instance in building an encyclopaedia (Wikipedia), or in generating software for others to use (open source). This co-operative, joint process of information creation and dissemination leads to a much more dynamic internet than the largely static web 1.0.

Last, one of the major technical differences between web 1.0 and web 2.0 is the fact that technology developers now create applications that are *embedded* into the internet, and are accessible via any browser. In the first generation of internet technologies competition between the major product developers revolved around creating browsers and desktop applications for users to access the net. Think for instance of Microsoft (Internet Explorer), Netscape (Navigator) and Oracle and SAP. In the second generation of the internet businesses create native web applications instead: applications that can be accessed by any user, for any kind of operating system, through any kind of browser. Businesses such as Google, Flickr and eBay were integrated into the web as native web-applications or environments from the get-go. The internet has thus turned into a *platform* from which users can start up a wide variety of tasks, queries and activities (O'Reilly, 2007: 19-21).

Since web 2.0 is a new phenomenon – the term was first coined in 1999 but the massive take-of of this latest generation of the internet is only a few years old – much is still to be learned with regard to both the benefits and the risks for users, businesses and governments in this new domain. Privacy issues relating to modern technologies have been high on the agenda of both government officials around the world, researchers, and the broader public, and for good measure, and it is obvious that the emergence of web 2.0 currently generates a wide range of new issues relating to privacy and security. In this deliverable we discuss our research on the construction, expression and management of identities in web 2.0 applications, and the privacy issues that arise in that area. In particular, we focus on two paradigmatic web 2.0 environments: social network sites (or social network sites for short) and collaborative workspaces (or CWs for short).

With this document we hope to have contributed to creating a better understanding of some of the issues by analysing them and developing a theoretical and analytical stance with which they can be attacked. We have also translated these theoretical and analytical findings into three practical tools, the so-called demonstrators, which will be discussed in the deliverable that accompanies this one (D1.2.2).

1.2 Overview of this deliverable

This deliverable consists of 9 chapters. In *Chapter 2*, called *Identity and sociality in web 2.0* we begin by delving a little deeper into the notion of web 2.0. We will discuss its key characteristics and expressions and distinguish between three general goals of web 2.0 applications, which we

base on the work of Richter and Koch (Richter and Koch, 2007): information management, management of the self (or identity management), and relationship management. These three goals are embodied in collaborative workspaces such as forums and wikis on the one hand, which revolve predominantly around information management, and social network sites on the other, which revolve around both the management of the self and relationship management. We will introduce both of these new web 2.0 domains and discuss their similarities and differences. In the rest of this deliverable social network sites and collaborative workspaces will form the technological focus. We have chosen to limit ourselves to the truly *social* web 2.0 applications, because this is the realm where most of the privacy issues arise. Hence more individually oriented web 2.0 applications, such as blogs, will not or only marginally be addressed in this deliverable. However, our analyses and findings regularly also apply to these self-management technologies. After our discussion of web 2.0 we will introduce our conception of identity. Since there are many conceptions and theories of identity in social science and philosophy we will introduce our own perspective on this difficult and highly diffuse notion, and explain why this perspective is relevant and productive in studying identity in online worlds. We will show how the internet has been used extensively as a platform for self-expression, experimentation and exploration from its earliest days onwards, and at the end of this chapter we will describe the role of identity and identity management in social network sites and collaborative workspaces.

In *Chapter 3*, called *Privacy: A complicated yet valuable concept* we start with conceptual analysis of the notion of privacy. In the twentieth century privacy has become a topic of much debate, and a lot of different perspectives on and interpretations of this notion have emerged. We provide an overview of some of its most common definitions and interpretations and sketch our own stance with respect to privacy: we align ourselves primarily with Helen Nissenbaum's interpretation of privacy as 'contextual integrity' (Nissenbaum, 1998, 2004, 2010). In the second part of this chapter we clarify why privacy is an especially relevant topic of debate in a world of modern technology by categorizing a number of the privacy issues that may arise in relation to technology use. These include, for instance, the collection and manipulation of (personal) information on a massive scale, the indefinite storage of information and the possibility of undermining other people's reputation in web 2.0. We conclude the chapter by providing a model that was developed by Bennett and Raab (2006) to come to a better understanding of the causes of privacy problems.

In the two chapters that follow we will turn to each of the web 2.0 domains that we have chosen in turn and address the specific privacy issues in each of them in much greater detail. In *Chapter 4*, called *Privacy in collaborative workspaces* we start by analysing possible privacy threats that may arise for users and participants in collaborative workspaces. Three possible privacy attackers are distinguished: (1) third parties, (2) other users of the same collaborative workspace, and (3) the providers of these workspaces. We present two examples of collaborative workspaces, Wikipedia and the phpBB forum, and discuss the privacy problems that may arise in each. In the second part of the chapter we distil a number of general requirements that could be developed for (a next generation of) collaborative workspaces to make them more privacy-friendly for users participating in them. We end the chapter with a focus on one type privacy-enhancement: access control. Mechanisms of access control enable users to decide who has access to the content they share in collaborative workspaces. We explain the different approaches to building and administering mechanisms for access control and propose our own alternative.

In *Chapter 5* called *Privacy in social network sites* we study privacy issues in social network sites such as Facebook, MySpace, LinkedIn and Friendster. We argue that these issues arise on three levels: (1) between users, (2) because of actions (or lack thereof) by the provider of the social network site, and (3) because of actions (or lack thereof) by third parties. We discuss each of these levels in detail and, similar to what we've done in the previous chapter, we then present a set of requirements for (a next generation of) social network sites to make them more privacy-friendly.

In Chapter 6, called *Legal aspects of social network sites and collaborative workspaces* we analyze which European legal frameworks and directives are relevant to the two focal web 2.0 technologies of this deliverable, i.e. social network sites and collaborative workspaces. We investigate which legal issues could arise in these web 2.0 environments, predominantly with respect to privacy, but we also cast the net a little wider and look at legal issues relating to, for instance, copyright and e-commerce. While we discuss both social network sites and collaborative workspaces as relevant technologies for legal inspection in this chapter, in some sections the focus is on social network sites alone. There reason for this is that we have found that, due to their complexity and the high degree of explicit sharing of personal information, social network sites are more prone to create legal issues than collaborative workspaces. However, since legal issues may also arise in collaborative workspaces, we have chosen to discuss both technologies in the overall structure of this chapter.

In *Chapter 7* called *Towards a privacy-enhanced web 2.0* we introduce three demonstrators that we have built within Work Package 1.2 to provide pointers for solving some of the issues with respect to privacy and identity management that have been discussed in the previous chapters of this deliverable. Specifically, we introduce (1) a phpBB extension that we have built for users of phpBB forum software, which enables them to have fine-grained access control over the content they post in the forum; (2) a social network site demonstrator called Clique, in which we present a number of mechanisms for so-called 'audience segregation' and the preservation of 'contextual integrity' (these terms will be explained in detail in Chapters 5 and 3 respectively); and (3) Scramble!, a browser add-on that can encrypt any information shared by users in forms or fields, so that it becomes unreadable for anyone other than the intended audience.

In *Chapter 8* called *Legal aspects of Scramble!*, we delve into the legal consequences of using Scramble! in more detail. Specifically, we investigate the legal consequences of disseminating Scramble! within the European Union and in the United States respectively. We analyze existing legislation with respect to encryption, the export of encryption mechanisms, and a possible clash between the order to decrypt and individuals' right against self-incrimination.

We end this deliverable with *Chapter 9*, in which our conclusions are presented, along with an outline of suggestions for further research.

Chapter 2

Identity and sociality in web 2.0

Social network sites (SNSs) and collaborative workspaces (CWs) are the central focus of this deliverable. We investigate which issues relating to identity and privacy arise in both, and provide theoretical and practical solutions for overcoming some of these issues. In this chapter we outline our perspective on identity and identity management in online worlds. Since social network sites and collaborative workspaces are two central components of a new generation of internet applications and environments that have collectively come to be known as 'web 2.0', we begin by sketching the landscape of this new generation of the internet (section 2.1). We will introduce the two central pillars of this research: collaborative workspaces and social network sites, describe both their similarities and their differences (section 2.2), and then discuss each in more detail in turn 2.3 - 2.4).

After that we will turn to the highly social character of identity construction and expression in the early-twenty-first century, in a world that is filled with information and communication technologies. We will argue that ever since its earliest advent the internet has been used by individuals to express, construct and experiment with identities in myriad ways. We will show the ways in which social network sites and to a somewhat lesser degree other web 2.0 environments, such as collaborative workspaces, figure in identity construction and expression (section 2.5).

2.1 Web 2.0: An introduction

Time Magazine has a long tradition of choosing a person of the year, someone who has played a key role in events of that particular year, either in a good or a bad sense. In 2006 the magazine chose not to nominate one of the 'usual suspects', such as politician scientists or other opinion makers, but instead proclaimed that YOU, the reader and user of modern information and communication technologies, were person of the year 2006.[1] With this election *Time Magazine* acknowledged a role-shift of individual computer users in creating and shaping the world they inhabit through the use of modern information and communication technologies. According to the

[1] See http://www.time.com/time/covers/0,16641,20061225,00.html for the cover of that specific edition of Time Magazine, and http://www.time.com/time/magazine/article/0,9171,1569514,00.html for the article [last accessed on 15 March 2010].

magazine 2006 manifested "*community and collaboration on a scale never seen before. It's about the cosmic compendium of knowledge Wikipedia and the million-channel people's network YouTube and the online metropolis MySpace. It's about the many wresting power from the few and helping one another for nothing and how that will not only change the world, but also change the way the world changes. The tool that makes this possible is the World Wide Web. Not the Web that Tim Berners-Lee hacked together (15 years ago, according to Wikipedia) as a way for scientists to share research. It's not even the overhyped dotcom Web of the late 1990s. The new Web is a very different thing. It's a tool for bringing together the small contributions of millions of people and making them matter. Silicon Valley consultants call it Web 2.0, as if it were a new version of some old software. But it's really a revolution*" (Grossman, 2006).

But what is this 'web 2.0' and why is it so important? As said in Chapter 1 web 2.0 is a complicated concept, and one that is used in a wide variety of contexts to mean a range of different things. Tim O'Neill has defined it as a "*set of economic, social, and technological trends, that collectively form the basis of the next generation of the Internet – a more mature, distinct medium characterized by user participation, openness, and network effects*" (Tim O'Neill, cited in Mergel *et al.*, 2009: 3-4). However, this is still a rather loose definition. O'Reilly is aware of this fact, and in a 2007 article rightly remarks that we should maybe view web 2.0 as a "*gravitational core*[,] *a set of principles and practices that tie together a veritable solar system of sites that demonstrate some or all of those principles, at a varying distance from that core*" (O'Reilly, 2007: 18-19). This is why we have chosen to describe the key characteristics of this emergent phenomenon, which we've also briefly addressed in Chapter 1: (1) the role of end users, (2) sociality as a key driver, (3) co-operation and the wisdom of crowds, and (4) the web as platform and service.

Before addressing each of these characteristics in some more detail, we would like to begin by retracing the origins of the concept of 'web 2.0'. There is some debate about who coined the term web 2.0. While most researchers attribute this concept to O'Reilly Media, Tim O'Reilly's media company, there is in fact an earlier use of the term in Darcy DiNucci's 1999 article called *Fragmented Future*. DiNucci wrote: "*The Web we know now, which loads into a browser window in essentially static screenfulls, is only an embryo of the Web to come. The first glimmerings of Web 2.0 are beginning to appear, and we are just starting to see how that embryo might develop. The Web will be understood not as screenfulls of text and graphics but as a transport mechanism, the ether through which interactivity happens. It will* [...] *appear on your computer screen,* [...] *on your TV set* [...] *your car dashboard* [...] *your cell phone* [...] *hand-held game machines* [...] *maybe even your microwave oven*" (DiNucci, 1999).

However, DiNucci's use of the term web 2.0 was not picked up by the broader public. Then, in 2004, Dale Dougherty, the VP at O'Reilly Media used the term web 2.0 in a brainstorming session with MediaLive International, another media company. He noted that "*far from having 'crashed'* [in the wake of the dot-com bubble]*, the web was more important than ever, with new applications and sites popping up with surprising regularity.* […] *Could it be that the dot-com collapse marked some kind of turning point for the web, such that a call to action such as 'web 2.0' might make sense?*" (O'Reilly, 2007: 17). The participants in this brainstorm decided to organise an annual conference on this next generation of the internet, and from that time onwards the concept spread far and wide, and at a rapid pace.

Web 2.0 has been declared a hype or buzz word by several renowned scientists and technology developers, because it has come to mean a wide variety of things for businesses trying to be hip and attract customers. However, there is most certainly a core of a number of ideas that surface time and again when studying research literature on the subject. We have briefly introduced these ideas in Chapter 1 and will now discuss them in some more detail.

2.1.1 The role of end users

One of the first characteristics of web 2.0 that is mentioned in articles discussing this new phenomenon is the increasingly central role given to the *end users* of the internet in creating, sharing, ranking, and organizing content, products and services (cf. Howe, 2008; Leadbeater, 2008; Shirky, 2008; Weinberger, 2007). Whereas the first generation of the internet, now often retrospectively called 'web 1.0', was highly static and focused predominantly on the spread of information by businesses and non-profit organizations to the public at large, web 2.0 is characterized by the fact that users have become actively involved in a dynamic, open-ended, actively maintained world of services and information portals. In the words of Mergel *et al.* "[w]*hat many of the high-profile Web 2.0 sites have in common is that they harness the productive power of their users*" (Mergel *et al.*, 2009: 9). This participation comes in a wide variety of forms and degrees. For instance, users collectively rank products and information, either consciously and explicitly (e.g. on book-selling websites such as Amazon.com), or unconsciously and implicitly (e.g. through clicking on a link after conducting a search in Google; the more often a link is chosen, the higher it will rank when the same search terms are entered in a new search). They share media, such as video fragments via YouTube or pictures via Flickr, and their stories and ideas on virtually any topic via personal blogs. But they also work on open source software development projects and thus form so-called "*user-centered innovation networks*" (Von Hippel, cited in Mergel *et al.*, 2009: 12). And as we will see below users also collectively work on the creation and management of information databases, such as the online encyclopaedia Wikipedia and other collaborative workspaces.

One of the most interesting aspects of the central role of end users in web 2.0 is the level of self-organization that is accomplished in this second generation of the internet, and the ways in which it comes about. For most web 2.0 communities and environments there is no central organization, no preconceived plan or goal, and no structural or financial backing. Moreover, "*one of the main characteristics of* [web 2.0 communities and services] *is the fact that the rules and norms* [that govern them] *are produced by users themselves*" (Aguiton and Cardon, 2007: 56). Thus, web 2.0 communities become a kind of ecosystem, in which people act in a range of roles, for instance as developers or testers of new software that is embedded in the environments, either for all to use or aimed at specific communities.

As said, in web 2.0 end users become actively engaged in the production and distribution of information and entertainment services . They have now come to be labelled as 'prosumers', a contraction of 'consumer' and 'producer'. The term prosumer was coined by Marshall McLuhan in 1972, and developed further by Alvin Toffler in *The Third Wave* (Toffler, 1980). It can be defined as follows: "*Prosumerism is more than an extension of mass customization, customer centricity, or any of the other terms that boil down to companies making basic products and letting customers tweak the details. It's what happens when producers and consumers both actively participate in the creation of goods and services in an ongoing way*" (Tapscott, 2009: 208). While producers have always listened to the wishes of ('the average') consumers when developing or redesigning products, web 2.0 technologies enable users to participate in these processes to a much higher degree, and even to create products and services themselves that businesses have not developed (yet). As Tapscott, who has written extensively on prosumerism, writes: "*Today we have the mass-collaboration and mass-communications technologies that allow* [interest-based communities] *to function and flourish. If it's good enough, other people will want it – and the innovator becomes a prosumer overnight. With the onset of Web 2.0, blogs, wikis, and* […] *cheap video editing software and simpler interface tools, are increasing the opportunities for prosumerism. As the tools available to consumers grow ever more similar to those the 'professionals' use, anyone with the skills and interest can leverage them to create a new idea, service, or thing. Thanks to the democratization of technology availability, not only do the tools now exist, but everyone has access to them*" (Tapscott, 2009: 209).

The role of end users in contributing to the production of new information, knowledge, products and services can also be seen in the web 2.0 concept of "crowdsourcing" (cf. Howe, 2008). Crowdsourcing has been defined as "*the act of taking a job traditionally performed by a designated agent (usually an employee) and outsourcing it to an undefined, generally large group of people in the form of an open call*" (J.A. Howe, cited in Mergel *et al.*, 2009: 13). In the case of crowdsourcing companies place a call online for users to contribute to solving a particular problem for which the company itself does not have the resources or time. It differs from other open source projects in the sense that the solution to the problem becomes the property of the company, rather than that of the collective open source users. Moreover, as Mergel *et al.* note, crowdsourcing initiatives are often competitions between users for the best possible solution, at the request of a company, rather than peer-to-peer co-production efforts (idem : 14), which we will encounter in more detail below.

2.1.2 The social web

Web 2.0 has often been called the 'social web'. This name is apt, first of all, because of the highly co-operative character of much of the online activities that users engage in on the internet today, as we will see in more detail in the next paragraph. But it is also an apt descriptor in the sense that ever increasing numbers of individuals worldwide use the internet to engage in contact with other people. The web has become a platform for social interaction through a host of different kinds of environments, ranging from online games and virtual worlds, to social network sites, dating sites, job-hunting and other professional communities, hobby or interest groups, and various forms of collective action groups (Benkler, 2006).

All of these web communities and environments provide platforms for individuals to engage in social contact with known or unknown others – some explicitly aim at bringing together who don't know each other in the physical world (dating sites being the most obvious example), whereas others provide an extension of and a new channel for engaging in contact with others one already knows. Social network sites, which form one of the focal technologies of this deliverable, are an example of the latter. Research has shown that these sites provide people with an added channel of communication with others in their current social web of relations, on top of, for instance, using a telephone, e-mail, SMS or seeing them face-to-face. But at the same time these sites also enable users to find individuals long lost from their active web of social relations, such as old school friends. In both cases *relationality* is one of the core features of these environments (Aguiton and Cardon, 2007: 55).

But web 2.0 is not simply called the social web because individuals use it to engage in contact with others, or build and maintain relationships with them. After all, for several decades now significant amounts of people have turned to networked software platforms or virtual worlds (either on the internet of console based) for these same purposes – think for instance of the use of the message boards and multi-user domains (MUDs) in the early days of the internet. Of course, in web 2.0 the variety of social interaction mechanisms and opportunities has increased dramatically, and so has the number of people using them worldwide. What makes the new generation of the internet 'social' is also that users have begun to cluster and gather on an ad hoc basis and on a massive scale to share and create content, or organise themselves around a shared topic of interest or a political goal. We will look at this aspect of the social web in more detail in the next paragraph.

2.1.3 We create the web! Co-operation in online communities

The combination of the two characteristics of web 2.0 that we have described above – i.e. the central role of end users in producing, managing and distributing information on the web and the strong focus on sociality leading some to call web 2.0 the social web – implies a third important characteristic of this new generation of the internet: the emphasis on *co-operation*, on the joint creation and circulation of knowledge, information, products and services. Interestingly, there is a fundamental shift in the ways in which this co-operation comes about and what it leads to. Aguiton and Cardon remark that co-operation is traditionally linked with notions such as community and organisation, and that co-operating involves a *strong* sense of community, based on "*common sociability and a set of roles*" (Aguiton and Cardon, 2007: 51). However, in web 2.0 the notion of co-operation, and hence community building, takes a new form, according to these authors. They write: "*...the success of Web 2.0 services shows that its users mobilise much weaker cooperation between individuals. Web 2.0 services allow individual contributors to experience cooperation* ex post*. The strength of the weak cooperation comes from the fact that it is not necessary for individuals to have an* ex ante *cooperative action plan or altruist preoccupation. They discover cooperative opportunities only by making their individual production public, i.e. texts, photos, videos etc.*" (Aguiton and Cardon, 2007: 52, emphasis in the original). This means that communities emerge almost as a side-effect while individuals are co-operating to create the information, products or services they themselves need. Community is thus a result of a collective pursuing its individual, ego-focused goals. The organisation of web 2.0 communities is loose and transitory, but we suspect that the feeling of community is no less real or important for their participants.

It is often argued that one of the key factors that has made web 2.0 into a thriving success is that it reflects the collective intelligence of its worldwide users (cf. O'Reilly, 2007: 22-27), or the "*wisdom of crowds*", to borrow a phrase from Surowiecki (2004). An example of a site that has successfully harnessed this 'wisdom of the crowds' is, first and foremost, Wikipedia, which has surpassed not only the amount of entries of traditional encyclopaedias such as the *Encyclopaedia Britannica*, but according to some, has also become comparable or even better in terms of the quality and objectivity of its content (cf. Giles, 2005; Wilkinson and Huberman, 2007). But businesses have also started incorporating the wisdom of crowds into their online services. One of the earliest, and most famous, examples is the online bookstore Amazon.com. On this bookseller's website consumers can review the products sold. A second layer of consumer feedback is added by enabling users to review the review, by marking it on a scale of 'very helpful' to 'not helpful'. Many customers appreciate these reviews by fellow readers because of the extra information they provide with respect to the content of the book, and because it enables them to reflect "*the reviewers' needs and expertise against their own*" (Leino and Räihä, 2007, 139). This enables them to weigh their choice of buying the product more effectively.

2.1.4 The web as platform and software as service

The last characteristic we would like to discuss is the transition from the first generation to the second generation of the internet is that the web has now turned into a *platform* which hosts a wide variety of embedded applications and services. In web 1.0 technology businesses focused on creating stand-alone applications through which users could get *access* to the internet. Microsoft's Internet Explorer or Netscape's Navigator are examples in case. Web 2.0 guru O'Reilly explains the transition from web 1.0 to web 2.0 by comparing Netscape, which he typifies as 'the' web 1.0 standard bearer to Google, which he argues embodies web 2.0. Netscape Navigator, he writes, was the company's "*flagship product* […]*, a desktop application, and* [its] *strategy was to use* [its]

dominance in the browser market to establish a market for high-priced server products" (O'Reilly, 2007: 19). By contrast, Google never built a desktop application but started out as a "*native web application*", which "*never sold or packaged, but delivered as a service, with customers paying, directly or indirectly, for the use of that service. None of the trappings of the old software industry are present. No scheduled software releases, just continuous improvement. No licensing or sale, just usage. No porting to different platforms so that customers can run software on their own equipment, just a massively scalable collection of commodity PCs running open source operating systems plus homegrown applications and utilities that no one outside the company ever gets to see*" (O'Reilly, 2007: 20).

Related to this idea of the web as a platform of the key characteristics of the second generation of the internet is the ever increasing degree of *interoperability* and *interconnectedness* between different web applications and environments. Users can access different types of content (audio, video, text, pictures) within the same platform and distribute them via a host of channels to anyone who wishes to participate. Micro-blogging services such as Twitter.com increasingly enable users to access their service from other social network sites such as Facebook, thus increasing accessibility and, as a consequence, popularity and frequency of use. To an ever larger degree, therefore, the internet is no longer "*a medium supplied by millions of isolated sites*", but rather "*a platform for the free exchange of information and content produced, edited and distributed by internet surfers, belonging to organised communities and brought together by common interests*" (Mabillot, 2007: 39).

2.2 The web 2.0 triangle

The backbone of the new generation of the internet is often called 'social software'. Both collaborative workspaces and social network sites are examples of social software. In this section we will look into the notion of social software in more detail and shed light on the similarities and differences between social network sites and collaborative workspaces.

2.2.1 What is social software?

The term social software refers to infrastructures, platforms and applications that enable users to communicate and collaborate in networks, to establish and maintain relationships and thus in some way to map social aspects of real life to an online environment (cf. Benkler, 2006: 372-375). Schmidt defines social software as web-based applications that support the management of information, the management of relationships and the representation of one's self or identity to (a part of) the public in hyper-textual and social networks (Schmidt, 2006). Thus, three primary functions of social software can be identified (Richter and Koch, 2007):

- *Information management*: finding, evaluating and administrating information;
- *Self-management* or the management of identities: presenting (aspects of) yourself on the internet
- *Relationship management*: (re)engaging in and maintaining social relations with others via internet.

These three primary functions are visualized in triangle in Figure 1:

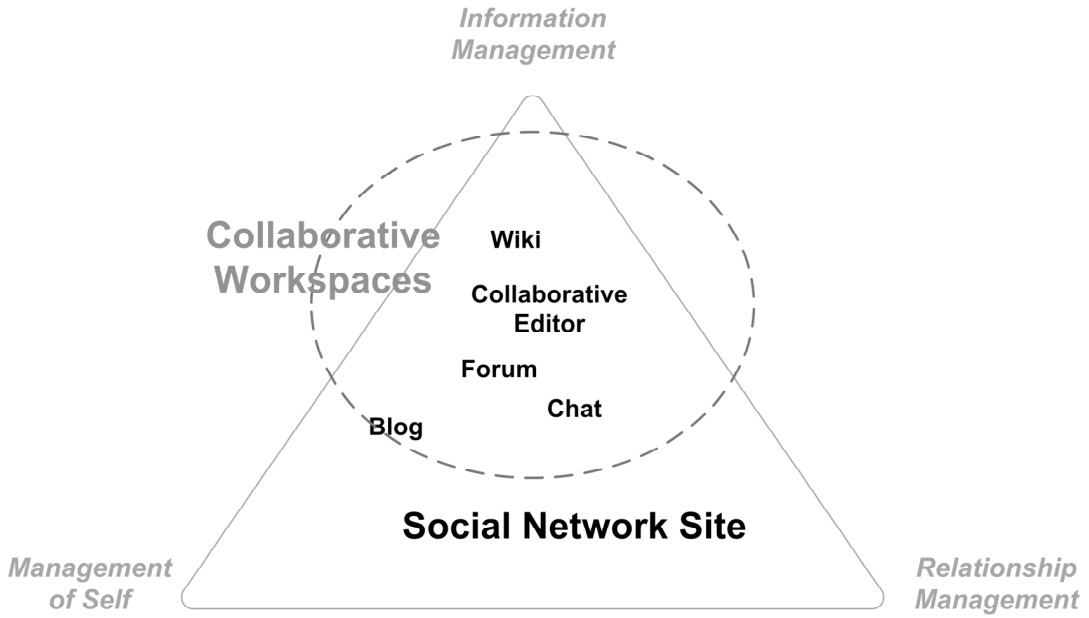


Figure 1: The functional triangle of social software, based on (Richter and Koch, 2007).

In light of the differences between these three functions, we distinguish between distinct types of social software applications. On the one hand we consider so-called 'collaborative workspaces', which encompass applications that primarily focus on the creation, management and dissemination of *content*, which is created in a collaborative manner (Pankoke-Babatz and Syri, 1997). This type of applications aims at supporting information management, and can be found at the top of the triangle in Figure 1.

A second type of social software consists of 'social network sites', which revolve around the self-presentation of social network site members, and the management of relationships between these members (boyd and Ellison, 2007). Since the activities of members of social network sites oscillate between the management of identities and that of relationships this type of social software is positioned in the middle between the left hand and the right hand corner at the bottom of the triangle in Figure 1.

2.2.2 Key differences and similarities between collaborative workspaces and social network sites

Social network sites and collaborative workspaces both aim at supporting users in online collaborations and interactions, but they take a different approach to the idea of collaboration and they serve different goals.

As we have seen above, the key features of social network sites are (1) that they offer an online podium for the presentation of identities through user profiles, and (2) the management of relationships in the form of connections between these profiles. Social network sites revolve around the individual – individual members of these platforms create a personal profile and invite other members of the same network to become their connections. Users can create content – usually related to their profiles, in the form of private messages, listed groups, writings on others' 'wall' or 'pin board' – to present themselves within their group of connections.

Collaborative workspaces start from and revolve around the collective rather than the individual, and they focus on content rather than on connection and self-presentation. The key feature of collaborative workspaces is the collaborative creation, management and dissemination of content. 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, whereas the value of a social network site lies in the network itself.

Table 1 provides an overview of a number of features that both types of social software share and points out differences and similarities in realization.

The features 'content creation and management' and 'user administration' (rows 3 and 4 of Table 1) are inversely important for these particular applications. Theoretically, collaborative workspaces can be realized only with features for creating and managing content and without any user administration. For example, a wiki system can allow everybody to read and modify all articles without any restriction. Vice versa, theoretically, an application that allows people to create profiles and indicate connections could fulfil all mandatory requirements of a social network site without providing additional features for communication and producing content in addition. 'Access control', 'history' and 'events' (rows 4-6 of Table 1) are realized slightly differently in current applications from both types. In any case, these features are subordinate functionalities.

Collaborative workspaces		**Social network sites**
Content is important.	**← key characteristic →**	The *network*, supported by user information and relationships, is important.
Content creation (creating and editing information) in co-operation with other users is a key feature.	**← content creation & management →**	Content creation is a subordinate feature.
User administration is a sub-ordinate feature.	**← user administration →**	User administration (managing a user profile and relations with other people) is a key feature.
If access control is restricted, then access to documents is identity-based, depending on the goal of the document and the knowledge of the user.	**← access control →**	If access control is restricted, then access to profiles is relationship-based, depending on the connection between the user and the profile owner.
The user sees the newest version per default; all former versions of content may also be available.	**← history →**	The user only sees the current version of others profiles and connections. Providers may have former versions stored in databases.
Users can be informed in case of changes made to (specified) content or when new content is available.	**← events →**	Users can be informed when contents changes in their network or when new content is available on their network.

Table 1: A comparison of features for collaborative workspaces and social network sites.

Collaborative workspaces and social network sites are both ICT tools to support interactions between participants. The underlying goals of these interactions may vary considerably. Members who have an account on a social software application aim to maintain social connections or to

share information with others. In order to become part of such a community, it is necessary to disclose at least some personal data that shows who you are, what skills you have and what you are interested in. This disclosure is facilitated directly by profile pages that contain basic information, such as name and age, but also other identity related data, like hobbies and interests, images, and personal opinions as expressed in blogs. Further, personal data is indirectly disclosed when content is provided by the user. This encompasses semantically included information, e.g. someone who writes his real name or place of residence in a forum, as well as writing style, habits of technology usage and other information. The digital availability of this data leads to potential privacy risks, since copying of data and tracing of users is simple and data, once disclosed, is out of control of the data supplier. In the next two chapters we will delve into the privacy issues arising in collaborative workspaces and social network sites respectively. For now, we turn to a more in-depth discussion of what collaborative workspaces and social network sites are (sections 2.3 and 2.4).

2.3 Collaborative workspaces: An overview

As said above, collaborative workspaces are infrastructures and platforms that enable users to work together, for instance in gathering information or creating content in a collaborative manner but also in sharing data with each other. There are a number of different types of applications that can be clustered under the heading of collaborative workspaces. These include knowledge management platform within an electronic environment, or idea generation environments that use computer-supported creativity techniques.

In this section we describe the concept and underlying principles of collaborative workspaces and presents existing infrastructures and tools that can be subsumed under this heading as examples. As we have seen, the focus of a collaborative workspace is on *content*. The fundamental idea behind these environments of co-operation is to *share resources* such as texts, sounds, pictures, movies, and combinations of them. Users of collaborative workspaces are allowed to access, display, move, remove, edit, and create resources in accordance with access control rules. The idea of access control will be discussed extensively in the next chapter, when we turn to presenting privacy issues in collaborative workspaces. For now it suffices to note that, as Pankoke-Babatz and Syri (1997) point out, privacy-friendly collaborative workspaces need to offer features for *member administration, access control, history, and events*.

Member administration and access control are needed to realise authentication and selected access to resources. Keeping track of history and events (for instance, receiving an alert when additions or changes are made to (specific) content in the collaborative workspace) contribute to 'workspace awareness', that is, an awareness of the dynamic and cooperative nature of the platform and a sense of involvement in its core goal, the creation, exchange and maintenance of content. Workspace awareness thus has an impact on the social aspects of collaborative workspaces – it strengthens user's involvements and contributes to interaction and collaboration.

There are several technical systems available that provide the described features and functionalities to qualify as a backbone for establishing collaborative workspaces. They can be grouped into the following categories:

- Wiki systems
- Collaborative real-time editors
- Internet forums
- Chats
- Weblogs

- Comprehensive groupware systems, and
- File sharing systems.

This categorisation is based on functional differences between the applications. We will describe each category and the differences between the various categories in more detail below.

2.3.1 Wiki systems

A wiki is a collection of HTML pages that are modified online by several users. Every wiki page, also called an 'article', can consist of various types of data, such as texts, images, videos, hyperlinks to other resources in the wiki or somewhere else on the internet, etcetera, or combinations of all or some of these. The objective of a wiki is to support users in collaboratively creating and editing content, which is shared with other users, either contributors themselves or just consumers of the information shared in that environment. Wikis also provide history functionality, which facilitates tracking down changes made by specific users, and resetting articles to a previous version, if necessary. Every wiki article has an author – the last user to have made a change –, a timestamp, a unique identifier (also called a 'permalink') and a version number (Kolbitsch, 2006).

While some wikis are accessible and editable without authentication, others use (different levels of) access control. Different kinds of wikis can thus be distinguished. For instance,

- In some wikis read access to contents is *non-restricted* (e.g. http://en.wikipedia.org);
- In some wikis read access *to some pages* of the wiki is restricted (e.g. https://wiki.c3d2.de);
- In some wikis read access is *completely restricted* (e.g. internal wikis of companies).

The same restriction levels hold for write access. In practice, most wikis have restrictions for modifying pages to at least some parts. In these cases an account is needed which includes at least a unique user ID and password in order to be able to modify content. Accounts are either created by users themselves or by a responsible person, e.g. the administrator, who issues accounts to users. In both cases the account data is stored on the wiki server. One of the best-known examples of a wiki system is the online encyclopaedia Wikipedia (http://www.wikipedia.org/), which we have already mentioned a few times above. Wikipedia is realised using Wikimedia software.

2.3.2 Collaborative real-time editors

Collaborative real-time editors are platforms that enable a number of users to compose and edit a shared resource, such as a text-based document, in a synchronous way. Collaborative real-time editors differ from wikis in the sense that they do not use HTML as the language in which documents are composed. Users of collaborative editors can be distributed among several clients that are connected, for example via a network[2].

The shared document is usually separated into several segments (such as sections, paragraphs, and chapters). All users are allowed to read all segments at any time, but concurrent writing in the

[2] To be technically correct: some kind of inter-process communication (e.g. a network) is needed to connect different instances of the client software.

same segment is not allowed, because it might create conflicting contributions. Features for managing the locking, synchronisation and updating of single segments are provided by the software for collaborative editing (Ellis *et al.*, 1991). An example of a collaborative real-time editor is the collaborative text editor Gobby (http://gobby.0x539.de/trac [last accessed on 21 January 2010]).

2.3.3 Internet forums

Internet forums are also known as 'bulletin boards'. These are websites on which users meet to discuss particular topics based on the forum's area of interest. Each entry into a forum made by a user is called a 'post' or 'posting'. When multiple postings refer to the same subtopic they are grouped into a 'thread' (Baechle, 2006). Thus, an internet forum usually consists of a number of threads and can be seen as a collection of collaborative workspaces. In order to submit postings, users usually have to create an account for the internet forum, which requires at least the indication of a (nick-)name and a valid e-mail address. Access control to internet forums can have the same restriction levels as wiki systems (see section 2.3.1 of this deliverable), that is reading and/or writing rights for some, all or none of the threads in the forum. A popular example of internet forum software is phpBB (http://www.phpbb.de), which we will encounter in much greater detail in chapters to come. One of the most important differences between an internet forum and a wiki is that a thread consists of multiple individual postings, expressing the users' opinions, whereas a wiki article is the actual result of collaborative work. In a wiki the collaborative effort comprises creating content together, and this overall goal means that the ideas and opinions and, more importantly, identities of the contributors are of lesser importance than their joint outcome. By contrast, in internet forums the exchange of opinions and ideas is key, which means that the identities and contributions of specific members have much greater value as such. This is also true of the chats tools we will discuss next.

2.3.4 Chats

Chat tools enable users to communicate via text messages with one or more partners in a synchronous manner (Baechle, 2006). Additionally, some tools provide video- and/or audio-streaming, and file exchange. The clients of the users involved in a chat session need to be connected, for instance via a network. When studying chat tools in a more detailed way, three sub-categories can be distinguished:

- '*Instant messengers*': Users of instant messaging tools have a 'lists of contacts', which contains contact information of the other users, such as a messenger ID. Furthermore, it is possible to store the history of communications locally. History files of chat communications can be conceived as documents that have been created in a collaborative manner. Instant messengers allow no editing of communication content after sending. An example of a widely known instant messenger is Skype (http://www.skype.com/).
- '*Internet relay chat*': This type of communication is organised using topics, also called 'channels'. A channel exists as long as participants are assigned to it and is terminated after the last user has quit. Sometimes channels are obtained by automated services ('bots'), which administer it and prevent the channel from termination when no real user is available.
- '*Web chat*': Web chats are comparable to internet relay chats and instant messengers in terms of functionality and use. The difference with the two types of chat mentioned above is the fact

that web chats do not require special client software – users can simply chat via their internet browser.

2.3.5 Weblogs

A weblog, or 'blog' for short, is an HMTL page consisting of a list of postings such as diary entries, ordered in reverse chronological order by date; the oldest postings are at the bottom of the page, the newest at the top. Many people use blogs as a public diary or personal news-flash about a distinct topic on the internet. Most blogs are regularly updated by the owner or a small group of owners. Each entry has an author, a timestamp and a unique identifier (a permalink), and it may contain different data types, such as text, images, videos, hyperlinks etcetera, or combinations thereof. Entries can only be written by the blog owner and oftentimes remain rather unedited after creation. Technically it is possible to modify entries later, but this is unusual. Weblogs may either be available to anyone on the internet or the access to weblogs can be restricted to a group of readers. In most cases any reader can attach comments to blog entries (Kolbitsch, 2006). Blogs are not collaborative workspaces in the strictest sense, since the content posted on them and the topics and threads initiated are generally created by the owner only. However, when frequent comments are made by readers of a weblog to the posts placed on it some collaborative aspects do materialize. While weblogs finds themselves in the margins of our categorization of collaborative workspaces we have chosen to include in our discussion of the various types of collaborative workspaces precisely because of this commenting functionality. WordPress is an example of common blog software (http://wordpress.com/).

In recent times the phenomenon of 'microblogging' has emerged as a new branch on the tree of blogging. Microblogging differs from normal blogging in the size of its contributions: microblogs are much smaller snippets of information that a person posts on his blog, both in terms of content and file size. Microblogging often includes functionality that enables users to post to their blog using a mobile phone, for instance via SMS or digital audio. Twitter (www.twitter.com) is one of the best known examples of microblogging.

2.3.6 Groupware systems

Groupware systems are environments that facilitate the synchronisation and exchange of information among members of a group, so that they can communicate, coordinate, and cooperate together (Schlichter *et al.*, 1998). They combine features and functionalities of, for instance, collaborative editors, instant messengers, and bulletin boards. Since groupware systems are targeted to existing groups of people who share a common task, such as colleagues working for (a group within) the same company, these systems hardly support any searching and finding of partners for collaboration. Popular groupware systems are BSCW and OpenGroupware (http://public.bscw.de/ and http://www.opengroupware.org/en/applications/index.html [last accessed on 21 January 2010]).

2.3.7 File sharing systems

A last type of collaborative workspaces are file sharing systems. File sharing systems facilitate the distributing or providing access to files from one user to (one or many) other(s). Files may consist of software, video or audio files, documents or e-books. Not all file sharing systems fit into our

definition of a collaborative workspace, which includes, among other things, a requirement of providing users with means of access control. YouTube (http://www.youtube.com), the famous platform for uploading and watching individual users' movie clips, is an example of a file sharing system that does meet the requirements and can therefore be called a genuine collaborative workspace. YouTube has a member administration and access control features – some videos are only shown to registered members over 18. YouTube also offers some history and event services, for instance statistics on how often a video was viewed, and notifications when a video is deleted. However, there are also quite a few file sharing systems that do not keep a member administration, or have history and event services. Especially users of the 'not so legal'[3] file sharing systems, for instance exchanging movie or music files (e.g. www.bittorent.com/), benefit from the fact that there are no such things. This means that these file sharing systems do not fall into our definition of collaborative workspaces. In conclusion, file sharing, while a core activity of web 2.0, only meets our criteria of a collaborative workspace in some cases, while not in others.

2.4 Social network sites: An overview

In recent years social network sites (or SNSs for short) have become a global and widespread phenomenon. One of the most oft-quoted definitions of social network sites was developed by boyd and Ellison, who write that these are "*web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system. The nature and nomenclature of these connections may vary from site to site*" (boyd and Ellison, 2007: 211).

This definition contains several elements, which we will now discuss in more detail. First, social network sites are defined as 'web-based'. This sets them apart from services supporting social networks that do not essentially require the usage of internet technology. Examples of the latter category would be all types of (loosely or tightly structured or institutionalised) social interaction that have existed before the advent of information and communication technologies, such as social clubs (e.g. sports clubs) or professional associations. Social network sites are web-based, which means they can be accessed via regular internet but more recently also increasingly via the mobile web. An example of the latter variant of social network sites are so-called location-based services (LBSs) for mobile phones, which display, for instance, which other members of the same social network site are currently within a certain physical distance from the mobile phone owner.

Second, social network sites offer users the possibility to create a public or semi-public profile. This means that the visibility of the profile is open to everyone or can be restricted to a smaller audience with certain privacy settings or access control systems. In Chapter 5 of this deliverable we will look at this aspect of social network sites in great detail. The profile itself usually contains a name (or nickname), one or more profile photos, data about gender, age, and hometown, and information about hobbies or interests. In principle, the amount and type of information in the profile can be expanded without limitations. Moreover, many social network site providers offer users the possibility to customise the profile page colour scheme and background thus allowing them to personalize the profile not only through adding content but also by adding its form and appearance.

[3] Note that what is 'not so legal' about these kinds of file sharing systems is not the file sharing per se, but the fact that copyrighted materials, such as music and movie files, over which the rights do not belong to those sharing them, are exchanged.

Third, social network sites enable members to compose a list of other users with whom they have established a connection. Such contacts are generally called 'friends', but that term is misleading, since it hides much of the complexity and richness of social relations as these exist in real life (RL). Social relationships come in a wide variety of forms and have different levels of intimacy (friend, relative, colleague, acquaintance, neighbour, fellow-villager, fellow-member of the same club and so on), and deflating this variety of relationships to the single denominator 'friends' does not do justice to the rich texture of social life. This issue will be discussed in more detail below. Following James Grimmelmann, we prefer to use the terms 'contacts' or 'connections' for the list of 'friends' that a person gathers in a social network site, since "*...it's more neutral about the nature of the relationship than the terms used by many sites*" (Grimmelmann, 2008: 5). After all, as Grimmelmann rightly notes "*…'friends'* [in a social network site] *include not just people we'd call 'friends' offline but also those we'd call 'acquaintances'* […]. *Contact links are a mixture of what sociologists would call 'strong ties' and 'weak ties'*" (Grimmelmann, 2008: 28).

Establishing connections in social network sites can occur either unidirectionally or bidirectionally – in the case of unidirectional connections when user A adds user B to his contact list, B receives a message that this has taken place, but doesn't need not confirm it, and A does not automatically appear in B's list of contacts as well; alternatively, bidirectional confirmation entails that when user A adds user B to his list of contacts, user B has to confirm this act, and in doing so A also becomes part of B's list of contacts. Most social network sites use the latter form, although some offer functionality for unidirectional connections as well. An example of unidirectional establishment of connections in social network sites is the practice of fandom, where users can add themselves to a profile or group page of people with similar interests, for instance fans of a pop star.

The last element of social network services is the possibility to view and traverse the list of connections and those made by others within the system. By showing all connections one has gathered, these sites function as a "*public display of connections*" (Donath and boyd, 2004). The entire network of first-degree personal connections belonging to an individual is often made visible via personal profile pages within the social network site.

2.4.1 A short history and overview of social network sites

Online social networks and other social software have conquered the internet in a relatively short time. One of the first manifestations of social network site were classmates.com (founded in 1995) and sixdegrees.com (founded in 1997). Currently, the most popular social network sites are Facebook (http://www.facebook.com/) and MySpace (http://www.myspace.com/). Facebook recently passed the 400 million user bar[4], and the social networks sites combined easily have more than a billion users, each of whom spends a considerable amount of time maintaining their online presence and interacting with their contacts. A PEW study conducted in late 2006 revealed that 55% of online teens aged 12-17 have created profiles on social network sites, and 64% of teens aged 15-17 (Lenhart, 2007). In 2009 Lenhart conducted another survey on social network site membership, this time looking at a much wider range of age groups. She found that by early 2008 65% of teens aged 12-17 are members of a social network site – an increase of 10% in little over one year. Moreover, in 2009 she found that 46% of American adults (aged over 18) also use social network sites – an increase of almost 40% when compared to the last survey, which was conducted in early 2005 (Lenhart, 2009). Some countries have their own social network sites. Hyves (http://www.hyves.net), the most important social network site in the Netherlands, is one of

[4] See http://www.facebook.com/press/info.php?statistics [last accessed on 25 February 2010].

the better-known examples. Hyves has about 9.5 million users, on a population of 16 million people.

Despite the fact that social network sites are a recent phenomenon there is quite a bit of variation in the intended *goals* of individual social network sites – ranging from dating and meeting friends, to connecting with work relations and finding new jobs (e.g. http://www.linkedin.com/), to providing recommendations for products, services and information (Gross and Acquisti, 2005: 71). Moreover, not all social network environments have the same *make-up*. Gross and Acquisti write: "*The most common model is based on the presentation of the participant's profile and the visualization of her network of relations to others – such is the case of Friendster*[5]*. This model can stretch towards different directions. In matchmaking sites, like Match.com or Nerve and Salon Personals, the profile is critical and the network of relations is absent. In diary/online journal sites like LiveJournal, profiles become secondary, networks may or may not be visible, while participants' online journal entries take a central role. Online social networking thus can morph into online classified in one direction and blogging in another*" (Gross and Acquisti, 2005: 72).

One interesting question is whether one could label online worlds such as Second Life[6] – also known as 'online multi-user virtual environments' (MUVEs) – as social network sites as well. After all, social interaction and the maintenance of interpersonal networks are key characteristics of such environments, besides the creation of objects and engaging in economic interaction (Smart *et al.*, 2007). Moreover, in online worlds users construct a virtual persona – also called an *avatar* or *character* – that engages in social interaction with the avatars of other users, and these avatars have their own profile page and contact lists through which users can communicate with their peers. One could argue that the characters that roam online worlds form an extra layer between individuals engaging in interaction with one another – a layer that allows for enriched communication through the bodily guise these avatars take. Because the elements of a profile page, a contact list, social interaction and a web-based environment are all present in online worlds the interactions users engage in while in these worlds are not unlike those occurring in social network sites, and online worlds thus meet the central criteria for qualifying as social network sites, although they are social network sites of a special kind.

2.4.2 The social dynamics of social network sites

Why do people turn to social network sites to connect with others and present themselves to the world? For an answer to this question we need to look at the social dynamics underlying these social network sites. As danah boyd, one of the most prominent researchers of this recent phenomenon, states people (and especially teens) massively flock to these new interaction environments "*because, that's where* [their] *friends are*" (boyd, 2008c). Large-scale online presence of other people (teenagers) is a network effect. The value of the network lies in its size and hence networks become more attractive as they grow. Conversely, when people flee the network in large numbers the decline will progress in a non-linear fashion.

However, the popularity and massive increase of use of social network sites is not merely the result of a network effect. The three primary characteristics of social network sites: *identity*, *relationship*, and *community* are really at the root of their rapid advance (boyd, 2008c;

[5] The internet addresses for the social network sites mentioned in this citation are: http://www.friendster.com/, http://uk.match.com/, http://www.nerve.com/ , http://personals.salon.com/, and http://www.livejournal.com/ [all sites last accessed on 29 October 2009].

[6] Note that, technically speaking, Second Life is not web-based, which is one of the elements of our definition of a social network site. To use Second Life users have to download software to their computers, which they then use to connect to other users via the internet.

Grimmelmann, 2009). Especially teenagers are in a phase in their lives where they are particularly busy with constructing their identities. In the next section of this deliverable we will delve deeper into the reasons why social network sites provide a good platform for them for experimenting with and expressing their identities. For now, we will focus on the other two characteristics of social network sites: relationship and community.

Building, maintaining, expanding, managing and regaining relationships is one of the key features of social network sites, as we have also argued earlier in this chapter (section 2.2.2). This feature is one of its most important attractions, not only for young people but for all users. Social network sites allow their users to connect with others on a one-to-one basis. As we have seen this is done by inviting them to become part of their list of contacts. Although the act of adding someone as a contact is a multivalent act (Grimmelmann, 2009) – it can mean anything from 'I am your friend' to 'I don't even know you (but still want to be associated to you)' – it signals a link between two individuals and shows that people care about each other (Leenes, 2010). Therefore even simple communication between users, such as writing on someone's wall, gives users the idea that they are appreciated. Profiles are also used to connect with potential soul-mates (Leenes, 2010). This is especially relevant for those who are not the centre of attention in the offline world. danah boyd quotes a typical example of this: "*I'm in the 7th grade. I'm 13. I'm not a cheerleader. I'm not the president of the student body. Or captain of the debate team. I'm not the prettiest girl in my class. I'm not the most popular girl in my class. I'm just a kid. I'm a little shy. And it's really hard in this school to impress people enough to be your friend if you're not any of those things. But I go on these really great vacations with my parents between Christmas and New Year's every year. And I take pictures of places we go. And I write about those places. And I post this on my [social network site profile]. Because I think if kids in school read what I have to say and how I say it, they'll want to be my friend*" (Vivien, 13, to Parry Aftab during a 'Teen Angels' meeting, cited in boyd, 2008c). Social network sites thus provide shy teenagers a platform to advertise themselves in a relatively safe way. They have control over their own page and can shield (and remove) themselves from insults more easily than in the real world.

The third characteristic that helps attract users to social network sites is *community*. In our post-modern societies and in a globalised world of high technology senses of community revolve around doing things together and sharing thoughts and ideas with a group in online worlds. As Gerard Delanty writes: "*Today global forms of communication are offering many opportunities for the construction of community. This leads to an understanding of community that is neither a form of social integration nor one of meaning but is an open-ended system of communication about belonging. Belonging today is participation in communication more than anything else…*" (Delanty, 2003: 187-188). Online worlds, with their wealth of possibilities for interaction and communication turn out to be an important source for the creation of new forms of belonging, and hence new forms of community: "*It is in these new and essentially communicative spaces, where a kind of proximity is to be found, that community is created*" (Delanty, 2003: 193-194).

Social network sites are a key example of these communicative, community-building spaces. But it is not just communication and interaction that are important in social network sites in relation to community – so are social position and social capital (Leenes, 2010). In social network sites the size of one's network and its composition are clearly visible to outsiders in social network sites. This provides a marker of how well-connected one is, and perhaps of how popular one is. Several researchers have argued that the visibility of users' list of contacts to others, both in terms of the amount of connections and the names of people on their list, entails that various forms of social pressure emerge with respect to creating a friends list. For one, users "*may choose to accept requests from peers they know but do not feel close to if only to avoid offending them. They may also choose to exclude people they know well but do not wish to connect with on* [a social network site]" (boyd, 2008b: 213). Moreover, peer pressure may lead users to hesitate when declining a friend request. boyd discovered that "*most users tend to list anyone who they know and do not actively dislike. This often means that people are indicated as Friends even though the user does*

not particularly know or trust the person" (boyd, cited in Gross and Acquisti, 2005: 73). At the same time, the importance of a sizeable community is not absolute. On Friendster the urge of some users to collect as many friends as possible inspired the notion of a 'Friendster whore' (Donath and boyd, 2004), which obviously carries a connotation of undesirable social behaviour. Moreover, and in response to these changing trends in social pressure, recently the idea of carefully pruning one's network has gained prominence, has given rise to new vocabulary with a term such as 'defriending', which means to eliminate any formerly accepted contacts that are not deemed valuable as social capital. Some sites, such as MySpace and Facebook, now allow their users to list their top 8 or 10 friends. This represents clear indicators of the social position of people within one's network and inspires wall postings such as "*Hey ZOE!!! WHAT THE HELL!!! Why aren't I on your top friends?*" (a post by 'The Trickster' on someone's wall in Facebook dated 13 December 2007 (6:45 AM), cited in Leenes, 2010).

The wall also plays a role in delineating social positions. On the surface, wall postings are awkward ways of communicating between individuals because they show only one side of a two-way communication channel. The reader only gets to see the communication posted by the poster, not the responses by the profile owner, unless he or she has access to the profile page of the poster too. However, on closer inspection, the wall has several social functions that extend beyond the two primary actors in the communication. First, a wall post communicates certain content to the profile owner (and others who have access to the page), but it also shows others the author's affection for the profile owner and therefore provides a public display of this affection. Wall posting consequently are signals of one's social position within a network. Second, writing on someone's wall has strong reverberations with graffiti culture, where members of specific groups will leave messages in public places that are largely unintelligible for the public at large, but not for those who are also members of the same subculture. Leaving messages for individuals in public toilets or spray-painting 'tags' on walls in public places has thus been a public-yet-private-messaging practice for decades. In social network sites, too, the messages that users leave on one another's walls often have this cryptic, unintelligible character for those not part of the same clique reading them.

2.5 Identity and web 2.0

Throughout the twentieth century the notion of identity gained prominence as a subject of research in various disciplines, but also as a subject of discussion in the popular press and in national and international politics. Sociologist Zygmunt Bauman is one of the most prominent social scientists who has attempted to find an explanation for this increased prominence (Bauman, 2001; Bauman and Vecchi, 2004). He argues that the reason why identity is a hotly debated topic in our modern world is because with the advent of modernity, identity as a concept has changed in fundamental ways. The rise of modernity has changed our conception of the world and ourselves from a 'given' into a 'project'. While in premodern times we conceived of the natural and the social world as predestined 'Divine creation', for us to accept as is, the advent of modernity led to a whole new perspective on the world: a world to be shaped and moulded into whatever form we human beings figured would most suit our (rationally construed) ends and needs. So, too, with identity, says Bauman. In premodern times identity was viewed as a 'given', but like everything else modernity turned identity into a 'life project' (Bauman, 2001: 142). And the key concept in this development, according to Bauman, was the notion of individualization: "'*individualization' consists in transforming human 'identity' from a 'given' into a 'task' – and charging the actors with the responsibility for performing that task and for the consequences (also the side-effects) of their performance; in other words, it consists in establishing a 'de jure' autonomy (though not necessarily a* de facto *one).* […] *Needing to* become *what one* is *is the feature of modern living*" (Bauman, 2001: 144-145, emphasis in the original). With the fact that identity has become a life-

long project, a problem to be addressed by each and every individual, and one filled with difficulties and anxieties at that, it is not surprising that scientists, writers, journalists, politicians and the public at large have turned their attention to this difficult concept. Identity has indeed become one of the most important 'issues' of our times – not only as a result of the immense displacement and redistribution of people, goods, and wealth that have emerged in the recent decades of globalization, but also in light of technological developments, and social, economic and religious processes of realignment, redefinition, and reshaping that have affected nation states, institutions, cultures, social groups and individuals the world over. All of these consequently feel a need to (re)consider their identities, to redefine their senses of self and to persistently, no constantly, answer this vital question: 'who am I?' Answering that question is not an easy task – for individuals in their own lives, and for researchers alike. The notion of identity is highly complex and multi-faceted. This is why we will clarify what we mean when we use this term in the following section.

2.5.1 What is identity?

In this deliverable we take an *interactionist* perspective to identity. Interactionism emerged as a distinctive branch of identity theory in the early twentieth century and it eventually became one of the most popular sociological perspectives of the twentieth century – some even go so far as to claim that over time all of sociology has become "*interactionist in its conceptual makeup*" (Maines, 2003: 5). According to interactionism identities are constructed and expressed in and through *interactions* between people. Whenever people engage in interactions with others they go through the following cycle: they formulate an interpretation of the 'definition of the situation' – i.e. they attempt to answer the question 'what is going on here?' (Goffman, 1986: 8; Meyrowitz, 1985: 24; 1990: 67; 2005: 24), what behavioural repertoire is expected or called for here, both for themselves and others? Based on that definition they choose a certain 'role' to play. Assuming that role they then engage in 'performances' or 'presentations', with the aim of convincing the observers "*to take seriously the impression that is fostered before them. They are asked to believe that the character they see actually possesses the attributes he appears to possess*" (Goffman, 1959: 17).

When roles are frequently portrayed and consistently valued by both the audience and the performer himself a person may come to identify with that role to such an extent that it becomes part of his self-image. In the words of Robert Ezra Park: "*In the end, our conception of our role becomes second nature and an integral part of our personality. We come into the world as individuals, achieve character, and become persons*." (Robert Ezra Park, cited in Goffman, 1959: 19-20) Identities, then, are not essences – ready-made, up for grabs – that we display in front of others. Rather, they are *constructs*, and more precisely, they are the social *result* of interactions with other people. Identities are constructed in social interactions, and hence are dynamic and open-ended. They may change over time, and a person may have conflicting sides to his or her identity – through identification with and internalization of conflicting roles in different situations one may display selves that are incoherent and complex, yet nevertheless exist alongside each other in one and the same person. Identities, thus, are multidimensional, multifaceted, variable, and changeable. At the same time, though, there are social constraints both on the performance of roles and the construction of selves. Thinking of identities as constructs may seem to imply that we are entirely free to create our selves at will – that by choosing whatever role we want, we may actually become whatever we want. This, however, is not the case. As said, we choose our performances on the basis of our interpretation of the 'definition of the situation', a definition that is thoroughly imbued with ideas on social rules, the appropriateness of behaviour, and the limits within which one's performance 'ought' to stay if one wants it to be labelled as befitting the situation and the expectations that apply there. Identities, then, are the result of interactions with

other people, which at the same time form their constructive source and their constraint. They are not solid properties, but rather an evolving network of various relational roles. Moreover, identities are not a given, but "*a dynamic,* emergent *aspect of collective action*." (Schlesinger, cited in Morley and Robins, 1995: 46, emphasis in the original).

As we argued above, processes of globalisation, individualisation, secularisation and increased mobility have all contributed greatly to the increased prominence of a search for individual and group identity. The rapid and widespread technological changes of the twentieth century, and especially the emergence of information and communication technologies have also played a vital role in the centrality of identity as a topic for investigation – both for researchers (cf. Castells, 2004; Gergen, 1991; Turkle, 1984, 2007) and for individuals using these technologies. In the next sections we will look at the ways in which the emergence and maturation of the internet have both aided individuals in their quests for identity, and at the same time also helped shape the form and content of these quests.

2.5.2 Identity in online worlds

Soon after the massive spread of the internet in the 1990s users discovered its potential for self-expression and self-presentation through a variety of different (plat)forms. The recent emergence of web 2.0 has only increased opportunities for identity expression and management. Over the past decades millions of users have turned to the internet to create virtual (re)presentations of their identities. These range from personal homepages, blogs and professional profiles, to avatars in online worlds such as Second Life and online gaming communities such as Multi-User Domains (MUDs) or Massively Multiplayer Online Role-Playing Games (MMORPGs). The massive use of the internet for identity expression and experimentation shows that, apparently, individuals find that there are definite gains in online self-expression and interaction. What these gains consist of, of course, varies from person to person, from group to group, and from internet application to application – creating a personal homepage obviously has different gains and provides an individual with different opportunities than participating in an online world such as Second Life. However, what counts first and foremost is the fact *that* individuals turn to the internet to engage in social interactions with others and to express ideas about themselves or experiment with identities in various online environments and formats.

We have discussed a wide variety of online environments that are open to users for presenting (aspects of) themselves – both social network sites and, to a lesser degree, collaborative workspaces are key examples of web 2.0 in which self-presentation is at stake. The different types of environments currently available for online identity construction and management can best be understood as a *continuum* running from domains in which 'entirely fictional' identities are presented at one extreme, to those in which 'entirely real' identities are presented at the other[7]. As an example of the former one might think of avatars or digital (re)presentations that show no (bodily or other) similarity with an individual's real life persona, created in an online world such as Second Life. Personal or professional webpages are an example of the latter. Let's look at these two extremes, and some of the intermediary environments on the continuum between them in some more detail.

[7] The phrases 'entirely real' and 'entirely fictional' are put between inverted commas to express the fact that such a distinction should not be taken too literally or factually. In fact, all 'fictional' identities are 'real' in a sense, while all 'real' identities are 'fictional' in character, too. This distinction, then, is intended more as a conceptual one than as one referring to actual practices and/or realities.

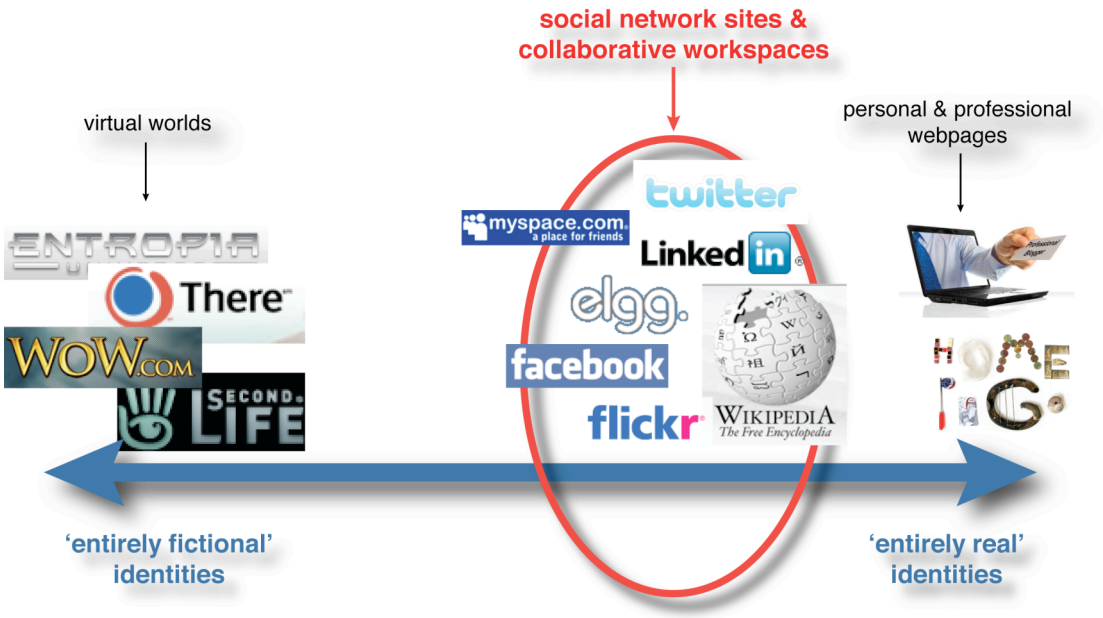


Figure 2: The continuum from 'entirely fictional' to 'entirely real' identities.

2.5.3 Experimenting with 'fictional' identities

At the dawn of the age of personal computing and the internet many researchers suggested that virtual worlds opened up a whole new horizon for the construction and expression of identities. Sherry Turkle is one of the most well-known advocates of this position (cf. Turkle, 1984, 1995, 1996). Turkle investigated identity construction and expression in Multi-User Domains (MUDs) (Turkle, 1995), and argued that virtual worlds such as these allow users to engage in self-exploration and self-experimentation in a way that was unheard of in everyday life for several reasons, all of which relate to the medium-specific characteristics of virtual reality. First of all, when (inter)acting in virtual worlds individuals leave their bodily selves behind in the world of everyday life, which means that they can experiment with the construction of different identities in ways that fall outside the range of possibilities open to them in the physical, embodied ordinary world. In the words of Deborah Chambers: "[interacting in online worlds] *allows people from any location to experiment with communication and self-representation. Internet communication is unlike direct experience as the medium itself enables a masking and distancing of users' identity*" (Chambers, 2006: 134-135). For instance, users can experiment with taking on a different gender or age to experience what it would be like to be a different person. Users are free to devise entirely new identities for themselves, and only the limits of their imagination form the boundaries of where they may go in terms of self-creation and experimentation[8]. This means, for instance, that

[8] This is a bit of an overstatement. While virtual worlds provide an *apparent* total freedom of experimentation with identity construction and expression, in fact no such thing exists. Even in 'free zones' for identity experimentation such as Second Life the degree of freedom for such experimentation is limited. For one thing, as David Velleman has argued, the users in such worlds "*cannot make stipulative additions or alterations to the fictional truths of the game. Their play is governed by a single, master fiction* […]. *This fictional truth is given to the players, not invented by them*" (Velleman, 2007: 5). As Velleman points out, this clearly distinguishes virtual worlds and the actions and roles users can play in them from a real life identity experimentations, for instance in pretend play. In pretend play the players can change the rules of the game themselves at any moment during game-play. No such

identities created and maintained in online worlds such as Second Life need not necessarily take the human form, and it appears that people do, in fact, devise alternative bodily guises for themselves, as the large community of so-called 'furries'[9] in Second Life shows.

Moreover, since online worlds, Multi-User Domains and Massively Multiplayer Online Role-Playing Games allow individuals to engage in interaction and communication with millions of other computer users worldwide they may be exposed to ideas, feelings, and self-conceptions that they would not (easily) have been able to encounter in their physical, everyday lives. This means that their horizons are widened and that they may be invited to discover new ideas about their own identities, based on the wide variety of identities present in such worlds, created by others. According to Turkle, these two factors – disembodiment and massive interaction and communication – make virtual worlds into an important vehicle for (re)evaluating and changing self-conceptions and self-expressions.

Arguably, one could experiment with identities in real life (RL) as well. We see this, for example, in the phenomenon of 'pretend play' that children (and some adults[10]) engage in. In pretend play players create a storyline, rules to play by and each takes on an alternative identity. They then engage in role-playing and experimenting with those identities, which are not, or not fully coincide with, their own. For instance, they play at being cops and robbers, or pirates, or grown-ups. What is the difference between playing or experimenting with identities in everyday life, i.e. engaging in pretend play, versus doing so in virtual worlds? The difference between the two revolves around what David Velleman has labelled the *opacity* of virtual identities versus the *transparency* of identity experimentation in pretend play. He writes: "*In pretend-play, the make-believe characters are impersonated by actual children who know one another and see one another playing their roles. What a child chooses to do as a make-believe pirate is therefore attributed both to the pirate, as his action within the fiction, and to the child, as his contribution to the game. The role of the pirate is consequently* transparent*: it allows the player to show through.* […] *In virtual worlds, the actual players are usually unknown to one another: they interact only through their avatars. Even if the owners of different avatars know one another's identities, those identities are not on display in the virtual world: the players don't see one another's faces as they would in pretend play. Hence their avatar-identities are* opaque*. There is no way for players to emerge from behind their avatars to speak or act as their actual selves*" (Velleman, 2007: 8-9, emphasis in the original). Obviously, the opaque character of avatars in online worlds is precisely the reason why users are able to experiment with alternative identities in the first place – if these avatars were transparent the believability of being a furry in Second Life, for example, would be undermined to a serious degree.

In conclusion, we can say that virtual worlds enable users to experiment with alternative identities, separated (to a smaller or larger degree) from their actual identities in real life. One could even argue (although this is debatable) that for MUDs, MMORPGs and online worlds such as Second Life the possibility of creating alternative identities is the whole purpose of such environments, that their sole *raison d'être* is to allow people to 'escape the bonds' of everyday life and be what they are not (and/or cannot be) in the real world.

---

liberty is available for users in virtual worlds, and this has obvious consequences for who they can 'choose to be' in such worlds.

[9] See http://en.wikipedia.org/wiki/Furry [last accessed on 11 June 2009].

[10] One form of pretend play that some adults now engage in is called 'live action role-playing' (or LARP) – a real world parallel to online role-playing games such as MMORPGs. LARPs involve the physical impersonation of (virtual) characters. The participants play out a certain role in a real world setting, thereby remaining in character. See http://en.wikipedia.org/wiki/LARP [last accessed on 11 August 2009].

2.5.4 Expressing 'real' identities

Of course, some forms of internet communication and interaction are more inviting to identity experimentation than others. Online environments such as discussion groups, personal or professional webpages and personal profiles are much less often used to create and present such alternative identities. As Daniel Chandler writes when discussing the phenomenon of personal webpages: "*Personal home pages often include such ties to* [real life, RL] *as: photographs of the authors which are at least identifiable by those who know them in RL; e-mail addresses which often reveal institutional affiliations; links to other people who know the authors in RL; RL home and/or institutional addresses, and so on. The social ties typically embedded in personal home pages [...] would tend to make assumed identities hard to sustain. Personal home pages are thus not the favoured medium of those who wish to adopt identities which would be completely unrecognizable to those who know them in RL*" (Chandler, 1998).

At the other end of the continuum, then, we find online environments in which users display information that makes them *recognizable* as the persons they are in everyday life. These online environments include personal and professional webpages, but also expert panels in collaborative workspaces. The reason why users are keen on presenting information that makes them recognizable as unique individuals in such environments is simple: most of the time such environments are used to communicate with people who already know the individual in real life, or alternatively, may get to know his real life person through an online encounter. The goal of such environments, then, is to present a *believable*, *actual* self rather than an alternative, imagined self, as is the case in virtual worlds. In environments such as these, then, information regarding the 'real' identity of individual persons or collections is presented, rather than 'fictional' identities.

In between the two extremes of the continuum sketched above we find many current-day online environments, in which 'entirely fictional' and 'entirely real' identities may potentially be, or actually are, combined. The focal web 2.0 environments of this deliverable, collaborative workspaces and social network sites are examples in case. In social network sites identities are communicated through a person's profile page, and in some collaborative workspaces the identities of members are displayed to strengthen the believability of their (expert) contributions.

As we have seen, users currently turn to different social network sites to for different goals – for instance, they present professional information about themselves in LinkedIn and more private information on Facebook or Friendster. The same goes for collaborative workspaces: users log onto different platforms and environments to participate in various content creation and dissemination tasks. However, since this involves managing and updating several profiles and documents in disparate contexts, future generations of social network sites and collaborative workspaces might start integrating more and more of these data into a single environment, thus providing users with an opportunity to keep different profiles within one and the same network. If this were to be realized, then these networks might eventually evolve into becoming a *central environment into which all of a person's disparate identities* (i.e. both 'entirely real' and ' entirely fictional' ones) *are brought together*, thus turning them into real identity management systems (in many senses of the term 'real'). This means that individuals would have to 'juggle various faces' in that environment.

2.5.5 Identity in social network sites

As we have argued in section 2.2.2 social network sites have two main functions: the management of relationships, and the management of the self, i.e. self-presentation and construction. Identity, therefore, is one of the key elements of social network sites. In these online platforms users literally "*write themselves into being*" in the words of Jenny Sundén (2003). Users adjust their

identities and profiles on the basis of the responses of their peers. This process of performance, interpretation, and adjustment is what Goffman calls 'impression management' (Goffman, 1959). Impression management is an ongoing process throughout individuals' lives, both in real life and in online communities. Thus, in social network sites it is not only an important aspect of identity construction and expression for teens, who are in the earlier stages of identity development, but for all of us.

Social network sites contain different mechanisms to provoke active identity construction, some of which we have briefly mentioned above. For one, many sites enable users to customise significant aspects of the 'feel' of their profile page, by allowing them to change the backgrounds of their profile, and modify the CSS style sheets employed on their pages. Simply browsing through the public profiles on any social network site will reveal a multitude of different styles, backgrounds etcetera – many may look utterly horrible, but so do many teenager bedrooms. In any case, these customised backgrounds are individual expressions and are hardly ever accidental (Leenes, 2010). But there are other ways in which social network site providers promote identity-related activity on the profile pages as well. Most social network sites allow other users to post comments on a profile page – as we have seen above this functionality is called the 'wall' (Facebook), 'testimonials and comments' (Friendster) or 'scribblings' (Hyves). At time, these postings create communication between the profile owner and visitors because the owner will respond to the comments, for instance by updating or changing the page. Facebook holds several patents, some of which are related to inducing users to actively nurture their pages and interact with other users.

An interesting phenomenon to keep in mind with respect to identity construction and expression in social network sites is that sometimes not everything is what it seems. As we have seen above (for certain purposes) the internet can be used as an ideal place for people to experiment with (aspects of) their identities and to explore the boundaries of their personality (cf. Turkle, 1995, 1996). This holds true for social network sites as well. Most of the time online profiles in social network sites are fairly close to the offline identities of their creators, or phrased differently, identity experiments are a limited phenomenon in this domain. There is, however, one particular group of users in social network sites that takes experimenting with their identities to the extreme in social network sites. They are called 'Fakesters'. As danah boyd writes: "*From the earliest days, participants took advantage of the flexibility of the system to craft 'Fakesters,' or nonbiographical profiles. Fakesters were created for famous people, fictional characters, objects, places and locations, identity markers, concepts, animals, and communities. Angelina Jolie was there, as were Homer Simpson, Giant Squid, New Jersey, FemSex, Pure Evil, Rex, and Space Cowboys*" (boyd, 2008a). An interesting issue with respect to Fakesters is that others judge the information presented on their profile pages irrespective of whether it is accurate. Therefore fake profiles may also have real consequences for their creators.

2.5.6 Identity in collaborative workspaces

The web 2.0 triangle that we discussed at the beginning of this chapter places collaborative workspaces such as wikis and forums at the top of the triangle, since their main function is content management. The management of relationships and that of identities is of lesser importance in these environments. However, this does not mean that identities and relationships are not relevant at all in collaborative workspaces. In fact, depending on the kind of platform identities matter more or less. When labelling collaborative workspaces in terms of the importance of identity and self-presentation we find that there is a continuum of different domains, ranging from platforms in which identity is not important to platforms in which it is very important. Starting off with the latter, two examples in case are weblogs, and (some) file sharing systems, such as the movie clip environment YouTube.

As we discussed in section 2.3.5 weblogs are often collections of diary entries from a single individual, either of a highly personal nature, or revolving around a central theme or specific interest, such as a hobby, a favourite brand or type of product, or a particular kind of news items. Weblogs can be labelled as collaborative workspaces when readers comment on postings and discussions with the blog owner ensue. Identity expression is a relevant parameter in this type of collaborative workspaces on two levels. First, blogs contain information about the person behind them. Some authors devote just a few words to their identities, while others compose a more detailed profile expressing personal details of the weblog's author. In most cases authors use an identity that can be traced back to a person in the real world. Second, weblogs reflect the ideas, opinions, knowledge and preferences of the person filling them, and when others comment on posts they also reflect the ideas and opinions of the commentators. Both of these types of postings are expressions of the identities of their writers. Moreover, the choice of topics discussed, the style in which blog postings are presented and the background, pictures and layout of the blog pages are also a reflection of the identity of those creating and maintaining them.

A second example of collaborative workspaces in which the identities of those sharing or creating content may be relevant and visible revolves around certain types of file sharing sites, viz. sites in which users share self-made creative materials, such as movie clips, music, or poetry and short stories. YouTube is an example in case. While many YouTube users post movie clips from TV shows they liked, many also use this platform to post movies either made by themselves, or in which they play a main role. Especially this latter kind of movies literally revolves around self-presentation. Booksie (http://www.booksie.com/) and The Next Big Writer (http://www.thenextbigwriter.com/) are examples of a web 2.0 platform in which anyone can post their writings (novels, poems, short stories, articles) for others to read. Readers can leave comments, and there is a ranking system for the contributions that get read the most. As with blogs booksie's writers and readers express their identities through the ideas, topics and opinions in their work, but also, in many cases, by attaching their personal information to their writings in the form of a profile.

At the other end of the continuum we find collaborative workspaces in which the identities of contributors are not important. Contributors to a wiki or users posting messages to a forum are usually not out to present information about themselves predominantly, but rather to work with others on the creation of content on which they have some knowledge. In many collaborative workspaces of this kind users do need a username and password to log on and be allowed to contribute, and since a username is a marker of identity this would entail that identity is also a relevant parameter in this kind of collaborative workspaces. However, in practice it turns out that most users opt to use a screen name rather than their own name when participating in wikis and forums, and in some cases collaborative workspaces enable users to contribute anonymously after they have logged onto the system with a username and password (i.e. the username or screen name is not shown with postings). We will see much more of this latter kind of mechanism in the Chapter 4 on privacy in collaborative workspaces.

In this chapter we have provided a broad overview of the topic under discussion in this deliverable: sociality and identity in web 2.0 domains, with a focus on collaborative workspaces and social network sites. We have begun this chapter with a description of the four most important features of the second generation of the internet, also known as 'web 2.0'. These four characteristics are: (1) the increased importance of end users as participant or even prosumers on the web; (2) the increased importance of social interaction and sociality on the web; (3) the increased importance of user contributions for the creation, management and distribution of content; and (4) the changing nature of the web as a platform, and of software as a service. After this introduction to web 2.0 we have introduced the two focal pillars of this deliverable: collaborative workspaces and social network sites. Both are examples of social software and can

be placed within the web 2.0 triangle, a model that reveals that the second generation of the internet revolves around three angles: (a) content management; (b) the management of relationships; and (c) the management of the self (identities). We have explained what collaborative workspaces consist of, and have discussed key examples of these kinds of platforms, such as wikis, collaborative real-time editors, forums and weblogs. After that we have discussed the key characteristics and definitions of social network sites, and we have described the social dynamics underlying these environments. Then we turned to a discussion of the notion of identity and its relevance on the internet in general, and in social network sites and (some) collaborative workspaces in particular. This has brought us to the end of this chapter. We will now turn to the main topic at stake in this deliverable: that of privacy, and the ways in which it is affected by and becomes an issue in collaborative workspaces and social network sites. Before turning to an analysis of privacy issues in these two focal web 2.0 domains, however, we need to clarify what we mean by 'privacy' and which aspects of privacy are really at stake in online worlds such as these. This is the topic of the next chapter.

Chapter 3

Privacy: A complicated yet valuable concept

'Privacy' is perhaps one of the most complicated and hotly debated concepts in social science, legal science and philosophy in the last decades. Many different definitions have been put forth with respect to this notion, depending on the context of its use and the goals of their proponents. Especially in recent times, with the massive spread of information and communication technologies, debates surrounding the meaning and value of privacy have sprung up everywhere. Some have argued that its relevance and value has been undermined by modern technologies, some have gone so far as to claim that it no longer exists. Other fiercely protect 'the right to privacy' and claim that it is one of the cornerstones of our democratic societies. But what is privacy? Why is it important (or not)? And how is it affected by the rise and spread of modern technologies? These are the question that we will attempt to answer in this chapter. As said, debates on privacy are in abundance today, as are scholarly books and articles about the subject. In this chapter we cannot possibly do justice to all the many sound arguments and ideas presented in them. We have restricted ourselves, for lack of space, to collecting and presenting some of the most well-known theories and ideas from scholars working on privacy and information technology.

3.1 What do we mean by 'privacy'?

What do we mean by 'privacy'? While almost all of us have an intuitive 'feel' with regards to what this notion entails, when setting oneself to circumscribing it in detail, let alone formulating a clear definition of it, it turns out that privacy is a hard-to-grasp concept indeed. Therefore, the question of the meaning of privacy is not easy to answer. As Anton Vedder notes one of the reasons why it is difficult to articulate what we mean by privacy is because discussions on this subject revolve around three different aspects: (1) "factual *conditions in reality (for instance conditions with respect to seclusion or not being followed, spied on or observed)*"; (2) "desirable *conditions (desired conditions with respect to seclusion or not being spied upon, not being followed or observed*"; and (3) "*the* reasons *for the desirability of these conditions (for instance the desire to prevent that people's vulnerabilities may lead to actual harm, the desire to respect*

the individuality and autonomy of individuals, etc.)" (Vedder, 2009: 7, emphasis added). This distinction, between different levels of discussion with respect to privacy, is often overlooked. The result is that in debates on the subject these levels become blurred. Thus, examples of the status quo involving privacy-issues in relation to, for instance, institutions or information, get entangled with proposals for improvement based on a specific normative stance (which is often left un(der)addressed itself), and interwoven with more or less explicit references to the value of privacy as such, i.e. whether privacy needs protection in the first place. Facts, ideals and values are not delineated as separate items for discussion, which entails that articles or books on the subject highlight a wide (and wild) variety of topics and issues, while all are attempting to shed light on the same concept. In the following we will attempt to give an overview of some of the key aspects relating to the concept of privacy without mixing these different levels.

3.1.1 Three examples of defining privacy

One of the most famous and commonly used definitions of privacy is also its oldest known one: "*the right to be let alone*" (Warren and Brandeis, 1890). In an article by the same title Warren and Brandeis were the first to raise privacy as a theme of concern. Interestingly, Warren and Brandeis claimed that privacy had become an issue in light of various developments in the realm of technology – and this has remained one of the key reasons for discussing privacy until this day. In section 3.3 we will examine in more detail why this is the case. Warren and Brandeis were quick to pick up some of the key problems that might arise with respect to the introduction of new technologies, although the kind of technologies that were threatening privacy in their days (the late 1800s), were very different from our own. For one, Warren and Brandeis were worried about the advent of photography, of newspaper reporting and of recording techniques. They write: "*Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops*' (Warren and Brandeis, 1890) While our current privacy concerns do not (predominantly) revolve around those same technologies anymore these two authors had a remarkably early sense of the changing nature of privacy and publicness that has proven to be at stake all throughout the twentieth century.

A second, well-known definition of privacy is that of Burgoon *et al.*, who tackled the issue of defining privacy by investigating its various dimensions. They write that privacy is "*the ability to control and limit* physical*,* interactional*,* psychological *and* informational *access to the self or one's group*" (Burgoon et al., cited in Paine *et al.*, 2007: 526, emphasis in the original). This definition of privacy is more precise than that of Warren and Brandeis, and it also sheds some light on the various realms in which privacy issues may occur. They may arise, first, in or over physical-spatial matters. An example of such an issue would be when someone peeks into the windows of your home. Second, privacy issues may occur in interactions between people, as a result of the fact that we engage with different people in different degrees of intimacy. For example, privacy issues may arise when information about a person's private life, which is intended only for others in her most intimate sphere, leaves that sphere and reaches others with whom she has a much less intimate relationship. Third, privacy has a psychological (or decisional) dimension. This means that individuals need to have room for making personal choices with respect to their own lives, without intervention of or pressure from others, for instance with respect to their religion, sexual orientation and political opinions. Last, privacy issues may occur when information about a person is shared with one or more third parties against her will or without her knowledge. Examples of this kind of privacy issues will be addressed in detail below.

A third definition of privacy that is worth noting, especially in relation to our own investigations into identity and privacy in this deliverable, is that of Agre and Rotenberg, who state that privacy

is "*the freedom from unreasonable constraints on the construction of one's own identity*" (Agre and Rotenberg, 1997: 7). As Hildebrandt notes "*this* […] *definition has the advantage of understanding privacy as a relational and dynamic concept that does not take one's identity for granted as a given that must be protected from outside influence*" (Hildebrandt, 2009: 448). This interpretation of privacy fits in well with our conception of identity, as we have sketched it in the previous chapter. Moreover, it shows that there is a close connection between privacy and identity: individuals deem information 'private' because they reveal something *about who they are*. Privacy issues arise, and are experienced by human beings as violations of their person, autonomy or integrity, because they revolve around humans' identities. Also, this definition by Agre and Rotenberg turns privacy and its experience into something that is dynamic and open-ended: what we deem private may change over the course of our lifetime, just like our identities change throughout our lifetime – one could even argue that privacy perceptions and identities develop in a mutual relationship.

3.1.2 Categorizing the various definitions of privacy

These three different definitions of privacy show that there are a number of interpretations of what privacy means. In his influential book *Understanding privacy* Daniel Solove, one of the leading researchers in the field of privacy, categorises the most common interpretations of privacy that have developed in the century after Warren and Brandeis put the topic on the agenda. Roughly, he says, privacy has been understood to mean the following things (Solove, 2008: 18-37):

- "*limited access to the self*", which can mean either that the individual has control over who has access to his person or to information about his person, or, alternatively, a particular "*state of existence*", in which the individual's experiences are not freely accessible to others. Privacy in this meaning revolves around the notion of access control, which we will also encounter more extensively in chapters to come;
- "*secrecy*", or the idea that individuals should be able to keep certain information, especially information that may be deemed discreditable, to themselves. Privacy here means being able to withhold certain information from others;
- "*control over personal information*", which is, in fact, a more precise formulation of the first understanding of privacy, that of limited access to the self. It entails that individuals know and have control over who has access to which items of information that they deem personal. Privacy in this case pertains to a person's *information* only, and is not so much about, for instance, restricting access to certain physical spaces that one may deem private, nor to one's person per se. This interpretation of privacy became more prevalent since the 1960s. Alan Westin's definition of privacy, which another oft-quoted one, fits into this category. According to Westin privacy is "*the claim of individuals, groups, or institutions to determine for themselves, when, how and to what extent information about them is communicated to others*" (Westin, 1967: 7)[11]. The focus on controlling and protecting personal information has become especially relevant in light of the introduction and spread of information and communication technologies, as we will see in more detail below. It has lead, among others, to legal guidelines on the protection of personal data in numerous countries worldwide, for instance the European Data Protection Directive 95/46/EC[12].
  Note also that this conception of privacy may also relates to individuals' concerns over the

[11] For an interesting critique of this perception of privacy, see (Austin, 2010).
[12] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L281, pp. 31-50 (23 November 1995).

potential abuse of, or errors made with respect to, their personal data when these are held by others;[13]

- "*protecting personhood*", which is a more normative approach to privacy that claims that privacy violations are violations to a person's selfhood, autonomy, and/or integrity. In this interpretation privacy is a value that is part of a normative order, in which personhood has fundamental worth, and therefore its concordant rights and values, of which privacy is part, need to be respected;
- "*a form of intimacy*", which means that privacy is considered to be a requirement for the development of personal relationships. Solove writes: "*We form relationships with differing degrees of intimacy and self-revelation, and we value privacy so that we can maintain the desired levels of intimacy for each of our varied relationships*" (Solove, 2008: 34). In this conception privacy pertains, for instance, to the idea that a person's family life ought to be devoid of the intervention of outsiders. This means that privacy, in this conception, relates to a certain free zone for intimate feelings (Vedder, 2009: 11).

All of these conceptions have been criticized from various directions (for an overview, cf. Nissenbaum, 2010; Solove, 2008). What the criticisms often come down to is that (a) the notion of privacy is left too vague or too broad, or alternatively, that it is defined so narrowly that many things that we consider to be private are not covered by it; or (b) that the arguments raised for privacy protection do not explain why it is that we *value* privacy, i.e. why it is worth protecting in the first place.

In order to solve the first problem Solove has argued that "*instead of conceptualizing privacy with the traditional method, we should instead understand privacy as a set of family resemblances*" (Solove, 2007a: 756), referring to the later Ludwig Wittgenstein's explanation of the way in which many concepts in language lack a single, 'essential' meaning, but rather are made up of a variety of overlapping yet also diverging meanings. To Solove, thus, privacy is a notion that has several interrelated meanings in different contexts. Solove writes: "*privacy is not reducible to a singular essence; it is a plurality of different things that do not share one element in common but that nevertheless bear a resemblance to each other*" (Solove, 2007a: 756). This is why, he concludes, all theoretical attempts to conceptualize the (one) essence of the notion of privacy have failed in by being either too broad or too narrow.

3.1.3 Choosing a perspective: Contextual integrity

In this deliverable we follow the privacy conception of Helen Nissenbaum, which is especially relevant in relation to modern technology. Nissenbaum defines privacy as "*contextual integrity*" (Nissenbaum, 1998, 2004, 2010).[14] Having privacy, she argues, means that the personal integrity of individuals is maintained across and between the various contexts they engage in each day in their everyday lives (also see O'Hara and Shadbolt, 2008: 77 ff.). Nissenbaum starts from the following observation: "*Observing the texture of people's lives, we find them* [...] *moving about, into, and out of a plurality of distinct realms. They are at home with families, they go to work, they seek medical care, visit friends, consult with psychiatrists, talk with lawyers, go to the bank, attend religious services, vote, shop, and more. Each of these spheres, realms, or contexts involves, indeed may even be defined by, a distinct set of norms, which governs its various aspects such as*

[13] Think, for instance, of situations in which one's credit rating may suffer, one's insurance premium will go up, or worse, one experiences the results of identity theft due to errors in and/or abuse of one's personal information by third parties, for examples businesses.

[14] James Rachels formulated a similar position in his 1975 article *Why privacy is important*, in which he emphasized the relational character of privacy (Rachels, 1975).

roles, expectations, actions, and practices" (Nissenbaum, 2004: 137). Using Michael Walzer's theory of different spheres of justice (1983), Nissenbaum argues that what privacy is all about is respecting the contextual boundedness of the (personal) information individuals share in each of these distinct realms. Phrased differently, according to this view privacy revolves around a person's ability to compartmentalize his or her (social) life, so that information about him or her that may be damaging or create embarrassment outside the context in which it is regularly (made) known to others is protected. For instance, when a person has a certain medical condition, she will not consider this information private for her doctor or (certain) other health professionals involved in treatment. But she might very well consider this information private with respect to her employer or to an acquaintance encountered at the grocery shop. Context, therefore, is one of the key parameters with respect to privacy, according to Nissenbaum.

It is not helpful to claim that specific items of information 'are' public or private, as if their status as one or the other (or a little in between) is an essential element of the information itself. Many privacy researchers assume "*the existence of distinctive realms of the personal, familial, and intimate, on the one hand, contrasted with the public, on the other. Scholars interested in this kind of privacy protection emphasize the importance of a realm to which people may go, from which others are excluded. They conceive of this realm in terms of a secure physical space, in terms of a private psychological space, or even in terms of a class of information that is sensitive or intimate over which one would have supreme control*" (Nissenbaum, 1998). But this is not an adequate description of what people conceive of a 'private' in their everyday lives. What makes information private is not chiselled in stone. It does not (necessarily) relate to the *content* of that information. Sometimes individuals share information that is exceptionally intimate and personal, and do so without much concern. Moreover, sometimes they feel that their privacy is violated when information about them is shared, even when that information is *not* of a sensitive or personal nature. This is so, says Nissenbaum, because whether or not information is deemed private relates to the context in which it is used and considered appropriate. Thus, information may be deemed private in one context and less private or even public in another. What makes it private or public is the context in which the information is accessed and used, and the 'audience' that has access to this information in that context.[15]

What is crucial in Nissenbaum's interpretation of privacy is that it is a *social* concept, rather than an informational one, as it is often taken to be. Nissenbaum emphasizes that sharing information *per se* is not an issue – we all share information with others every day and are entirely unconcerned about privacy issues with respect to these sharing practices most of the time. What is at stake, she says, is what happens when information is shared *outside* the context in which it was shared in the first place. This is a social issue, rather than a problem with sharing information as such. Nissenbaum summarizes her position as follows: "*When information is judged appropriate for a particular situation it usually is readily shared; when appropriate information is recorded and applied appropriately to a particular circumstance it draws no objection. People do not object to providing to doctors, for example, the details of their physical condition, discussing their children's problems with their children's teachers, divulging financial information to loan officers at banks, sharing with close friends the details of their romantic relationships. For the myriad transactions, situations and relationships in which people engage, there are norms — explicit and implicit — governing how much information and what type of information is fitting for them. Where these norms are respected I will say that contextual integrity is maintained; where violated, I will say that contextual integrity has been violated*" (Nissenbaum, 1998). As we will show below this view of privacy is highly relevant in a world of high technology, and is very applicable to social network sites and collaborative workspaces in particular.

---

[15] Our PRIME Surveys confirmed this claim.

3.2 Privacy or security: A bad trade-off

In recent times, especially after the 9/11 terrorist attacks and those in Madrid (2004) and London (2005), the value of protecting privacy has often been contrasted with that of collective safety and security (cf. Solove, 2008: 83). Many governments have adjusted the balance between these two apparently conflicting values by claiming that in order to safeguard collective security it is necessary to gather data about the behaviour of their citizens through massive surveillance and data mining (cf. Hildebrandt, 2009; Hough, 2009; Nissenbaum, 1998; Nissenbaum, 2010). As a justification, both governments and individuals often argue that those who are not engaged in any illegal activities need not worry about their privacy, because they have 'nothing to hide' (cf. Solove, 2007a).

Solove correctly critiques this claim by pointing out that "*the problem with the nothing to hide argument is the underlying assumption that privacy is about hiding bad things*" (Solove, 2007a: 764). Privacy, thus, would serve only those people who attempt to operate on the fringes of, or even outside the law (to a larger or smaller degree). Therefore, the argument goes, it is justified to diminish the extent of individuals' privacy, since this enables law enforcement to track down these individuals. Security and lawful behaviour are placed on one side of the equation, whereas privacy, secrecy and illegal behaviour are placed on the other. However, this distinction is flawed for several reasons. First, from our interpretation of privacy as contextual integrity it follows that, in fact, *everyone* has something to hide. The examples we have discussed in the previous paragraph are tell-tale: we do not want medical information to leave the doctor's office, and we do not want financial information to leave the bank or the loan company. If medical information reaches one's employer or financial information reaches one's insurance company all of us would feel that something was revealed that ought to have remained hidden. But more we can also think of more 'innocent' examples such as this: when we buy someone a birthday gift online, we do not want our social network site to share the purchase with the birthday boy or girl beforehand. The choice to hide or share information is contextual, therefore, as we have seen above. What is deemed private depends on the context, which means that at times even the most intimate information is not private, whereas at other times even the most public information is considered private. Creating a dichotomy between privacy-and-illegality versus security-and-legality is misleading, therefore: it misrepresents the complexity of our privacy perception in everyday life.

Second, – and this is an even more fundamental argument against the proposal of promoting security and surveillance at the expense of a seriously diminished level of privacy – as Solove and many other privacy researchers note, privacy is a key element of living in a free and democratic society. It enables individuals to speak their minds – even if, or maybe especially when their ideas oppose those of the dominant political institutions of their society. Moreover, it stimulates creativity and openness between people, and it allows individuals to retreat into a space they call private, where state intervention is not allowed. Part of what makes a society a good place to live in is the extent to which it allows people freedom from the intrusiveness of others. A society without privacy protection would be suffocating, and it might not be a place in which most would want to live. Therefore, claiming that the privacy of citizens should be diminished in favour of their (alleged) security goes against some of the core values of our democracies and the freedom we hold dear. When protecting individual rights, we as a society must find a balance between security and privacy, of course, but as Solove points out it is crucial that we respect privacy in order to create the kinds of free zones for individuals to flourish (Solove, 2007a: 762).

3.3 Privacy and modern technology

As we mentioned at the beginning of this chapter privacy has become an important topic for debate in the past century, especially in light of a number of technological developments. Privacy issues often occur in relation to the use of such technologies. Warren and Brandeis already foresaw this fact, and their concerns have been echoed by many in recent decades, particularly after the introduction and rapid proliferation of information and communication technologies. A variety of different issues are mentioned in debates on privacy and technology. We have clustered them in the following categories: (1) information and communication technologies enable us to collect, copy, link and distribute (personal) information, thus allowing for the creation of extensive profiles of individual persons; (2) information and communication technologies enable us to store information indefinitely, thus making it impossible to erase or forget this information; (3) participatory information and communication technologies (e.g. web 2.0) enable anyone to publish another's personal information, which may have serious consequences for the other's reputation; and (4) a lack of privacy-awareness when using information and communication technologies may lead to information leaks and leaving unintended and/or unobserved virtual traces. We will discuss each of these issues in turn below and distil a more general model from them at the end of this section.

3.3.1 Collecting, copying, linking and distributing information

Information and communication technologies derive the first part of their name from the fact that they facilitate the collection, manipulation, distribution, and maintenance of information. They do so on a massive, currently even on a global scale, while offering these possibilities with great ease for users and at little or no cost. While these features have contributed to immensely increased efficiency and effectiveness with regard to the management and spread of information, these advantages are also one of the most important downsides to the use of information and communication technologies. Information about individuals can be collected, copied, linked and distributed easily, efficiently and cheaply, thereby offering various risks for the privacy of the individuals involved. Michelle Hough phrases it as follows: "*Before the introduction of advanced computing and communication technologies, aggregating information about even a single individual could be exhausting, time-consuming, and was highly dependent upon the whims of the human gatekeepers of the information. Imagine, for example, the effort required to compile the profile of an individual for a deep background check. The compiler would need to make separate visits to hospitals and physicians, to any schools the individual may have attended, to former places of employment, to banks and other possible places of business, and to law enforcement agencies in any locations where the individual lived or likely spent time. At each destination, the compiler of the data likely would have had to interact with a human keeper of the records, presenting arguments as to why the information was needed as well as credentials to ensure that the compiler was authorized to collect the data. As inefficient as it now sounds, the storage of paper records in disparate locations actually created a protective buffer, ensuring that data was not released without considerable effort and only with just cause*" (Hough, 2009: 406). But gathering information was not the only cumbersome and difficult task. Because information was recorded on paper and stored in files and folders at different locations it was difficult and time-intensive to copy and move information from one place to the next. Disseminating it, in turn, was also complicated and labour-intensive – it involved such steps as, for instance, running it through a copying machine and mailing it off to one or more specific addressees. Nowadays, information is stored in files that can be copied or moved with the simple click of a mouse, and the information in these files is often easily extractable or even directly compatible with that in other files. Creating links between different files is easy as well.

By combining and linking various pieces of disparate information through the use of technology an image emerges of what Solove calls a person's 'digital persona'. The scale on which the combination and aggregation about individuals takes place becomes clear from an example from Solove's book *The digital person* (2004). He describes a company called Regulatory DataCorp (RDC), which has "*created a massive database to investigate people opening new bank accounts*". In the database information is gathered "*from over 20,000 different sources around the world*" (Solove, 2004: 21). RDC provides this information to loan and insurance companies so that these can do an extensive background check on prospective clients. Considering the amount of sources that RDC taps from it is obvious that the information gathered in their database reveals much more about individuals than their financial status alone – which, one could rightly argue, would be the only information needed to judge whether a prospective client is a risk to the company or not – thus giving these businesses a rather detailed picture of their clients' lives.

In the process of combining, moving, copying, editing and connecting disparate pieces of information privacy problems may occur that can be understood as violations of contextual integrity. Nissenbaum points out that "*the process of compiling and aggregating information almost always involves shifting information taken from an appropriate context and inserting it into one perceived not to be so* […]. [Moreover,] *while isolated bits of information (as generated, for example, by merely walking around in public spaces and not taking active steps to avoid notice) are not especially revealing, assemblages are capable of exposing people quite profoundly*" (Nissenbaum, 1998). Thus, two levels of privacy problems can be distinguished in this area: issues that arise over the *movement* of information from one context to another, and issues that occur because of the *combination* of different pieces of information. Note that both can be understood within the realm of contextual integrity. First, when moving information from one context to another this may violate a person's privacy because information that is not intended for use outside that context is made accessible. We have seen examples of this type of privacy violation above (medical information, financial information etc.). Second, when compiling or aggregating information the result may reveal things about a person within one or more specific contexts that are not deemed appropriate. For instance, certain insurance and mortgage companies demand that some individuals applying for a mortgage undergo extensive medical testing as a requirement for having their mortgage approved. This happens, these companies argue, when the prospective clients are deemed 'risky', for instance because they have a low income or because they have requested a high mortgage. However, the aggregate client profile that mortgage and insurance companies thus procure about individuals may reveal information that is irrelevant or unnecessary for the risk assessment made by these companies, and what's worse, violates these individuals' privacy.

3.3.2 Storing information indefinitely and the right to be forgotten

A second characteristic of information and communication technologies that is often mentioned in debates on privacy is the fact that these technologies facilitate the *indefinite storage* of data, and hence also of personal or private information. Solove writes that these technologies enable "*the preservation of the minutia of our everyday comings and goings, of our likes and dislikes, of who we are and what we own. It is ever more possible to create an electronic collage that covers much of a person's life — a life captured in records, a digital person composed in the collective computer networks of the world*" (Solove, 2004: 1). By storing a wide array of data about individuals throughout their lifetime, it becomes possible to get an intimate and quite complete image of who they are (and have been), what they do (and have done), and whom they know (and have known). Moreover, the image that arises in this fashion is incredibly difficult to remove or delete, since the information it contains may come from a variety of sources, be hosted by different servers and services, and be stored in a number of places. Also, as we have seen above,

information can easily be moved, transferred and copied, which makes it even more difficult for individuals to manage, alter or delete personal information about themselves. In *The future of reputation* (2007b) Solove predicts that in the not so distant future we will have to learn to live in a world in which for all of us there is "*a detailed record beginning with childhood*" which can be accessed through the internet, a record "*that will stay with us for life wherever we go, searchable and accessible from anywhere in the world*" (Solove, 2007b: 17). The permanency of information that is created through the use of information and communication technologies (and especially through our use of the internet) has serious consequences for the level of freedom that individuals have to shape their lives, and hence for their privacy. "*We may find it increasingly difficult to have a fresh start, a second chance, or a clean slate*" (Solove, 2007b: 17). Personal information from the past can have a negative impact on finding a job today, or meeting a spouse, or engaging in contact with others.

As we will see below in more detail the permanent storage of personal information can also have a negative impact on individuals' freedom to construct their identities. The personal information that is gathered and stored in databases and on the internet functions as '*identity pegs*', to use a term by Erving Goffman. Identity pegs are fixating mechanisms to consolidate or pin down a person's identity. They are created and maintained both by individuals themselves, and by others surrounding that individual. We see this, for instance, in practices such as name-giving or handing out "*documentation that individuals carry around with them purportedly establishing personal identity*", but also in the composition of files about a person with information that identifies as being that specific individual (Goffman, 1968: 77). And think also of identification numbers, social security numbers and other so-called Globally Unique Identifiers (GUIDs) that facilitate the pegging of individuals. When identity pegs such as these are difficult or even impossible to erase for the individual to whom they refer, this may hinder that person in the construction and expression of his identity.

These facts combined have led several privacy advocates to argue that we should find ways to implement what they call 'the right to be forgotten' in databases and on the internet (Mayer-Schönberger, 2009). Their position starts from the idea that before the advent of extensive storing facilities for all kinds of data through the use of information and communication technologies a lot of information about a person's life or past actions tended to sink away in other people's memories over time. In the words of Mayer-Schönberger: "*Since the beginning of time, for us humans, forgetting has been the norm and remembering the exception.* […] *Today, with the help of widespread technology, forgetting has become the exception, and remembering the default*" (Mayer-Schönberger, 2009: 2). Even if it was contained in paper files the physical inaccessibility of such records, the stand-alone character of such files and the difficulties of searching through them contributed to the fact that much of a person's past was forgotten as his life progressed. As we have argued above, information technologies, with their easy search functionalities and interconnected databases, in which individuals can easily be traced, for instance through the use of GUIDs, contribute to the disappearance of this kind of forgetfulness – and hence it becomes necessary to think about artificial (legal, institutional, technical) solutions for forgetting – or at least of progressively restricting access to personal data over time – in a world of information technologies to recreate (some level of) the 'natural forgetfulness' of the past.

3.3.3 Web 2.0 and the value of reputation

Daniel Solove begins his book *The future of reputation* with a telling example of the third issue relating to privacy in the modern world: that of managing one's reputation in a world of web 2.0. He describes the case of what has widely come to be known as 'the dog poop girl'. A girl on a subway train in South Korea was accompanied by her dog, which pooped on the floor. When

asked to remove her dog's droppings she refused. A passenger on the train took some photographs of the girl and posted a blog about the incident on the internet and within days this posting spread far and wide, reaching a worldwide audience of unknown but undoubtedly massive proportions. The girl's name became public and all sorts of details about her past and personal life were revealed online. Her reputation was ruined, which led her to drop out of university.

In the previous chapter we have seen that one of the key characteristics of web 2.0 is the fact that individual users have become actively engaged in the creation of content and in sharing information on the internet. On the one hand this is a wonderful development, for instance because it taps into 'the wisdom of crowds' (Surowiecki, 2004), because it promotes the creation of all sorts of open source software and other content, because it enhances the diversity of information available and because it increases the amount of topics on which users can find information. Also, users' opinions and ideas truly count – anyone can participate and share his vision about any topic of his liking, making the current generation of the internet a more democratic realm for free expression than its first generation forerunner.

However, the possibilities for sharing information about others, and especially in the case of damaging information about others, also offer a serious downside to web 2.0. Reputations can be made or ruined with a few strokes on a keyboard, and, as the dog poop girl's example shows, anyone can easily become a target for negative publicity, with devastating consequences. Gossiping and storytelling have always been key ingredients of communities and social groups – they are part of what brings people together and functions as the cement of social relations. Before the advent of information and communication technologies, and especially before the advent of web 2.0, gossip, rumours and stories about other people generally had a limited reach – they were contained within the community from which they originated. The second generation of the internet has changed this. Nowadays gossip and rumours have moved to the internet, thereby changing the rules of this social practice, both for those who engage in gossiping and for those whose reputation is at stake.

Several elements play a role in this new phenomenon. First, there is the fact that contributions and comments about other people can often be made in a rather anonymous fashion. The writer can hide behind a screen name, thereby undermining norms of visibility and reciprocity, as these govern interactions in the offline world. Oftentimes, the impression arises that writers are less inhibited and less socially compliant when communicating in what they perceive to be the relatively private anonymous world of online forums, wikis and message boards. But even when the author does make himself known, for instance in a blog posting, the distance created by a mediating screen appears to invoke a less socially constrained form of communication. It is easier to write negatively about another person from the privacy of one's own living room, than to speak the same words in the presence of the person they are about. Ridiculing others is thus made easier and taken to more extreme levels than it would in face-to-face interaction in the offline world.

Second, there is the issue of the size of the audience. The blog about the dog poop girl was picked up by other bloggers and then found its way to more traditional media such as newspapers and television, first in South Korea, and then also in other countries around the world. A small incident concerning what could rightly be called a relatively minor social transgression thus turns into a worldwide scandal with an audience of maybe millions. Without information and communication technologies this would not have happened. The advent of mobile technologies only increases this trend. Many mobile telephones are equipped with cameras and other recording facilities these days, which enables users to quickly and easily capture images and sounds as they move through their everyday lives. Mobile internet, and the advent of blogging and social network facilities for mobile phones further facilitate 'reporting on the fly' by any laymen 'correspondent'.

Kate Raynes-Goldie makes an interesting observation with respect to privacy and the current generation of web 2.0 technologies. She explains that from the 1970s onwards privacy has been understood predominantly in *institutional* and *informational* terms, that is as a means of protecting

personal information from institutions (e.g. companies, corporations and government organisations) (Raynes-Goldie, 2010: 4). However, in web 2.0 the *social* aspects of privacy appear to have become much more central, at the expense of the institutional aspects of it. Research on web 2.0 environments, for instance social network sites, shows that users in these domains are primarily concerned about privacy in a *social* sense, i.e. they worry about privacy issues that may arise in relation to or between the users of these networks, rather than the providers of these sites or other (government) organizations. We will come back to this phenomenon in much more detail in Chapter 5 on privacy issues in social network sites. What is relevant for now is that with her emphasis on the social aspects of privacy Raynes-Goldie may in fact have hit the nail on the head in a much broader sense with respect to web 2.0: if reputation becomes a more critical factor to manage in virtual worlds, and if users can more easily make or break the reputations of others by posting personal information about them online, then Raynes-Goldie is correct to point out that these are not the 'traditional' institutional privacy issues, but rather that they emerge because of social interactions between ordinary individuals. Therefore, it is helpful to bear the relevance of social privacy in mind in the chapters to come.

3.3.4 Leaking information and leaving traces

As we have seen in the previous paragraphs privacy issues may occur easily in a world of information and communication technologies, because of the massive collection, combination, multiplication, dissemination and permanent storage that these technologies facilitate, and because of users' possibilities for making or breaking the reputation of others. A last category of privacy issues arises because individuals using these technologies leave digital traces, sometimes without knowing they do so and sometimes in full awareness, and thus leak information about themselves as they go about their business in virtual worlds but also in the real world. Search engines register the keywords we use to find information on the internet, but also the links we click on and the paths we take while navigating in the online realm. CCTV cameras register our images as we move through airports, train stations, shops, and even entire city centres of many cities in the Western world. Credit and debit card details are stored with each of our purchases. Electronic ticketing systems or vehicle tracking systems register out itinerary as we travel from home to work or to the cinema. And the list goes on.

Worryingly, a variety of scientific studies has shown that "*the 'average' citizen or consumer*" has "*a serious lack of awareness* […] *with respect to the technical possibilities for gathering, storing and processing data about* [his person]" (Vedder, 2009: 8). While privacy has become a topic of debate amongst the general public and in the popular press in recent years, many people still have very little overview of the totality of all the digital traces they leave on any average day. Studies show that the majority of subjects expresses genuine concern with respect to their privacy, for instance when they go on the internet (cf. Paine *et al.*, 2007). However, as an in-depth study by Paine et al. reveals, what users are concerned with and label as 'privacy' is not clear at all, and refers to a bundle of fears for various aspects of technology use. The study showed that their concerns range from security breaches (fear of viruses, Trojans and spyware) to fear of attracting spam or encountering hackers. Moreover, and this is particularly important for the current topic at hand, while a significant number of users is concerned about their privacy in online environments they lack the tools or knowledge to better secure themselves against perceived threats (Paine *et al.*, 2007). Thus, even when privacy-awareness is in place individuals may still lack the ability to protect themselves adequately in the complex world of modern technology.

A last element that is relevant in relation to leaving digital traces and leaking information is this: as the discussion in the previous section revealed, unfortunately it is not just users themselves who (intentionally or unintentionally) spread their personal information on the internet. Other people

and organisations do so as well. In the words of Solove: "*...it is not just we ourselves who might leak information – data about us can be revealed by our friends or enemies, spouses or lovers, employers or employees, teachers or students... and even by strangers on the subway. We live in an age when many fragments of information about our lives are being gathered by new technologies, horded by companies in databases, and scattered across the Internet. Even people who have never gone online are likely to have some personal information on the Internet*" (Solove, 2007b: 10). Sometimes unintentionally, sometimes wilfully, individuals and businesses disseminate information about us, leading to serious privacy hazards.

3.3.5 Technology and/or its human users: What is the source of privacy problems?

What can we conclude with respect to privacy issues and modern technologies? In the previous sections we have encountered a number of different sources from which privacy problems may arise in relation to information and communication technologies. Sometimes they are caused by technological advances themselves, such as the possibility to link and store massive amounts of data. Sometimes people are the cause of privacy problems, for instance when they spread (discrediting) information about others in online communities or when they leave information traces in virtual and offline worlds. Colin Bennett and Charles Raab have created a model on privacy issues and technology that brings together these seemingly disparate causes in a single framework (Bennett and Raab, 2006). Their model is depicted in Figure 3 below.

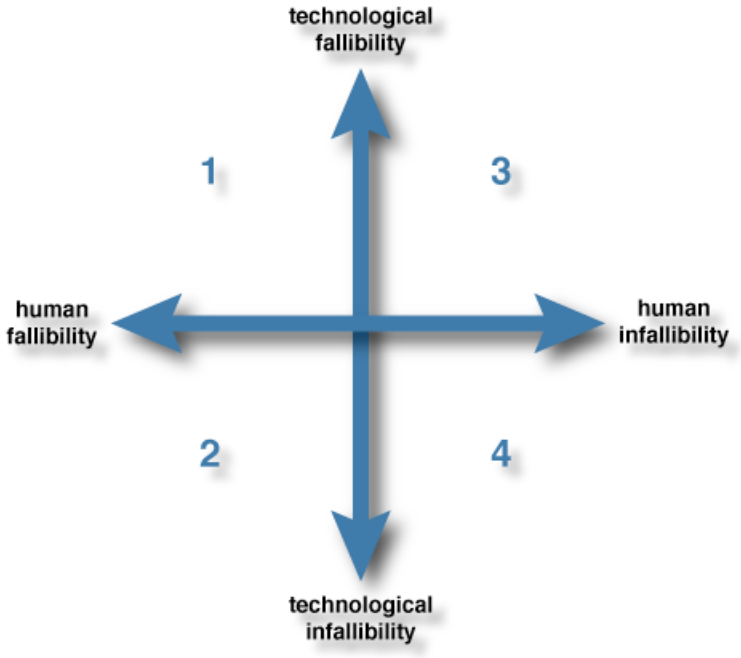


Figure 3: Privacy issues model, based on (Bennett and Raab, 2006).

Bennett and Raab argue that "*the problem of privacy has its roots in human agency as well as in structural conditions*" (Bennett and Raab, 2006: 25), that is, it may originate both from humans

and from the technologies themselves. They continue by discussing each of the four quadrants of their model (Bennett and Raab, 2006: 26):

- Privacy issues arise most easily and most often in quadrant 1, where human fallibility meets technological fallibility, that is where humans use technologies to gather, store or disseminate the wrong personal information or too many details, while the technology they use is insufficiently safe. Examples of privacy transgressions in this quadrant are "*excessive collection of personal data, inaccuracies, inappropriate disclosures, and so on*";
- Sometimes privacy issues may occur because of human actions, despite the fact that the technological systems with which they work are sound enough. Individuals may "*draw the wrong inferences or conclusions from outputs of data produced by the system, whether because of inadequate training, the biases inherent in the pursuit of certain organizational goals, the pressures of reward systems in the organization, or some other reason related to the workings of human agency*". Unintentional privacy leaks and leaks due to a lack of knowledge or capacities when working with technologies can also be included in this category, which is represented by quadrant 2;
- The reverse can happen as well: sometimes privacy issues arise because of flaws in technology, even when or in spite of the fact that the individuals working with this technology do their best to prevent them. This is what happens in quadrant 3. Examples of this combination, Bennett and Raab say, include the following: "*databases may be obsolete or highly inaccurate, or data-processing capacity may be deficient, or computer systems may be vulnerable to a variety of malicious attacks*";
- Privacy issues of a very different kind may occur in the last quadrant of this model. The cause of privacy problems in this fourth quadrant does not have its roots in human or technological errors, but rather in the opposite: it is their perfect *cooperation* that may cause problems. After all, when humans and technologies cooperate as harmoniously as possible to gather, combine, store and disseminate personal information the 'surveillance society' that so many privacy advocates fear may come one step closer. In the words of Raab and Bennett: "*...the fear of the 'surveillance society' in which our personal data can be matched, profiled, mined, warehoused, and manipulated for a range of social and economic ends is premised exactly on the fear that human agents and new technologies will combine* as intended *to reach new levels of intrusiveness, and from which there is no escape*" (Bennett and Raab, 2006: 26, emphasis in the original).

All of the privacy problems we have discussed in the chapter in relation to modern technologies can easily be fit into Bennett and Raab's model. Collecting, linking, copying and storing information can cause privacy problems due to technical fallibility and to human fallibility, but also due to the combination of technical and human *in*fallibility. Therefore, it can occur in all four quadrants of the model. Leaking information and leaving traces can be caused both by human and technological fallibility, so this, too, can occur in all four quadrants of the model. Last, our description of privacy issues that result from a damaged reputation because others share personal information about a person in web 2.0 environments is a result of human fallibility, and thus occurs in quadrants 1 and 2 of the model. What the model enables us to do, then, is to categorize the privacy issues that arise and cluster them into groups based on their originators (humans or technologies), and hence also point towards (the most straightforward steps in the direction of) their solution.

With this model we have come to the end of this chapter. We now have a firm idea of what privacy is, why it is a valuable concept, in particular in a world of high technology, and we have an understanding of why privacy is a concept in disarray in relation to modern technologies. Now it is time to turn to the two focal web 2.0 technologies of this deliverable, collaborative workspaces and social network sites, and investigate in more detail which privacy issues may occur in these environments. In the next chapter we will turn to collaborative workspaces; in Chapter 5 we will discuss privacy issues in social network sites.

Chapter 4

Privacy in collaborative workspaces

In the previous chapter we have discussed a number of aspects of privacy, and we have explained why with the advent of modern technologies privacy has come under pressure from different directions. Internet technologies (both web 1.0 and web 2.0) contribute to this development. In this chapter we will discuss in more detail how and which privacy issues arise in collaborative workspaces, the first of the two technologies we review in this deliverable.

To begin with we must identify and briefly describe the 'privacy stakeholders' and 'privacy adversaries' that are relevant in the context of collaborative workspaces. This we will do in section 4.1. After that we present a list of privacy protection goals (section 4.2). Then we heuristically inspect two examples of collaborative workspaces, Wikipedia and phpBB, to see whether they met the goals formulated (sections 4.3 and 4.4). In the second part of this chapter we provide an analysis of the possible contradictions that with respect to the privacy protection goals (section 4.5), and distil a set of general requirements for privacy enhanced collaborative workspaces from the privacy protection goals and our analysis of the examples in this chapter (section 4.6). We end this chapter with a specific form of privacy protection that is relevant to collaborative workspaces: access control (section 4.7).

4.1 Stakeholders

The collaborative creation and modification of content is the main feature of collaborative workspaces. Thus, in collaborative workspaces privacy issues may arise due to the activities of creating, modifying or consuming content or stem from the content itself. Thus, the privacy of three different stakeholders could be at risk:

- First, privacy issues may arise *uninvolved third parties* ('non-readers'), for instance when the content of a collaborative workspace describes or discusses a natural person, who is not even aware of this discussion on the internet. Think, for instance, of a wiki page about a celebrity, or blog posts such as the one on the 'dog poop girl', which we've discussed in the previous chapter;
- Second, the privacy of *content consumers* ('readers') may be compromised when all activities of the reader – for instance how long someone spent reading which article in a wiki – are

tracked and stored by the provider, or when personal data of the reader are discussed by others in a public forum thread;

- Third, privacy issues may arise with respect to *content creators* ('authors') in collaborative workspaces, for instance when authors contribute to the same forum on a regular basis and reveal snippets of information about themselves each time. In these cases combined information may be a threat to their privacy.

Obviously, these three groups are not completely distinct. An uninvolved third person may easily become a reader of a wiki page about herself, and even modify the page and become an author by simply clicking the 'edit' button. In general, all privacy issues that arise with respect to third parties are also true for content consumers (readers), and all issues that may compromise the privacy of content consumers (readers) also apply to content creators (authors).

Besides the question *whose* privacy is at stake, it is also relevant who the *adversaries* are, that is which parties can threaten the privacy of others, and which privileges they have. We distinguish between three possible classes of adversaries to individuals' privacy in collaborative workspaces: (a) third parties, (b) users and (c) providers.

- *Third parties* are outsiders of the system who have only minor options to execute legitimate features within the application;
- *Users* are participants of the collaborative workspace and have all privileges and features of (registered[16]) members available;
- *Providers* (including administrators, moderators, developers, etc.) of collaborative workspaces have extended privileges and access to data of the application and thus can be considered as the strongest attacker.

Table 2 provides an overview of the various privacy stakeholders and the adversaries that may undermine or jeopardise the privacy of the former, and indicates who may undermine whose privacy. As the table shows, the privacy of readers and non-readers is not jeopardized in collaborative workspaces by third parties or by registered readers. This is so, since readers and non-readers do not leave traces of their presence in collaborative workspaces for these groups – their reading activities are only visible to authors and providers of these workspaces. In all other cases, the privacy of participants in collaborative workspaces may be threatened from various directions. In our discussion of the two examples of collaborative workspaces we have investigated for this deliverable (sections 4.3-4.4) we will return to this table each time to show, using the numbers in the table, which type of users of collaborative workspaces (i.e. authors, readers, non-readers) may be attacked by which type of party (i.e. third parties, users as registered readers, users as authors, and providers).

[16] If registration is required or possible at all. If registration is not available, there is no difference between third parties and users with regard to their strength as adversaries.

		…can be violated by…			
		Third parties	**Users**		**Providers**
		in their role of…			
		non-registered readers	**registered readers**	**authors**	**admins, moderators, developers**
The privacy of…	**Authors**	(1)	(2)	(3)	(4)
	Readers	no privacy issues arise	no privacy issues arise	(5)	(6)
	Non-readers	no privacy issues arise	no privacy issues arise	(7)	(8)

Table 2: Privacy stakeholders and privacy adversaries in collaborative workspaces.

4.2 Privacy protection goals in collaborative workspaces

In a collaborative workspace each party that we have described above has its own particular protection goals related to privacy and security during interactions. The protection goals of a provider are not the same as those of an individual user, and these, in turn, are different from the privacy protection goals of third parties. We have composed a list of privacy protection goals based on a combination of two key articles in this field, one by Pfitzmann and Koehntopp (2001), and one by Wolf and Pfitzmann (2000). This list is presented in Table 3 below. The privacy protection goals in this table were used as a basis for the analysis of privacy issues in collaborative workspaces in the following sections (4.3 and 4.4).

Privacy protection goal:	**Description:**
1. Confidentiality	Personal data is *confidential* within a group if nobody other than the owner of the data and parties explicitly selected by the owner of the data (e.g. other users, the provider) are able to access this data.
2. Anonymity	A user of collaborative workspaces acts *anonymously*, if he or she is not identifiable within a set of subjects (for instance, within the set of all other users). Such a set is called the 'anonymity set'.
3. Unobservability	Working in collaborative workspaces (for example, reading, adding or modifying content) is *unobservable* if nobody except the legitimate users of the workspace can notice the actions in this workspace.
4. Unlinkability	*Unlinkability* ensures that it cannot be distinguished whether two or more items (e.g. pseudonyms, actions) are related to each other or not, and in particular whether they are connected

Privacy protection goal:	Description:
	to the same natural person or not.
5. Integrity	*Integrity* of personal data ensures that nobody is able to retrospectively modify the data or circumstances of disclosure, or that everybody can notice such an illegitimate modification.
6. Accountability (or repudiation)	*Accountability* ensures that the owner of personal data cannot successfully deny that this data belongs to him/her (for instance, he or she cannot deny that a statement was written by him or her).
7. Availability	*Availability* of resources, services and systems ensures that a user can access his/her personal data on the system whenever he/she wants.
8. Legal enforceability	*Legal enforceability* guarantees that users and providers are legally responsible for their actions and the data that they have disclosed (e.g. statements containing personal opinions).
9. Authenticity	The *authenticity of an individual*, for instance a user of a collaborative workspace, guarantees that the receiver of personal data is the person who was reasonably intended by the sender who discloses these personal data (e.g. based on previous interactions). In general, authenticity means that users are who they claim to be. *Authenticity of content* means, that the information at hand, for instance personal data referring to an individual, is truthful.

Table 3: Privacy protection goals for collaborative workspaces.

Figure 4 represents the underlying model we used in our analysis of privacy issues in collaborative workspaces. The analysis starts from the perspective of authors, readers and non-readers of collaborative workspaces, since it is their privacy that is at stake.

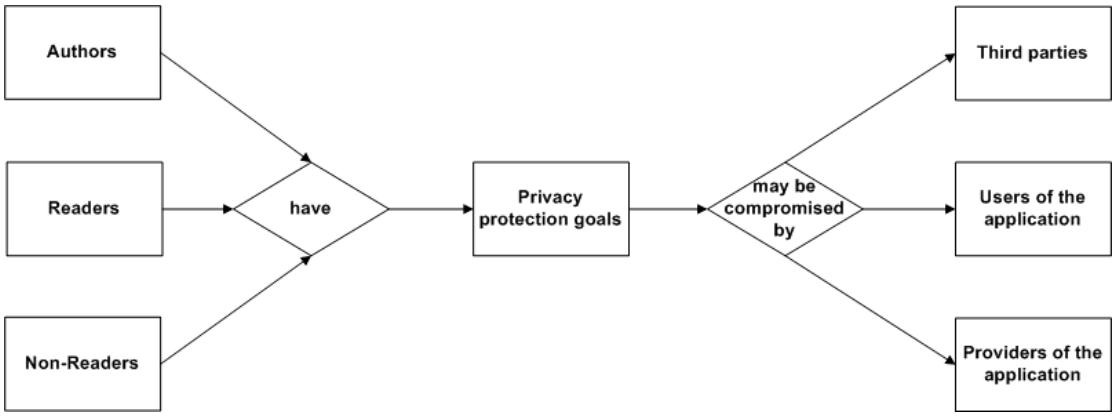


Figure 4: Model for the privacy analysis of collaborative workspaces.

In the following we present an analysis of privacy issues as they may happen to different stakeholders collaborative workspaces. As we have argued in Chapter 2 the term 'collaborative workspace' refers to a number of different web 2.0 environments, ranging from forums and wikis to blogs and file sharing systems. In our analysis of privacy issues we have chosen two examples of collaborative workspaces that met two criteria. First of all, the examples had to fit into different categories (i.e. we will discuss one example of a wiki system, and one of a forum), and second, they had to be popular and relatively well-known.

4.3 Example 1: Wikipedia

One of the most widely known examples of a collaborative workspace is the wiki-system Wikipedia (http://www.wikipedia.org). In this online encyclopaedia members of the Wikipedia community collectively create content in the form of lemmas. Readers can easily become an author and modify content in Wikipedia without registration beforehand. In early 2010, the online encyclopaedia was available in more than 250 languages, among which English (about 3,100,000 articles) and German (about 1,019,000 articles) were the largest ones (numbers based on Wikipedia's data [last accessed on 3 February 2010]).

Wikipedia uses Media Wiki software. For our analysis of privacy issues we have chosen to investigate the Wikipedia implementation rather than its software backbone provided by Media Wiki. In the following sections we will discuss privacy protection goals from the perspective of the registered and/or contributing Wikipedia user and describe how these goals can be compromised by attackers using current features and workflows in Wikipedia. As we have explained above, we distinguish between three possible attackers:

- *Third parties*: The attacker does not have his own Wikipedia account or any other special privileges;
- Wikipedia users: The attacker has a Wikipedia account, i.e. username and password, and similar rights and privileges as the target user[17];
- *Wikipedia providers* (including administrators, developers, etc.): The attacker has special privileges, for instance physical access to servers, or access to comprehensive usage data. Attackers of this kind may be considered the strongest one.

4.3.1 Privacy issues in Wikipedia caused by third parties

In this section we discuss the privacy protection goals that we presented in Table 3 above in relation to Wikipedia, and the ways in which some of the goals can be compromised by any third party.

 # 1. Confidentiality of personal data

All content pages in Wikipedia are open to the public. While this seems unproblematic on the face of it, in fact it is not. This is because Wikipedia does not merely consist of encyclopaedia lemmas,

[17] For details about privileges see http://en.wikipedia.org/wiki/Special:ListGroupRights [last accessed on 4 February 2010].

but also so-called '*user pages*', listing the personal information and contributions of the registered contributors to this online encyclopaedia. These contributors cannot restrict read access to their personal information, that is, they cannot make it accessible only to certain users. Moreover, just like with almost all other Wikipedia pages anyone can contribute to a person's user page. This means that personal information about a user can be added by the user himself, but also by others. Even if this information is correct, when published by someone else without the user's consent, this information could harm the user that it refers to. Moreover, as with all other information contributed via a wiki this personal data immediately becomes public. In conclusion, the privacy protection goal of 'confidentiality' – revolving around the idea that personal data can only be accessed by the owner or individuals or groups explicitly chosen by the owner – is not met in this collaborative workspace, since personal data on user pages are visible to third parties, users and providers of Wikipedia.

→ This issue applies to fields (1), (2), (3) and (4) of Table 2 above.

 # 2. Anonymity

When individuals wish to modify or add content to Wikipedia and are not signed in with a registered account, Wikipedia publicly logs their IP addresses. At least, the individual receives a message of this practice such as the one displayed in Figure 5 below before the IP address is actually stored and shown to the public. If the content editing is done anyway, the public display of the IP address enables any third party to know which IP address is responsible for the modification. When the contributor whose IP address is stored has a static IP addresses, it is possible to link him or her to a specific civil identity, or at least to identify a group of possible people who might be this contributor. Alternatively, cooperation with the Internet Service Provider (ISP) might reveal this information even for dynamic IP addresses (even if that is usually not possible for any third party).

Users who do not want to have their IP addresses published when editing in Wikipedia must sign in with a username and password. In this case the IP address is replaced by the username for the public. In both cases the privacy protection goal of 'anonymity' is not met to the fullest extent – users cannot contribute completely anonymously, since they are either identifiable through their IP address or through their user account, and anyone accessing Wikipedia can see these details.

→ This issue applies to fields (1), (2), (3) and (4) of Table 2 above.

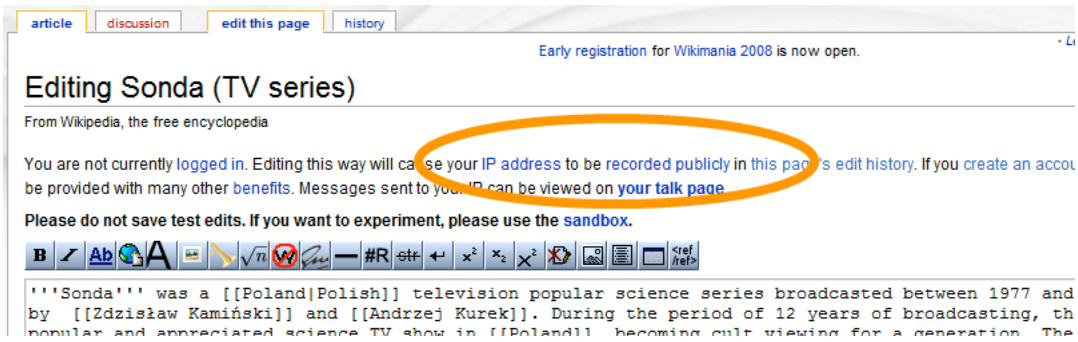


Figure 5: Message about the storage of the user's IP address when editing a page on Wikipedia.

To show how this privacy issue may arise in practice, and that it is also related to the balancing act between privacy on the one hand, and the objectivity and freedom of information on the other, we report a case from Wikipedia in the Netherlands revolving around one of the members of the

Royal Family and his then-fiancée, who learnt that she was less anonymous than she thought she was on the internet. In September 2007 Friso, one of the princes of the house of Orange, announced his engagement to a woman called Mabel Wisse Smit. Since Ms. Wisse Smit was to become a member of the Royal Family and be in line for the throne through her marriage with the prince, Parliament had to approve of the marriage, and thus a procedural background check by the Dutch Secret Service was started. It revealed that she had had a close relationship with a heavyweight Dutch drug criminal, a fact she had declined to mention at the beginning of her background check, thereby embarrassing Parliament and instigating controversy. The Dutch Prime Minister stated on television that he had received "*incomplete and false information*" about Ms. Wisse Smit's background by the young couple. These words were added to a Wikipedia page about the affair[18]. Soon thereafter they were removed, and when the public learnt that it was Ms. Wisse Smit herself who had removed them, using a computer in one of the Royal Palaces – a fact that can revealed easily by any third party through checking the IP address – public anger and outcry ensued.

Ms. Wisse Smit apologized for her actions by saying that she should not have edited these two words since they reflected a quote by the Prime Minister, but that she felt that it was her right to change a Wikipedia page discussing her person nevertheless, since it was in her interest that the page was an adequate representation of her person and personal information. The debate went on for several weeks in the press, and while most citizens understood that she had merely attempted to save her reputation and contain and minimize the negative publicity about her by deleting these words and changing the Wikipedia entry on her person, most felt outraged by the fact that her editing actions undermined the objectivity of the page, which is perceived to stem especially from its creation and editing by many different writers. The Wisse Smit case thus reveals an element of tension in privacy protection on collaborative workspaces: that between the individuals seeking to protect their reputation and good name, and the objectivity of the system which is guaranteed by the collective efforts of many.

 # 3. Unobservability

When someone decides to create a lemma about a new topic, this lemma is public from its earliest draft version onwards. All following changes, removals and additions, both in terms of the content of the article, the structure, and its spelling mistakes, are documented and accessible by everybody. There is no option to keep new ideas and draft versions private, nor is there a possibility to prevent others from modifying this lemma after its first release. Hence, the entire development of a lemma is observable by all, both providers, users of Wikipedia and anyone who is not a member of this platform. The privacy protection goal of 'unobservability' refers to the idea that only the legitimate users of a collaborative workspace – here in a narrow sense the particular article page – have access to the actions taken in that workspace. In the case of Wikipedia, however, everyone (both providers, registered contributors, non-registered contributors and outsiders who only access the encyclopaedia to find information) has access to those actions. Hence, the privacy protection goal of 'unobservability' is not met in Wikipedia.

→ This issue applies to fields (1), (2), (3) and (4) of Table 2.

 # 4. Unlinkability

As we have seen in Table 3 unlinkability means that it should be impossible to find out whether two or more items (e.g. pseudonyms, actions) are related to each other or not, and in particular

[18] See http://en.wikipedia.org/wiki/Mabel_Wisse_Smit [last accessed on 4 February 2010].

whether they are connected to the same natural person. Wikipedia does not meet this privacy protection goal either. It has a built-in search function that can be used to find out which user has made contributions to the system and in which lemmas. When using this search functionality it is easy to get a complete list of all modifications by the same registered user or IP address, including the time stamps that reveal when these modifications were made. This facilitates profiling: one could construct and image of the interests and habits of internet usage, at least for users who contribute frequently (see Figure 6 below). Journalist Thomas Crampton, for instance, gives an example of which topics contain contributions from people using the network of the European Broadcasting Union and summarises that these editors may have disclosed information about their organisation and themselves, probably unintentionally (Crampton, 2007). The WikiScanner[19], an elaborated search tool for Wikipedia, offers even more options for the search based on IP addresses from Wikipedia editors.

→ This issue applies to fields (1), (2), (3) and (4) of Table 2.

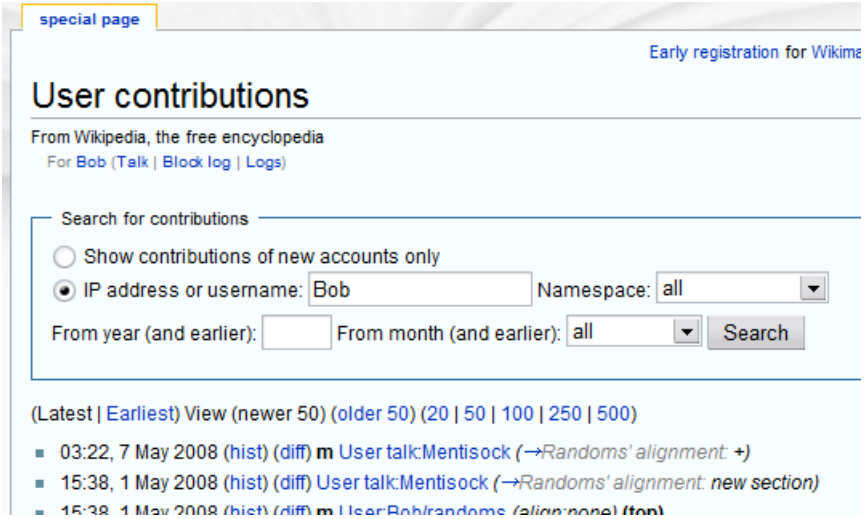


Figure 6: Search for all contributions of a single user on Wikipedia.

5. Integrity and # 6. Accountability

There are no features available in Wikipedia that would allow third parties to compromise the privacy protection goals of 'integrity' or 'accountability'.

7. Availability

Malicious third parties may be able to perform a so-called 'Denial-of-Service'-attack on Wikipedia, for instance by flooding the servers with too much traffic. The result would be that Wikipedia articles (including those that contain personal data) would become temporarily or indefinitely unavailable. So far, this issue is only a theoretical one and we are not aware of a reported incident about a successful Denial-of-Service-attack on Wikipedia.

→ This issue applies to fields (1), (2), (3) and (4) of Table 2.

[19] http://wikiscanner.virgil.gr [last accessed on 17 July 2008].

 # 8. Legal enforceability and # 9. Authenticity

There are no features available in Wikipedia that would allow third parties to compromise the privacy protection goal of 'legal enforceability' or 'authenticity'.

4.3.2 Privacy issues caused by other users in Wikipedia

People who actively participate in Wikipedia by being authors and/or registered readers are considered 'Wikipedia users' for our analysis. Wikipedia users may perform all of the same attacks as third parties that we have discussed in the previous section. This means that they, too, can cause privacy issues with respect to the confidentiality of personal data disclosed in Wikipedia, the lack of anonymity of contributors, the lack of unobservability of actions undertaken there, and the lack of unlinkability content created there. Wikipedia users may also violate the protection goal of 'availability' of (personal) data. In this section we will only describe further issues that may be caused by registered users of Wikipedia.

 # 1. Confidentiality

Besides the privacy issues with regard to the confidentiality of personal data that are described in the previous section, further issues revolve around the fact that some lemmas of the online encyclopaedia describe individuals who are of public interest, for instance movie stars, singers, politicians and other public figures. Authors may decide to write a lemma on them. Thus, these individuals may read their own biography or other personal information, written and posted online by Wikipedia users, maybe even without knowing about the disclosure of their personal data. Even if the article is revised or completely deleted after some time, the personal data that once was on Wikipedia may have been copied and duplicated anyway. Therefore, this clearly is a violation of the confidentiality of the person's privacy.

→ This issue applies to fields (3), (4), (5), (6) and (7) of Table 2.

 # 2. Anonymity

Wikipedia authors can compromise the anonymity of others by disclosing the real name of individuals who otherwise use a pseudonym or abbreviation when being in public – this applies especially to people who operate in the public's spotlight such as authors, pop stars and so on and so forth. An example from Wikipedia is that of the computer hacker Tron, whose real name, Boris Floricic, was added to the Wikipedia article about him after his mysterious death in 1998. The family of Boris Floricic sued Wikipedia and obtained a temporary restraining order against Wikipedia Germany, which forbade Wikipedia Germany to link their German domain (http://www.wikipedia.de) to the American resource (de.wikipedia.org), since the latter still contained the article with the complete real name of Tron. In their final decision in 2006 the Berlin State Court rejected the parents' claim and Tron's real name is still part of the Wikipedia article in all available languages – now complemented with a section about the controversy itself[20].

Another interesting example related to the issue of anonymity is a case around a Wikipedia entry on the German half-brothers Wolfgang Werlé and Manfred Lauber[21]. Werlé and Lauber were convicted of the murder of the German actor Walter Sedlmayer in 1990. After serving a fifteen-

[20] See http://en.wikipedia.org/wiki/Tron_(hacker) and for the German version http://de.wikipedia.org/wiki/Tron_(Hacker) [both lemmas last accessed on 17 February 2010].
[21] See http://en.wikipedia.org/wiki/Wolfgang_Werlé_and_Manfred_Lauber [last accessed on 4 February 2010].

year prison sentence the half-brothers were released in 2007 and 2008 respectively. After his release Werlé filed a lawsuit against Wikipedia, because he wanted his name removed from this encyclopaedia in connection with the murder of Sedlmayer. He claimed that the description of his role in the Sedlmayer murder case was a violation of his privacy, and that he had, moreover, just innocently served 15 years in prison for this crime. As a letter from his lawyer to Wikimedia, the company behind Wikipedia, which is also posted online [sic] states: "*His rehabilitation and his future life outside the prison system is severely impacted by your unwillingness to anonymize any articles dealing with the murder of Mr. Walter Sedlmayr with regard to our client's involvement*"[22].

While Werlé won his lawsuit in Germany, and the information was removed from the German version of Wikipedia in response to the verdict, the story of Seldmayer's murder case and of Werlé and Lauber's conviction for it remains on the English version to this day, and has now been complemented with detailed information of Werlé's lawsuit against Wikipedia. The Wikipedia page on the two half-brothers explains why this is so: "*Wikimedia is based in the United States, where the First Amendment to the United States Constitution protects freedom of speech and freedom of the press, under which the articles on Wikipedia would fall. In Germany, the law seeks to protect the name and likenesses of private persons from unwanted publicity*"[23]. What this reveals is that privacy is not an absolute right and that it is weighed differently in different legal systems around the world when it clashes with other rights, such as the right to free speech.

The Werlé case reveals another facet of privacy with respect to personal data disseminated in content on collaborative workspaces: while information that is collectively created in an online workspaces such as Wikipedia may be objectively sound and true, it may nevertheless reveal personal data about natural persons whose interests are not served or are even undermined by their publication, and who hence seek to regain control over their privacy and reputation by blocking the publication and accessibility of this content. In such cases the value of truthfulness and objectivity collides with that of an individuals' right to protect his good name.

→ These issues apply to fields (3), (4), (5), (6) and (7) of Table 2.

 # 3. Unobservability and # 4. Unlinkability

Wikipedia users can cause the same privacy issues with regard to the privacy protection goals of 'unobservability' and 'unlinkability' as third parties.

 # 5. Integrity and # 6. Accountability

There are no features available in Wikipedia that would allow Wikipedia users to compromise the privacy protection goal of 'integrity'. The same goes for the privacy protection goal of 'accountability', since all content (including personal data) is stored with an IP address or a user name.

 # 7. Availability

Authors can delete content from Wikipedia articles or user pages and thus limit the availability of this content. However, there are two points to consider: first, the deleted section remains in the history of the page and this history will still be available to all readers. Second, Wikipedia has a

[22] See http://www.chillingeffects.org/international/notice.cgi?NoticeID=30443 [last accessed on 4 February 2010].
[23] See http://en.wikipedia.org/wiki/Wolfgang_Werlé_and_Manfred_Lauber [last accessed on 4 February 2010].

lot of dedicated users who check latest edits and who will undo actions that, to their minds, do not improve the quality of an article but rather damage it.

→ This issue applies to fields (3), (4), (5) and (6) of Table 2.

 # 8. Legal enforceability

There are no features available in Wikipedia that would allow Wikipedia users to compromise the privacy protection goal of 'legal enforceability'. Since all content (including personal data) is stored with the user name or IP address of the person who contributed it, users can be held legally responsible for their actions and the data they have disclosed.

 # 9. Authenticity

As we have seen in the table of privacy protection goals (Table 3) in general 'authenticity of individuals' refers to the idea that users are who they claim to be, so that when they share personal information about themselves others may be certain that they are not being deceived. In Wikipedia authenticity is at stake. Since Wikipedia requires no proof of identity for registration, users can pretend to be someone else. After choosing a username (e.g. 'Florence Hervieux') and a password, a user can easily create a user page for this username, for instance by presenting a picture and a short curriculum vitae of the person in question. Afterwards, editing pages while using this account may give other users the impression that the person in question (in this case Florence Hervieux) has contributed to this lemma, when in fact this is not the case.

But the authenticity of individuals is not the only kind of authenticity that is at stake in Wikipedia. So is the 'authenticity of content', that is, the fact that the information presented in lemmas, for instance personal data referring to an individual, is truthful. In the so-called 'user pages' of Wikipedia, which we've discussed above, this is an issue. Wikipedia describes these user pages as follows: "*Wikipedia provides user pages to facilitate communication among participants in its project to build an encyclopedia. Generally, you should avoid substantial content on your user page that is unrelated to Wikipedia.* […] *...your user page is not a personal website. Your user page is about you as a Wikipedian, and pages in your user space should be used as part of your efforts to contribute to the project*"[24]. While Wikipedia states that user pages should not be used as personal websites, usually these pages do in fact contain personal data since their objective is to shape the digital identity of the Wikipedia user. However, we've seen above that there are no special access restrictions on such pages, so anyone who wishes to access them – regardless if they are registered users themselves or not – can access and edit any user page. Since write access is granted to everybody, a users' personal data can be modified by any other author, which – depending on the added or modified information – may lead to a bad reputation for the user, and in any cases constitutes an issue regarding the confidentiality of personal data. This issue is also true for Wikipedia articles about other persons, e.g., politicians, researchers, celebrities, etc. If the published information is wrong or damaging to their reputation, the individuals affected may correct the information or delete it, since they have write access in Wikipedia just like everyone else. However, the information they have corrected or deleted will still be available in the history of the page and may have been copied to other contexts outside Wikipedia as well.

An example of a privacy issues due to the lack of authenticity of content was the so-called 'Wikipedia biography controversy'[25] that occurred in 2005. In that year an anonymous writer created a hoax lemma on John Seigenthaler, a well-known American journalist. On this wiki page

[24] See https://secure.wikimedia.org/wikipedia/en/wiki/User_page [last accessed on 4 February 2010].
[25] See http://en.wikipedia.org/wiki/Wikipedia_biography_controversy [last accessed on 4 February 2010].

it was claimed that Seigenthaler had been a suspect in the assassinations of Robert and John F. Kennedy. This information was wrong, since in fact, Seigenthaler was a close friend of Robert Kennedy and had even acted as pallbearer at the latter's funeral. Seigenthaler was deeply shocked and hurt by the allegations. According to Wikipedia's Terms of Use and access settings, anyone with access to a computer with an internet connection can add, change, and delete content on almost all Wikipedia pages (the opening page is one exception). Thus, Seigenthaler could change this harmful information about his person (or ask someone to do so on behalf of him). In this case, moreover, Wikipedia took the unusual step of blocking the previous version of the page in its history as well, so that the content would no longer be accessible and could not be reinstated on Seigenthaler's page. However, unfortunately the information had been copied to other 'mirror' sites of Wikipedia, and hence a number of copies of the old page with the wrong and defamatory information were still available on the internet for several weeks.

While this case is not a privacy violation in the strictest sense, since it revolved around the dissemination of information that was false, and hence did not actually disclose any personal details about Seigenthaler, it did affect him immensely that others could spread such a story about him *as if* it were an interesting piece of personal information. Thus, even if the information was wrong, it surely was considered sensitive and intimate to John Seigenthaler himself. The central issue that this example reveals with respect to the privacy of natural persons is that while certain types of collaborative workspaces appear to have a high degree of reliability with respect to the content presented there, due to the collaborative efforts of many contributors behind them, at times personal information revealed in these environments may be untrue, and hence damaging to the subjects to whom they relate.

These examples illustrate that the privacy protection goal of 'authenticity' is not met in Wikipedia in any case.

→ This issue applies to fields (3), (4), (5), (6) and (7) of Table 2.

4.3.3 Privacy issues caused by the Wikipedia provider

What was said at the beginning of the previous section goes for the providers of Wikipedia as well: they may create all of the same privacy hazards as third parties. Thus, they do not meet the following privacy protection goals: (1) confidentiality, (2) anonymity, (3) unobservability, (4) unlinkability, and (7) availability. Moreover, just like other users they may create privacy problems relating to authenticity as well. But on top of that there are also a number of specific issues that can only be caused by the providers themselves. In this section we will discuss the particular privacy threats to users that derive from the role of the Wikipedia provider.

 # 1. Confidentiality

Since the providers are the highest authority regarding the management and control of all data stored in Wikipedia, in theory they could compromise the confidentiality of personal data in more ways than Wikipedia users or third parties can. For instance, Wikipedia providers could sell detailed user statistics and e-mail addresses from registered users to advertising partners. However, such behaviour would contradict the main principles of Wikipedia as a non-profit-organisation and have very negative consequences with respect to users' future participation in the online encyclopaedia.

→ This issue would apply to fields (4) and (6) of Table 2.

 # 2. Anonymity

First, as we stated above the providers of Wikipedia store all the IP addresses of contributors and editors, regardless of whether they are registered users or not. Anyone contributing to Wikipedia is not anonymous and participating in this online encyclopaedia in an anonymous fashion is impossible. On the Wikipedia website no hint can be found concerning the prohibition to create and edit pages while using so-called 'anonymisation services' (such as Anon or Tor[26]). However, it is technically impossible to edit Wikipedia pages while using these services. Thus, it can be assumed that Wikipedia does not allow completely anonymous editing, that is, editing by users whose IP address is invisible or inaccessible to the Wikipedia providers. In cooperation with the Internet Service Provider (ISP) of the user it is possible identify users as natural persons through their stored IP addresses.

Second, according to its privacy policy, Wikipedia stores personal data from each visitor, that is, both from contributors and from visitors who only read others' contributions. The data they store include the IP address, the requested Wiki page and data about a users' browser. It is stored for approximately two weeks. During this time it can be misused for identification or for the creation and improvement of user profiles of all visitors, despite the fact that Wikipedia states that the "*Wikimedia Foundation may keep raw logs of such transactions, but these will not be published or used to track legitimate users*"[27].

→ The first issue applies to field (4) of Table 2; the second to fields (4) and (6) of the same table.

#3. Unobservability

In Table 3 we described 'unobservability' as the possibility of reading, editing or creating content without any of the legitimate stakeholders (providers, users, third parties) of the workspace being able to observe these actions. Besides observing the actions of authors, Wikipedia providers are also able to observe the actions of alls readers. For instance, they can trace which Wikipedia pages a person visits.

→ This issue applies to fields (4) and (6) of Table 2.

 # 4. Unlinkability

By storing personal data such as IP addresses, requested Wiki pages and browser information from each reader and author, Wikipedia providers can link different actions from the same user. The level of accuracy for deciding whether two actions belong to the same user or not, depends on the question which data from the browser are actually collected. As the tool *panopticlick*[28] demonstrates the combination of a browser type, browser version, plugins and system fonts is usually enough to uniquely re-identify a user when he visits the same website again, and thus it is quite easy to link the Wikipedia pages that they individual currently visits with other actions of the same individual in the past.

→ This issue applies to fields (4) and (6) of Table 2.

---

[26] See http://anon.inf.tu-dresden.de/index_en.html and http://www.torproject.org/ [last accessed 4 February 2010].
[27] See the Wikipedia Privacy Policy http://wikimediafoundation.org/wiki/Privacy_policy [last accessed on 4 February 2010].
[28] See https://panopticlick.eff.org [last accessed on 18 February 2010].

 # 5. Integrity

As said above, the providers are the highest authority regarding the management and control of all data stored in Wikipedia. This means that in theory they could, for instance, change information on user pages or manipulate the history of articles retrospectively. These illegitimate modifications could be done in such a way that Wikipedia users would not notice them. Through these actions, the integrity of (personal) data might be compromised by the providers. However, if such behaviour would become public, it would result in very negative consequences with respect to the users' trust and future participation in this online encyclopaedia.

→ This issue would apply to fields (4) and (6) of Table 2.

 # 7. Accountability

In theory, Wikipedia providers are able to manipulate the history of articles, for instance, to map the contribution of unlawful content to another IP address. If they did so, it would become impossible to hold the original author accountable. However, as was the case with the privacy protection goal of integrity, it would be very unwise of Wikipedia to undertake such actions, because, if revealed, they would have devastating consequences for the future of this encyclopaedia.

→ This issue would apply to field (6) of Table 2.

 # 8. Availability

Providers can delete content from Wikipedia, so that this information is no longer available on the wiki page, and is also eliminated from the history of the article or user page in question. Moreover, providers can shut down the whole service and thus prevent the availability of all content (including personal data).

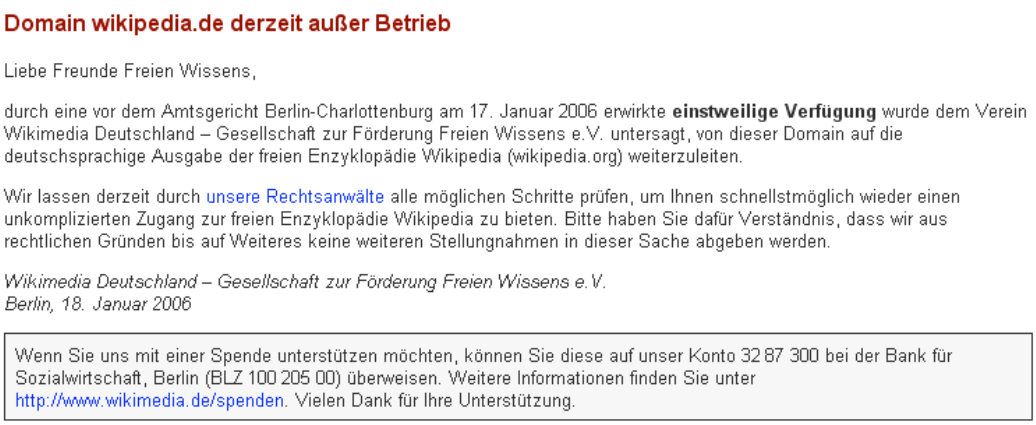
→ This issue applies to fields (4) and (6) of Table 2.

 # 9. Legal enforceability

The case of the German hacker Tron, whose real name was mentioned in a Wikipedia article about him against the will of his family, was introduced above in section 4.3.2. As a temporary consequence of the lawsuit, Wikipedia was forbidden to provide the article that included the real name in Germany. Instead of simply deleting the name from the article, Wikipedia decided to block the link from their German domain http://www.wikipedia.de to the American resource de.wikipedia.org, which still contained the article with Tron's real name. At this time, visitors of www.wikipedia.de attempting to access this lemma saw a notification of the block (Figure 7[29]). However, it was easy to side-step this block: if users typed de.wikipedia.org into their browsers' address bar they still had access to the German version of Wikipedia, including page that contained Tron's real name. This example demonstrates how a global organisation such as Wikipedia could bypass local legal judgements and thus hinder legal enforceability.

→ This issue applies to fields (4), (6) and (8) of Table 2.

[29] See http://en.wikipedia.org/wiki/File:Wikipedia_de_19_January_2006.png [last accessed on 18 February 2010].



Domain wikipedia.de derzeit außer Betrieb

Liebe Freunde Freien Wissens,

durch eine vor dem Amtsgericht Berlin-Charlottenburg am 17. Januar 2006 erwirkte **einstweilige Verfügung** wurde dem Verein Wikimedia Deutschland – Gesellschaft zur Förderung Freien Wissens e.V. untersagt, von dieser Domain auf die deutschsprachige Ausgabe der freien Enzyklopädie Wikipedia (wikipedia.org) weiterzuleiten.

Wir lassen derzeit durch unsere Rechtsanwälte alle möglichen Schritte prüfen, um Ihnen schnellstmöglich wieder einen unkomplizierten Zugang zur freien Enzyklopädie Wikipedia zu bieten. Bitte haben Sie dafür Verständnis, dass wir aus rechtlichen Gründen bis auf Weiteres keine weiteren Stellungnahmen in dieser Sache abgeben werden.

Wikimedia Deutschland – Gesellschaft zur Förderung Freien Wissens e.V.
Berlin, 18. Januar 2006

Wenn Sie uns mit einer Spende unterstützen möchten, können Sie diese auf unser Konto 32 87 300 bei der Bank für Sozialwirtschaft, Berlin (BLZ 100 205 00) überweisen. Weitere Informationen finden Sie unter http://www.wikimedia.de/spenden. Vielen Dank für Ihre Unterstützung.

Figure 7: Notification of the block on a page in Wikipedia.de after a restraining order.

4.3.4 Access control in Wikipedia

As we will argue more extensively below, providing users with possibilities for *access control* can contribute to solving *some* of the privacy issues in collaborative workspaces. Access control enables those who determine the rules to have control over who sees what information. In Wikipedia access control can be classified as a *group-based approach*. This means that users are assigned to certain groups, whose rights and privileges are described in detail in the Wikipedia User Group Rights[30].

[30] See http://en.wikipedia.org/wiki/Special:ListGroupRights [last accessed on 4 August 2008].

Stakeholders	*Right / Privilege*				
	Read content	**Create content**	**Edit content**	**Delete content**	**Manage access control**
Non-registered users [identifiable by IP address]	X	X[31]	X[32]	-	-
Registered users of Wikipedia	X	X	X[33]	(X)[34]	-
Wikipedia providers [incl. administrators and developers]	X	X	X	X	X

Table 4: Overview of access control rights for relevant stakeholders in Wikipedia.

In order to become a registered user, the user only has to choose a user name and password and register on the Wikipedia server. No proof of identity is needed. Becoming an administrator in the Wikipedia community is open to anyone, at least in the English version. Wikipedia says that administrator status can be granted to anyone "*who has been an active and regular Wikipedia contributor for at least a few months, and who is familiar with Wikipedia and respects Wikipedia policy, and who has gained the trust of the community*". Furthermore, "*administrators can protect and delete pages, block other editors, and undo these actions as well.* [...] *Adminship is granted indefinitely, and is only removed upon request or under circumstances involving high-level intervention* […]. *Administrators undertake additional responsibilities on a voluntary basis, and are not employees of the Wikimedia Foundation*"[35]. Hence, the grant of enhanced privileges is based on a combination of reputation (duration of membership, number of edited pages) and a form of trust, which is not specified more precisely.

Table 4 provides an overview of access rights on pages in Wikipedia, considering the three types of stakeholders from the privacy analysis. Looking at this table, an imbalance which leads to some of the privacy issues explained previously becomes evident. Registered and non-registered users are allowed to create and modify content (including personal data) of the online encyclopaedia. However, they have no rights to control access to these data. The management of access control is exclusively reserved for Wikipedia providers.

[31] In order to create new content (for instance to add a new lemma), some Wikipedia editions, such as the English and the Dutch one, require a user registration; others, such as the German edition allow everybody to create new pages, with or without a user account.
[32] Except for a limited number of special pages, such as the Wikipedia main page.
[33] See the previous footnote.
[34] The 'deleted' content will still be available in the history of the wiki page.
[35] See https://secure.wikimedia.org/wikipedia/en/wiki/Wikipedia:ADMIN [last accessed on 4 December 2008].

4.4 Example 2: phpBB.de

PhpBB.de (http://www.phpbb.de/community) is the German support platform for the open source software phpBB and, at the same time, provides an application example of the phpBB forum software (http://www.phpbb.org). It is also the second example of collaborative workspaces that we investigate with respect to privacy issues in this deliverable.

When providers hosts their own phpBB forum, a number of the configurations can be set differently than is the case in phpBB.de. Moreover, forum providers can install so-called 'mods' (short for: modifications). Mods are small php programs that are installed together with the original phpBB forum software and that allow for more – privacy-friendly or privacy-intrusive – features. In the implementation under evaluation, forum users engage in discussions on the software. For instance, they ask for help when they have problems with their own forum installation, or share that fact that they have found a new mod. Each person who knows the URL www.phpBB.de/community or who finds it by accident via a search engine is allowed to read the content of the forum. Registration is only required in order to ask questions or to take part in discussions actively. In August 2008, phpBB.de had about 70,000 registered forum members, according to the website. Figure 8 shows the opening page of the forum.

Figure 8: The opening page of phpBB.de (2008).

In this section we provide an overview of privacy protection goals from the perspective of registered forum members. As with the previous example, we will show that these goals can come under attack from one of three directions: (1) third parties, (2) other members of the same forum, and (3) the providers of phpBB. In the case of phpBB.de these three parties take the following form:

- *Third parties*: The adversary has no phpBB.de account or any other special privileges;
- *Forum members*: The attacker has an account on phpBB.de, that is, he or she has a registered username and password. He or she can create postings and send and receive private messages;

- *phpBB.de providers* (including administrators, moderators, etc.): The adversary has special privileges, for instance enhanced access to user profiles, and therefore he is the strongest attacker out of the three.

4.4.1 Privacy issues caused by third parties in phpBB.de

In this section we will discuss a number of privacy issues that may be caused by third parties, i.e. non-registered users of the forum. In our description we follow the same strategy that we used when discussing Wikipedia: we will use Table 3 as our starting point, and discuss whether the privacy protection goals are met in phpBB.de.

 # 1. Confidentiality

Every registered user of phpBB.de has a user profile, which contains at least a username, a date of registration and the total number of postings of this registered user. Since the user profile is available to anyone on the web, it is impossible to keep the contained data confidential. This means that the privacy protection goal of confidentiality of personal data is not met in phpBB.de with respect to third parties. Figure 9 shows an example of a publicly available user profile.

→ This issue applies to fields (1), (2), (3), (4), (5) and (6) of Table 2.

Figure 9: An example of a user profile from phpBB.de.

A second issue with respect to confidentiality in phpBB.de revolves around the fact that all contributions to the forum are available to the public. Some of the posts contain personal data of the author and/or other people, e.g., in a thread where forum members organise a real world meeting they disclose time and location for their meeting to the public. Since all contributions are visible to the public these sensitive information are not protected and this is a second way in which phpBB does not meet the privacy protection goal of confidentiality with respect to third parties.

→ This issue applies to fields (1), (2), (3) and (4) of Table 2.

 # 2. Anonymity

Since posted content and member profiles are available to the public, third parties know all the facts that the profile owner discloses in the profile and in his/her contributions to the forum. Third parties can keep track of all contributions of the respective forum member over a longer period in time and thus also learn about forum usage patterns and about the personal interests of this user. Especially when links to personal web pages, social network site profiles or pictures of the user are posted, this may be enough information to identify a forum user even without being a member of the forum. Thus, the anonymity of forum members can be compromised when they disclose (too much) information related to themselves.

→ This issue applies to fields (1), (2), (3) and (4) of Table 2.

 # 3. Unobservability

In Table 3 we state that the protection goal 'unobservability' is met, if nobody except the legitimate users of the workspace can notice the actions in this workspace. The question here is, who are the legitimate users of a forum thread? If the answer is 'the public in general', then there is no privacy issue with regard to unobservability. However, if some contributors to the forum only have other forum members (and perhaps the provider) in mind when creating a post, then it could be argued that third parties are not legitimate forum users. Nevertheless, they can see when an author has written a contribution and from this point of view the goal 'unobservability' is not met.

→ This issue applies to fields (1), (2), (3) and (4) of Table 2.

 # 4. Unlinkability

As we have seen in Table 3 'unlinkability' revolves around the idea that when a user posts or contributes to several different items of content, these items cannot be linked, which prevents third parties from creating a profile of the users based on his interests and contributions. In phpBB.de the user profiles enable viewers to see all of the entries from a single user. Therefore, it is in fact possible for third parties to build up a profile based on the topics to which he or she contributed. Thus, the privacy protection goal of unlinkability is not met in phpBB.de with respect to third parties. Moreover, information about the user's status in the phpBB.de community can be gained from a feature that lists all users of the forum according to their membership in one or more groups.

→ This issue applies to fields (1), (2), (3) and (4) of Table 2.

 # 5. Integrity and # 6. Accountability

There are no features available in phpBB.de that would allow third parties to compromise the privacy protection goal of 'integrity' or of 'accountability'.

 # 7. Availability

Malicious third parties may be able to perform a 'Denial-of-Service'-attack on phpBB.de, for instance by flooding the server with too much traffic. Just as with Wikipedia above, the result would be that phpBB.de would be temporarily or indefinitely unavailable. This affects the privacy of authors, since they would not be able to control their personal data stored on the phpBB.de server.

→ This issue applies to fields (1), (2), (3) and (4) of Table 2.

 # 8. Legal enforceability and # 9. Authenticity

There are no features available in phpBB.de that would allow third parties to compromise the privacy protection goals of 'legal enforceability' and 'authenticity'.

4.4.2 Privacy issues caused by other forum members in phpBB.de

Registered users of the forum are able to cause the same issues as third parties as we have sketched these in the previous section. They, too, may glean personal data through the public visibility of all contributions to the forum and may derive information about other users through the links between content that is added by these users. An additional problem that may occur due to malicious intentions from registered user is explained below.

 # 1. Confidentiality

In addition to the confidentiality issues that may be caused by third parties, forum members have the option to exchange private messages with other forum members, for instance in order to ask them questions which they would not discuss in front of the public and all other members in the forum. If a user decides to copy the text of a private message from another user into a public forum thread or even somewhere else outside the forum, this would compromise the other user's privacy. Note that, in order to send and receive private messages, a user account is needed, but the owner of the account does not need to be an author in the sense that he has created at least one forum post.

Furthermore, forum users can post personal data of others, e.g., teachers, neighbours, politicians, celebrities, etc.

→ This issue applies to fields (1), (2), (3) and (4) of Table 2.

 # 2. Anonymity

In addition to the options that third parties have to identify a forum user, members of the forum can use private messages to pro-actively ask other users for information, including personal data. Therefore, forum members have enhanced options to compromise other members' anonymity and they can also post their de-anonymizing information in the forum. However, hopefully only highly privacy-unaware or very trusting users would fall victim to these kinds of adversaries, since otherwise they would steer clear of answering private questions.

→ This issue applies to fields (1), (2), (3) and (4) of Table 2.

 # 3. Unobservability and # 4. Unlinkability

phpBB.de members can cause the same privacy issues with regard to the privacy protection goals of 'unobservability' and 'unlinkability' as third parties.

 # 5. Integrity

The privacy protection goal of integrity refers to the fact that nobody can modify content or circumstances of disclosure retrospectively, or that everybody can notice such a modification. However, since forum members can modify their own profile at any time without a notice for other users (e.g., modification time, version number) that this profile has been changed, the goal of 'integrity' is not met in this case. Moreover, if users modify their own posting after they have published it to the forum, and no other user has posted in the meantime, there is no hint that the post was modified since its first publishing either. This means that if Inez has read a post in its first version and Florence reads it in the second version, they do not immediately realise that they did not read exactly the same text.

→ This issue applies to fields (3), (4), (5) and (6) of Table 2.

 # 6. Accountability

If a forum member always uses an anonymisation service (such as TOR or Anon) – that is, for the first registration and all other activities in the forum – then it would be practically impossible to allocate his/her contributions and actions (e.g., harassment of other users) to a real person. Hence, the protection goal of accountability can be compromised.

→ This issue applies to fields (3) and (4) of Table 2.

 # 7. Availability

phpBB.de members can delete their posts retrospectively and thus limit the availability of the original contribution. However, there are significant limitations to deleting one's own past posts. Users cannot delete copies of their post, and these may very well exist, since other users may have quoted the original contribution, for instance when replying to it.

→ This issue applies to fields (3) and (4) of Table 2.

 # 8. Legal enforceability

Related to the issue described above under # 6 in this section, a forum member that has posted, for instance, personal but false details about others, or who has stalked other forum members, cannot be held legally responsible for his/her posts and actions if he/she cannot be identified.

→ This issue applies to fields (3), (4), (5), (6), (7) and (8) of Table 2.

 # 9. Authenticity

When someone registers to become a member of phpBB.de he/she only needs to provide a unique user name, a password and a valid e-mail address. No proof of identity is required. This enables users to build up a user profile, including a name, an address and a picture while pretending to be someone they are not. With such a fake profile other users (e.g. colleagues of the simulated person) can be contacted and asked to provide sensitive or personal data. Furthermore, forum members can post any content they want, including manipulated photos or false information about third persons who are or are not members of the forum themselves. Hence, the privacy protection goal of 'authenticity' is not met in phpBB.de.

→ This issue applies to fields (3), (4), (5), (6), (7) and (8) of Table 2.

4.4.3 Privacy issues caused by the phpBB.de providers

Providers, administrators and moderators all have enhanced privileges. Hence, in addition to the attacks already stated in the previous sections, they can cause further privacy issues.

 # 1. Confidentiality

Since participation in the phpBB.de forum requires registration with a valid e-mail address, providers always have access to users' e-mail addresses[36], even if the user has marked it as private in his/her profile.

→ This issue applies to field (4) of Table 2.

 # 2. Anonymity

Providers always see the IP addresses of authors and the exact time when a contribution was made (Figure 10). In cooperation with the Internet Service Provider (ISP) this enables providers to reveal a forum member's real identity and thus, the protection goal 'anonymity' is not met.

→ This issue applies to field (4) of Table 2.

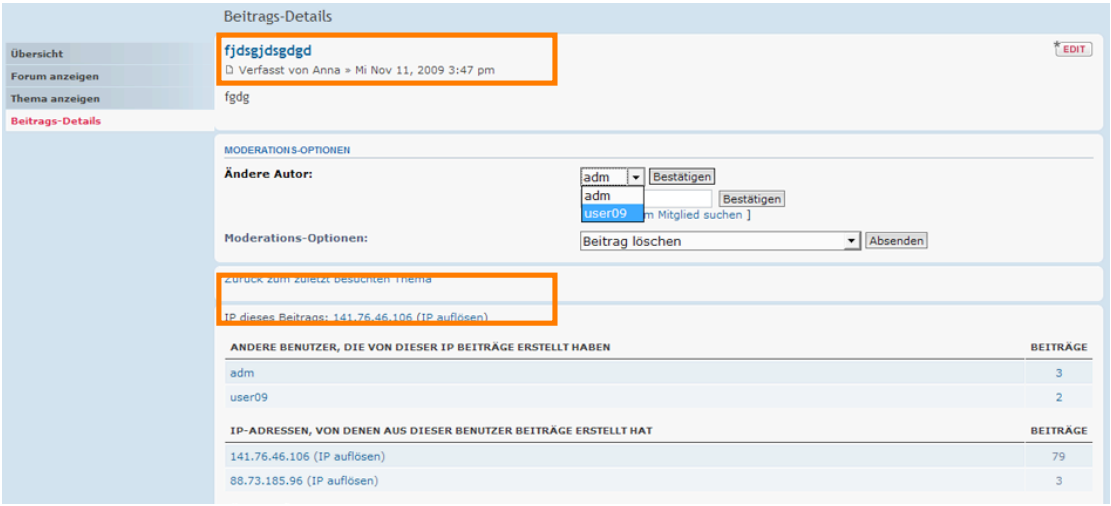


Figure 10: The phpBB.de provider's view, showing the user name, time, and IP address.

 # 3. Unobservability

phpBB.de providers can cause the same privacy issues with regard to the privacy protection goal of 'unobservability' as forum users.

[36] Note that users can protect themselves from this access by giving the provider a bucket address, for instance created at www.spam.la.

4. Unlinkability

When visiting phpBB.de, cookies are stored on the visitors' computer. Cookies are small text files that can be used to improve the usability of the forum by storing which post the user has already read and which ones are new. According to phpBB.de two of the cookies contain a unique user-ID[37]. This means that the cookies can also be used to re-identify a visitor and thus link different actions of the user and create a profile.

→ This issue applies to field (4) and (6) of Table 2.

Moreover, forum providers can see a list of all IP addresses that an author has used in phpBB.de so far (Figure 11). This means that these IP addresses are linked to the same user. With the help of geo-location information providers are able to build up a profile of the individual's movements, for instance to see whether the user always stays in the same region or whether he/she travels around the world and writes contributions from different countries.

→ This issue applies to field (4) of Table 2.

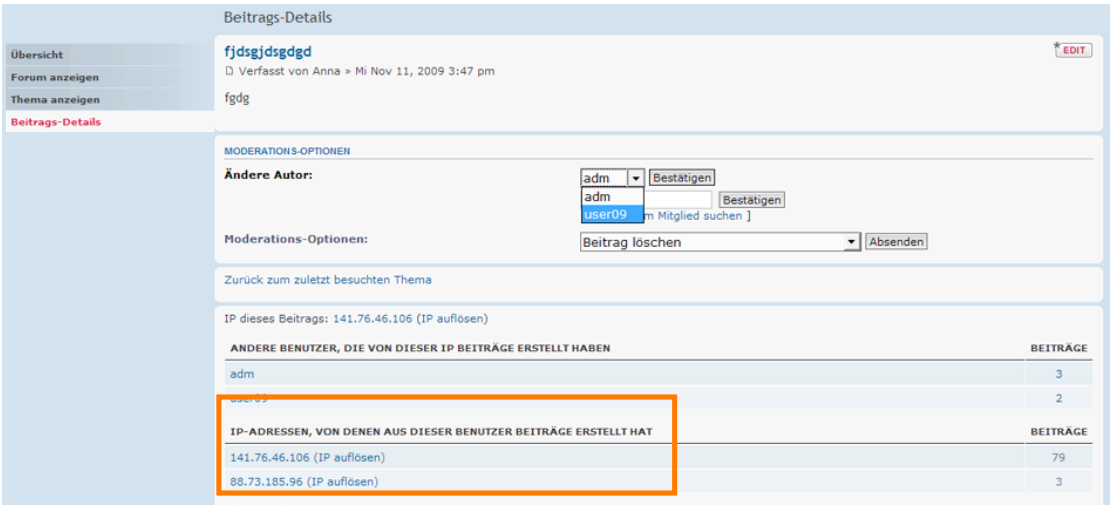


Figure 11: The phpBB.de provider's view showing a list of all the IP addresses of the same user.

5. Integrity

Forum providers can use a special administrative feature to change the author of a post by selecting one of the other registered users from a drop down list (Figure 12). This modification will not be indicated in the post, which means that readers cannot notice it. Hence, this feature compromises the protection goal of 'integrity'.

→ This issue applies to field (4) of Table 2.

[37] See: https://www.phpbb.de/community/ucp.php?mode=privacy [last accessed on 19 February 2010].

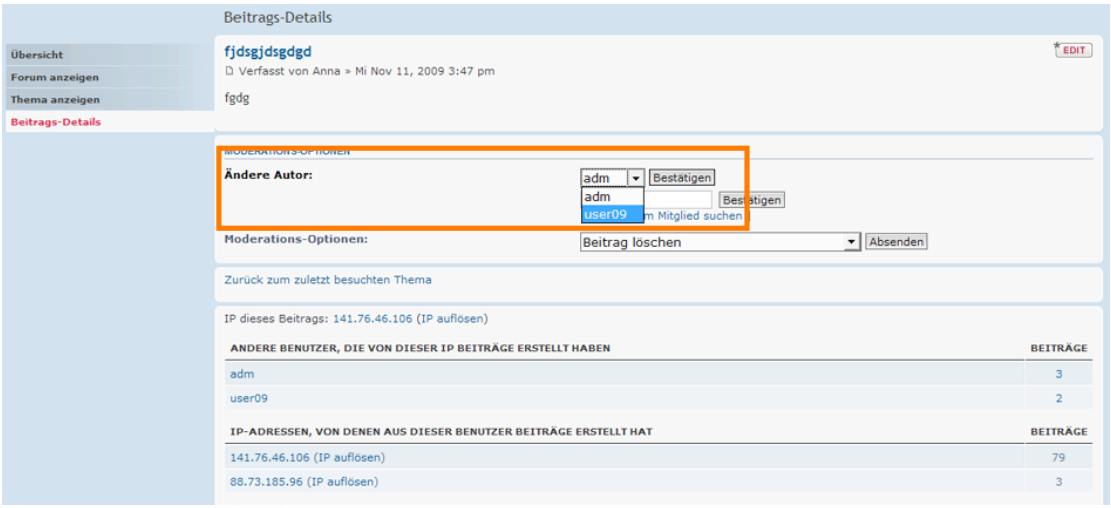


Figure 12: The phpBb.de provider's view showing the feature for changing the author of a post.

6. Accountability

The feature that allows forum providers to change the author of a post can also be used to compromise users' 'accountability', since it is easily possible to assign posts to users who are actually not responsible for them.

→ This issue applies to field (4) of Table 2.

7. Availability

The phpBB.de providers can shut down the whole forum at any time and thus block the availability of all posts, private messages and member profiles. Besides, the provider can also delete single posts or threads. Thus, the privacy protection goal of availability is not met in phpBB.de.

→ This issue applies to field (4) and (6) of Table 2.

8. Legal enforceability

If a forum user has posted very personal, yet false, details about another person, public authorities may want to know the IP address of the author (in order to find out his/her real identity), so that they may investigate the legal consequences of this action. In such a case, the privacy protection goals of 'legal enforceability' may not may feasible, if the forum provider refuses to cooperate by giving the IP address in question to the public authorities. This could be the case, for instance, because the provider has deleted the whole post including the IP address.

→ This issue applies to field (4), (6) and (8) of Table 2.

9. Authenticity

The privacy protection goal of 'authenticity' is not met in phpBB.de since forum providers can change the author of a contribution and then make readers believe that this post was written by someone other than the original author.

→ This issue applies to field (4) of Table 2.

4.4.4 Access control in phpBB.de

Access control in phpBB.de is realised in a *group-based approach*, which means that users are assigned to groups, and privileges are granted to these groups and not to users on an individual basis. Table 5 shows the access rights to forum postings and profiles for all three of the parties introduced in the privacy analysis of this forum.

	Right / Privilege						
Stakeholders	**Read postings**	**Create postings**	**Edit postings**	**Read profiles**	**Create profiles**	**Edit profiles**	**Manage Access Control**
Non-registered users	X	-	-	X	X	-	-
Forum members of phpBB	X	X	X[38]	X	X	X[39]	-
phpBB providers [incl. administrators and moderators]	X	X	X	X	X	X	X

Table 5: Access control for the three parties in phpBB.de.

To become a registered forum member of phpBB.de users need (at least) a username, a password and a valid e-mail address. However, they do not need to provide a proof-of-identity. On the phpBB.de website no explanation was found on how someone could become a moderator or administrator. We assume the procedure resembles that of Wikipedia, which we have described previously, that is that users who have been registered members for a certain time and have gained a reputation and some level of trust from the phpBB.de community can volunteer for such roles with enhanced privileges.

4.5 Contradicting privacy protection goals

In the first part of this chapter we have looked at the privacy issues and privacy protection goals as these evolve around two selected collaborative workspaces: Wikipedia and phpBB.de forum. We have seen that there are a number of ways in which the privacy of individuals can be threatened, and also that privacy threats may come from different directions, that is from third parties, from other users, and from the providers of these environments. Both examples demonstrate that there are opportunities for adversaries to spy out interests and build up profiles of authors in collaborative workspaces. However, some privacy issues are not a result of malicious intentions,

[38] Registered users may only edit their own postings.
[39] Registered users may only edit their own profiles.

but simply occur due to different but reasonable interests of the various parties involved in collaborative workspaces. Throughout the analysis of privacy issues in collaborative workspaces we have focused on explaining how the privacy of a single user may be compromised by third parties, other users and providers. In reality, not only the interests of this user need to be considered, but so do the interests of other users, or the interests of providers of the systems. In other words, in collaborative workspaces multiple perspectives on privacy goals and how these should best be served exist. In this section we discuss and illustrate contradictory protection goals in the relationship between users and providers first, and between one user and another second.

4.5.1 The users' interest versus the provider's responsibility

The *providers* of collaborative workspaces – that is, both the providers of hardware, and the developers, administrators, moderators, etc. who manage these workspaces – also have requirements related to personal data and the privacy of users.

As we have argued several times in this chapter the storage of IP addresses by the providers of collaborative workspaces can be labelled a privacy hazard for individual users, since it makes them identifiable with the help of the Internet Service Provider (ISP). On the other hand, however, providers are responsible for the enforcement of legal and social rules in collaborative workspaces, which means, for instance, that they must be able to identify users who publish unlawful content. This is why it is in the provider's interest to know and store the IP addresses of all users. Another aspect of the provider's responsibility that is relevant in this context is the fact that the provider stores personally identifiable information from citizens. Therefore, it has to comply with all the relevant legislation concerning how this data is to be treated. This may for instance force the provider to invest in an encryption/security infrastructure.

4.5.2 The users' interest versus that of other users

It is in the users' interest to protect their personal data by starting from maximum privacy when working in collaborative workspaces. This means that they do not want to disclose any personal or possibly identifying information. However, other users who may want to collaborate with them are interested to know what experiences and skills they have, or how they can be contacted and recognised in future collaborative working sessions, which means that the other users need some personal data about them.

Another interesting point is that users of collaborative workspaces post content not only about their own person, but that they may also disclose information about other natural persons – with or without these others' knowledge. As we have explained above, examples of such content are Wikipedia pages on celebrities or other well-known individuals, but also include discussions in forums about a natural person, or movie clips posted in file-sharing sites that contain images of a natural person. Since this information is about natural persons the collective creation of such content affects these subjects' privacy and may also have consequences for their reputation. We have seen an extreme example of this in the previous chapter, where we described the incident surrounding the 'dog poop girl'. Her name, personal information and picture travelled around the globe as a result of a single devastating blog post about her behaviour on a subway train in South Korea. The story of the 'dog poop girl' was spread via a blog posting. As we have argued in Chapter 2 weblogs can be considered collaborative workspaces, in the sense that they allow users to share their ideas, and facilitate readers with the option to comment, thus enabling discussion between the owner of the weblog and its audience. However, weblogs lack one of the important

characteristics of certain other types of collaborative workspaces: their goal of providing a forum for the creation of content that has a high degree of *objectivity*. For many wikis and some forums[40] this is, in fact, one of the implicit or even explicit goals. An online encyclopaedia such as Wikipedia couldn't have its current success if its readers and its contributors believed that the content that was created, edited, and stored there had a high level of accuracy, a significant truth-value, and hence could be considered (at least in the case of most lemmas) quite sound and objective. While much debate has been going on in scientific circles over whether or not Wikipedia does or does not provide users with objective information, based on its gradually more widespread use by an ever-increasing amount of people (including its increasing references in scientific articles) we may conclude that in general the public at large, whether rightly or wrongly so, does in fact trust the truth-value and objectivity of content obtained from Wikipedia and regards it as a valid reference source. Allegedly, this objectivity stems from the many contributors that wikis have. The wisdom of many ensures that the information in these environments is not the result of a single individual's opinions or wild ideas, but rather the shared view on a single topic as composed and confirmed by a group of people. The editing and delete functionalities of, for instance, Wikipedia, ensure that quirky or outlandish perspectives on a topic are generally quickly adjusted to a more mainstream description. If no other users have contributed to a lemma in Wikipedia this is clearly stated at the top of the page, so that readers may build in some reservation with respect to its objectivity. Systems such as Wikipedia are thus deemed more objective and less opinionated than the average weblog, both by the contributors themselves and by the readers of these different types of collaborative workspaces. However, as the examples above suggest, when these objective wikis present information about natural persons, this may result in a clash of interests between, on the one hand, the objectively true (yet possibly damaging) information about a natural person presented in this wiki, and the right of this person to protect his or her privacy on the other. The case of the 'dog poop girl' was instructive in some respects – it reveals that managing and guarding one's reputation has become a precarious business in the world of web 2.0, in which anyone can easily share his/her ideas and opinions with a possibly worldwide audience.

What can we conclude when attempting to learn lessons from examples such as this? They show that when personal information about natural persons is revealed in collaborative workspaces by others this may have serious consequences for the persons to which the information refers[41]. How can we solve issues such as these? When individual A writes something about individual B in a forum or a wiki, there are two people concerned. First, individual B, since he or she is the subject of the contribution, and second individual A, since he or she has written this contribution. Therefore, the contribution reflects his or her opinion and wording. While there are definite mechanisms for protecting the privacy of individual A (the writer), unfortunately it is practically impossible to enforce privacy protection mechanisms for individual B, the person that is written about. Most of the time, B will not even know about the fact that A has written something about him and that his privacy is at risk. Moreover, resorting to technology to acquire such knowledge is not feasible either. One would need a very well elaborated text recognition algorithm that automatically identifies any contributions about oneself in forums, wikis, and other collaborative workspaces. When we think about the complexity of human language, it is not very surprising that such an algorithm is not available in practice. But assuming we had such an algorithm, then we would still need to discuss a reasonable balance between B's right to privacy, which entails editing or deleting the contribution, and A's freedom of opinion, which entails leaving the contribution

[40] In many forums, however, we find a wide variety of different and maybe extremely opposed opinions instead of objectively formulated information. However, it is the sum of the different opinions that allows the reader to create his or her own 'objective' view on the topic at hand.

[41] This is true of other media, such as newspapers and television as well, of course. One important difference with these media, however, is the degree of accessibility for creating and disseminating content in collaborative workspaces – anyone can participate and share information, hence anyone can write about other persons.

unchanged. Therefore, thorny examples such as the ones discussed in this section will undoubtedly return on a regular basis.

4.6 General requirements for enhanced privacy protection in collaborative workspaces

In the previous sections of this chapter we have described a number of privacy issues that may arise in collaborative workspaces. On the basis of these findings recommendations can be made with respect to the requirements that collaborative workspaces should meet for enhanced privacy protection. In this section we return to the privacy protection goals of Table 3 once again and from these goals we derive a set of requirements for privacy enhanced collaborative workspaces. These are combined into a single table, which is presented below. Some of the identified requirements cannot be fulfilled at the same time, which underlines the statement that privacy goals of different parties do not always match, but can even be contradictory.

Privacy protection goal:	Leads to:	Requirement:	Description:
1. Confidentiality	→	**a. Awareness of the 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 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 collaborative workspaces 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. *Therefore, collaborative workspaces should provide features for the awareness of users with respect to the potential audience of their contributions*.
	→	**b. Deciding who the potential audience is**	Even if users would be aware of the potential audience, in the current generation of collaborative workspaces available users have hardly any options to self-determine access to their contributions. Instead, it is for instance the moderator of a forum or of a certain topic who specifies the access policies. Thus, the only chance users have to control the audience of their postings is to *not* contribute to the collaborative content. This, however, is not desirable since user participation is essential in collaborative workspaces. *Therefore, collaborative workspaces should provide options for users to define access control rules to their user-generated content in a privacy-respecting way*.
	→	**c. Facilitating options for long-term control over personal data**	After users make a contribution to a collaborative workspace they can only make this contribution undone by deleting or editing it. The same applies to the personal information they may have (accidentally) shared there. While users generally have access to their previous posts, they cannot automatically remove or edit it after a certain amount of time (which in practice entails that most users do not look back to what they have posted in the past and never 'clean up'). However, some options are open to providers to

Privacy protection goal:	Leads to:	Requirement:	Description:
			facilitate the removal of at least some personal data, for instance through the use of time-stamps. *Collaborative workspaces should provide options for users to specify a time period after that their contribution is deleted or marked as outdated.*
2. Anonymity	→	**a. Anonymous participation**	In the current generation of collaborative workspaces anonymous participation is almost always impossible. As we have seen above, either users have to create a user account before they can contribute, or their IP addresses are stored. While this is an understandable practice from the perspective of the provider, who has to moderate the workspace and guard the content created on it, it can undermine users' freedom of expression, especially with respect to sensitive topics. While contributing entirely anonymously may invoke unwanted social behaviours (rudeness, untrue or insulting content), providers could differentiate between various levels of anonymity to overcome these issues. *Therefore, collaborative workspaces should provide options for some form of anonymous participation (for instance anonymous for the public but not for the provider).*
	→	**b. Awareness of the level of anonymity**	Not having to provide any proof of identity gives users the idea that they can contribute to collaborative workspaces in a completely anonymous way. Many of them don't know that providers or authorities are, in fact, able to identify them anyway, at least under special circumstances, for instance, when they are requested by law, or when asked to create anonymous profiles for marketing purposes. *Collaborative workspaces should strengthen the privacy-awareness of users by informing them about their actual level of privacy, for example by pointing out their identifiablity from the perspective of service providers.*
3. Unobservability	→	**a. Unobserved content creation**	Writing and editing content in collaborative workspaces is sometimes (Wikipedia) visible to others from the first draft version on. *However, users should be given the opportunity to work on their texts in private before*

Privacy protection goal:	Leads to:	Requirement:	Description:
			they can decide to publish them and let a selected audience access the contribution.
	→	**b. Unobserved reading**	Reading content is registered in some collaborative workspaces as well (e.g. Wikipedia). Especially with respect to sensitive topics this is not a desirable practice – readers should be able to read information about, for instance, a contested political regime or a sensitive topic in the personal sphere (religion, sexuality) without registration and/or visibility of their doing so. *Collaborative workspaces should enable facilities for the unobserved reading of certain items of content, deemed politically or socially sensitive.*
4. Unlinkability	→	**Protection against surveillance**	Many users tend to use the collaborative workspaces over a longer period in their life. Throughout their contributions they disclose personal thoughts, wishes, experiences and maybe 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 of 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 is even more serious when we realize 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. *Collaborative workspaces should provide features for creating, managing and deleting different partial identities in order to reduce linkability of all actions of the same user.*
5. Integrity	→	**Protection of integrity**	In order to protect the integrity of contents and the circumstances of creating them, *collaborative workspaces should log all retrospective changes of content or circumstances of creation, for instance in a history or log file.*

Privacy protection goal:	Leads to:	Requirement:	Description:
6. Accountability (or repudiation)	→	**Proper accountability**	As we have seen in the example of phpBB.de providers of some collaborative workspaces can retrospectively replace the name of the author of a contribution with another user name. This means that readers cannot be sure whether a contribution associated with a user name was really created by this user. *In order to guarantee proper accountability, a non-destroyable link between a contribution and its creator needs to be established (for instance through the use of digital signatures).*
7. Availability	→	**Regular backups and distributed storage**	To guarantee a high availability of collaborative workspaces, *regular backups should be made and copies of all resources should be stored on different physical servers*. Distributed storage of a number of copies improves availability. However, it may also lead to inconsistency problems, because all copies need to be kept up to date.
8. Legal enforceability	→	**a. Data retention and surveillance**	Storage of IP addresses and other data that may help to identify the users of collaborative workspaces helps to enhance legal enforceability. In addition, *having a central instance that checks the civil identity of all users of collaborative workspaces before giving them an account to one or more workspaces would ensure that in the case of a legal issue, the person responsible can be identified*. **Note: these actions would contradict in a serious way with ensuring the privacy protection goal of anonymity!**
	→	**b. Prevention of offending behaviour**	Since users regularly seem to feel they can participate in collaborative workspaces in a relatively anonymous fashion for socially unwanted behaviours such as spamming or harassing others and circulating improper content are a problem for these environments. Users are insufficiently aware of the fact that their actions and disclosures online can have legal consequences when harming others. *Collaborative workspaces should raise awareness of users with respect to the legal consequences of behaviour that does not comply with the rules of these environments*

Privacy protection goal:	Leads to:	Requirement:	Description:
			(with respect to data disclosure, interactional requirements and etiquette).
9. Authenticity	→	**a. Protection against 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, that is, to pretend to be someone else, in order to spy on other members of the forum either in public threads or via private messages. *Collaborative workspaces should provide a privacy-friendly solution to prevent the abuse of other's identities, for instance through the use of a trusted third party that certifies the identity of users*.
	→	**b. Removal of wrong and outdated data**	Once contributions are posted in collaborative workspaces they usually stay there for a very long time, regardless of the question whether they are true or still up-to-date. *Collaborative workspaces should provide options for users to remove wrong and outdated data.*

Table 6: Requirements for privacy enhanced collaborative workspaces.

4.7 Enhancing users' privacy through user-controlled and privacy-respecting access control

Table 6 lists a set of requirements, based on the privacy protection goals that we presented at the beginning of this chapter, which can contribute to creating more privacy-friendly collaborative workspaces. One basic mechanism that can be distilled from this list revolves around so-called' access control policies' that can be defined by the originator of the content. That is, we propose to enhance users' privacy in collaborative workspaces by offering user-controlled, privacy-respecting access control. User-generated content is essential for Wikipedia, phpBB.de and all the other collaborative workspaces on the internet, and may contain personal data in terms of personal information, expressions of ideas and feelings of the writer. Moreover, the *circumstances* of creating the content can also be considered to be personal data. In general, as pointed out by Adams (1999), it is important what is deemed sensitive or intimate in the perception of the individual rather than if it can be evaluated by third parties (e.g., lawyers, computer specialists). Moreover, as we have seen in Chapter 3, where we presented Nissenbaum's work on privacy as contextual integrity, what is deemed sensitive or intimate is contextual (see section 3.1.3), and hence it is important to enable the individual sharing the information to decide the level of intimacy or sensitivity contextually, and on a case-by-case level. Some of the privacy problems in collaborative workspaces evolve due to the imbalance between *who creates* the content and *who decides about access* to the content. As we have seen in the analysis, at the moment it is not the authors but the providers of the workspaces who specify access control settings to the users' contributions.

Before we present our detailed requirements on user-controlled, privacy-respecting access control in section 4.7.2, we give a brief overview about the state of the art regarding access control for social software in the next section.

4.7.1 Access control: State of the art

'Access control' is a term that designates the idea that an authority over a certain location (virtual or real) or over certain resources has the ability and the right to restrict access to that location or those resources. Basically, any kind of structural, architectural, technical, legal or social barrier installed by one or more persons to limit access to a specific area or set of means can be labelled as a form of access control. This means that installing a lock on the door to one's home is a form of access control, but so is developing property law that gives the owner rights over his property and who has access to it. There is a wide variety of technical examples of realising access control as well.

In general, before access to a restricted resource or location is granted, some kind of 'authentication-authorisation'-procedure is needed, which is based on some kind of 'authentication credential'. For example, bank users receive a bankcard and a PIN number, and the number acts as a credential whenever they use the card to buy a product. After typing in the PIN number the user's credentials are checked with reference to an access control list to see if it can be verified, and if this is the case the user can make his purchase. Credentials can be physical objects (a badge you show to the doorman to enter a building), pieces of knowledge (a PIN code or a social security number) or an input based on your physical body (iris scan detection, a fingerprint, or facial recognition). From these examples we can learn, that credentials may contain a lot of personal data (e.g., an ID card), but there are also credentials without any link to the personal data of the holder (e.g., PIN number).

The most common access control mechanisms used in social software are:

- *Access Matrix Mode* (Lampson, 1971). The 'access control matrix' is a table, which lists all the users of the system in rows and all the resources in columns. Each element of the table specifies the access rights that user U has on resource R. Reading the access control matrix column-by-column provides tuples of rights and user names for each resource, called access control lists (ACLs). Reading the table line-by-line results in a capability list (CL). It indicates what access rights each user is granted in relation to which resources;
- *Role-Based Access Control* (Sandhu *et al.*, 1996). 'Role-based access control' mechanisms are similar to ACLs, with this difference: user names are assigned to one or more roles and for each resource it is defined which role is allowed to perform which action.
- *Team-Based or Group-Based Access Control* (Thomas, 1997). For this approach, user names are grouped in teams or groups, e.g., according to their current context of work. Access rights to resources are assigned to these teams or groups, respectively.

A detailed comparison of advantages and disadvantages of these mechanisms with regard to their applicability in the area of social software can be found in (Franz *et al.*, 2006; Razavi and Iversion, 2007; Tolone *et al.*, 2005).

All of the mechanisms indicated above are based on the idea of the existence of an administrative party (such as a provider) who defines lists, roles, or groups and assigns the names of all users of the system to these lists, roles, or groups in order to enable the management of access to resources. Even if this management task would not depend on a single administrative party, but could be set by each user for her own contributions – as is suggested, for instance by Razavi and Iversion (2008) in their approach to social network sites – another problem remains. In order to assign a user name to a list, role, or group, it would still be necessary to know of the existence of the user name. This entails that the author of a contribution and the user who is to be granted access need to meet at least once – either in the physical world or virtually. However, in a public forum for instance, the author of a post is potentially looking for new contacts, which fulfil specified requirements, for instance that they live in the same city or are a member of the same fitness centre. In such cases the author is unable to specify the names of all other users who should have access to the contribution. Both requirements, namely (1) the existence of an administrative party who decides about access control settings and (2) that user names are known, are our strongest points of criticism and the reason why we do not consider the approaches introduced above as applicable for user-controlled and privacy-respecting access control in collaborative workspaces.

4.7.2 Detailed requirements for user-controlled and privacy-respecting access control in collaborative workspaces

Based on the analysis of existing access control mechanisms and their shortcomings with respect to their applicability for collaborative workspaces, we can compose the following list of requirements on *user-controlled* and *privacy-respecting* access control for collaborative workspaces.

- No administrative party, but *each user* should be able to define and modify access rules with respect to his/her contributions, that is, with respect to personal information, and the expression of personal ideas and feelings;
- Other individuals, who should or should not be able to access a user's (personal) data are not necessarily *known* by the user;
- These other individuals also have an interest to protect their own privacy;

- User-controlled and privacy-respecting access control can be applied to different levels of *content granularity* (for instance, to the entire forum, to a topic (or discussion) within the forum, to a thread within a topic, or to a single post).
- An administrator of the collaborative workspace should be able to address the technical issues of the platform, but should *not necessarily have access to content* data;
- Moderators should be able to moderate *particular workspaces*;
- The owner of a resource must always be able to have access to it.

User-controlled, privacy-respecting access control which fulfils these detailed requirements functions as a valid mechanism for privacy protection in collaborative workspaces for the individuals *contributing* to and *using* these environments. It contributes to meeting a number of the general requirements we have developed in the previous section (Table 6), viz.:

- # 1.a *awareness of the potential audience:* user-controlled, privacy-respecting access control gives users feedback about the audience of a resource;
- # 1.b *deciding who the potential audience is*: user-controlled, privacy-respecting access control enables users to decide who sees which information;
- # 2.a *anonymous participation*: user-controlled, privacy-respecting access control allows authors and readers of collaborative workspaces to participate without creating an account;
- # 4 *protection against surveillance*: user-controlled, privacy-respecting access control allows users to contribute under various different nick names.

Obviously, user-controlled and privacy-respecting access control cannot solve all privacy issues in collaborative workspaces. However, it makes a significant contribution to addressing some central privacy issues that we have identified throughout our analysis in this chapter without causing new privacy issues.

In this chapter we have systematically analysed two examples of collaborative workspaces, Wikipedia and phpBB.de, with respect to possible violations of a list of privacy goals from the perspective of *single user*s. Further, we also pointed that there are different parties who have a reasonable interest in users' personal data in collaborative workspaces, namely the providers, other users and third parties. Consequently, the list of general requirements for enhanced privacy in collaborative workspaces that we collected contains various privacy requirements that may not only be dissimilar, but at times even conflicting. Therefore, it is practically impossible to build a demonstrator for privacy-enabled communities that addresses all of these requirements.

In building our own demonstrator for privacy-enhancing collaborative workspaces, thus, we decided to concentrate on access control as one important mechanism for the confidentiality of (personal) data in such spaces. We argued that there is an imbalance between those who create the contents of collaborative workspaces (the users) and those who manage the access control settings (providers) at the moment und presented more detailed requirements for a user-controlled and privacy-respecting access control functionality in collaborative workspaces.

In the next chapter we will turn to the second focal web 2.0 technology of this deliverable: social network sites and analyze privacy issues as they (may) arise in these domains.

Chapter 5

Privacy in social network sites

In November of 2009 the Canadian Broadcasting Corporation CBC published the story of a Canadian woman called Natalie Blanchard, whose monthly sick leave payments had been terminated because the insurance company had checked her Facebook profile and concluded that she was fit to work. Blanchard had been on sick leave from her job for a year and a half because she was suffering a depression, but in pictures on her Facebook profile she was seen laughing with friends at parties and having a good time at the beach.[42] Manulife, the insurance company, confirmed that it had used Blanchard's Facebook page to investigate the validity of her ongoing claim for monthly payments, but defended itself by saying it would never decide to terminate payments based on that information alone. What makes the case interesting that Blanchard claims her Facebook profile is accessible only to contacts she has given viewing rights, which means that it should have been impossible for Manulife to access her pictures. If this is true, she may have a case against the insurance company and possibly also against Facebook itself for violating her privacy rights.

Privacy violations have been in the news on a regular basis with respect to the relatively recent phenomenon of social network sites (or SNSs for short). In this chapter, we will look into this phenomenon and attempt to answer the following questions: (a) what kinds of privacy issues arise in social network sites and how are these related to the medium-specific characteristics of these sites? And (b) which requirements are needed (technically, socially and legally) to aid in solving privacy issues in social network sites?

5.1 Privacy issues in social network sites: An introduction

Over the last decade social network sites have turned into a blossoming phenomenon for online self-presentation and relationship management. In 2008, two of the biggest social network sites worldwide, MySpace and Facebook, had over 100 million and over 80 million users respectively (Grimmelmann, 2008: 6). In early 2010, the number of Facebook users alone had risen to 350

[42] See http://www.cbc.ca/canada/montreal/story/2009/11/19/quebec-facebook-sick-leave-benefits.html [last accessed on 8 February 2010].

million[43]. One of the most fascinating (and extensively researched) aspects of this emerging field of self-presentation and relationship management is the fact that users put such detailed and personal information about themselves in their profiles (cf. Tufekci, 2008: 17-31; Young and Quan-Haase, 2009: 268). Acquisti and Gross write: "*…one cannot help but marvel at the nature, amount, and detail of the personal information some users provide, and ponder how informed this information sharing is*" (Acquisti and Gross, 2006).

In an article on the privacy risks for individuals using Facebook, Grimmelmann dryly points out: "*Facebook knows an immense amount about its users. A fully filled-out Facebook profile contains about 40 pieces of recognizably personal information, including name; birthday; political and religious views; online and offline contact information; sex, sexual preference and relationship status; favorite books, movies, and so on; educational and employment history; and, of course, picture*. [...] *Facebook then offers multiple tools for users to search out and add potential contacts.* [...] B*y the time you're done, Facebook has a reasonably comprehensive snapshot both of who you are and of who you know*" (Grimmelmann, 2008: 9). What's more, "[a]*ll of this personal information, plus a user's activities, are stored in essentially a huge database, where it can be analyzed, manipulated, systematized, formalized, classified and aggregated*" (Raynes-Goldie, 2010: 1). And when viewed from a European legal perspective on privacy, almost all of this information (details on sexuality, religion, politics etc.) is considered 'sensitive' and hence requires "*particular conditions and safeguards* […] *when processed*" (Edwards and Brown, 2009).

So what makes people behave this way? The most basic answer, of course, is that users become members of social network sites because they want to get in touch with others and share information about themselves with them. At the same time, though, individuals generally want to restrict the amount of data disclosed to the minimum level required for each specific connection. These two opposing desires, the desire to restrict data disclosure and the desire to build and maintain relationships (which always involves data disclosure) is also known as the '*privacy paradox*' (cf. Oomen and Leenes, 2008). This privacy paradox is unavoidable for anyone who wishes to participate in (online) social interaction and self-presentation.

Sharing information and disclosing personal information is an inherent aspect of participating in social network sites, then. However, it appears that in practice individuals disclose more information than they intend to (Norberg *et al.*, 2007). Why does this happen? Why do users choose to provide such detailed – and true – personal information on their social network site profile? Many explanations can be given. For one, users have a high degree of confidence in digital technologies and have quickly become so familiar with them that they may lack the distance to see the possible downsides of using these technologies (Acquisti and Gross, 2006: 2). Second, some authors point out that the use of social network sites as such, and the degrees of self-exposure within them, must be understood as part of changing cultural trends with respect to social interaction and self-presentation (cf. Acquisti and Gross, 2006; Grimmelmann, 2008; Tufekci, 2008). Third, Grimmelmann points out people underestimate the risks involved in presenting detailed and personal information online.

This misunderstanding takes a number of forms. For one thing, users are often unaware of who has access to their personal profile and to the content they place online, because the architecture and design of social network sites is such that it provides individuals with a false sense of security and privacy. These sites "*systematically* [deliver] *them signals suggesting an intimate, confidential, and safe setting*" (Grimmelmann, 2008: 17), an environment that is private, "*closed to unwanted outsiders*" (Grimmelmann, 2008: 18). Users perceive social network sites as though

[43] See http://www.facebook.com/press/info.php?statistics [last accessed on 8 February 2010]. No reliable count of the number of MySpace users was available in early 2010.

they are a "*walled garden*" (Tufekci, 2008: 33), when in fact, as we will show below, in some respects they are far from that.

Moreover, users falsely believe that there is safety in numbers, in two senses of the expression. They believe that when everyone else around them massively starts using social network sites, these sites must be safe to use, because otherwise others would avoid them – a line of reasoning that obviously runs the risk of being flawed if everyone follows it –, and they believe the risks they run are very limited since there are so many members in social network sites that chances are really small that something bad will befall them as individuals (Grimmelmann, 2008: 17-18). But as danah boyd rightly argues this line of reasoning is flawed, especially for certain groups, such as teenagers. She writes: "[m]*ost people believe that security through obscurity will serve as a functional barrier online. For the most part, this is a reasonable assumption. Unless someone is of particular note or interest, why would anyone search for them? Unfortunately for teens, there are two groups who have a great deal of interest in them: those who hold power over them — parents, teachers, local government officials, etc. — and those who wish to prey on them — marketers and predators*" (boyd 2008: 133).

After this broad overview of the possible causes of privacy issues[44] as these may arise in social network sites we will now turn to a more detailed analysis of three possible *perspectives* with respect to privacy violations, each of which highlights different types of potential problems. We distinguish between the following perspectives: (1) the perspective of the *users* of social network sites; (2) the perspective of the *providers* of social network site; and (3) the perspective of *third parties*. In order to focus on relevant privacy issues related to the access to personal information in social network sites, we have used examples and issues presented in (empirical) scientific research by other researchers, and items that have recently appeared in the popular press. These highlight situations in which privacy intrusions of different kinds are documented, thus identifying situations and developments concerning social network sites where privacy is at stake and where potential improvements may be made. Technical developments and their potential privacy impacts are also considered.

5.2 The user's perspective

The first thing to consider when analyzing privacy issues from a user perspective is that information that individuals want to keep private, or only wish to share with a limited amount of people, should not spread further than they had originally intended. The most straightforward way to lose control over one's information is when one's user profile in a social network site is hacked. Although social network sites claim that the privacy of their users is their foremost concern, hacks are not unheard of, as Paris Hilton and Lindsay Lohan can confirm.[45] Obviously, the hacking of the MySpace profiles of these celebrities is a newsworthy item to many people, but it serves to underline the potential vulnerability of private information of ordinary users stored on social network sites as well.

Hacks are typically illegal means to gain access to private information, but there are many other concerns from the user perspective. They mainly stem from the plethora of information available on social network sites that is directly supplied by profile owners, which we have also mentioned above. Many users populate the attributes on their profile with a certain target audience in mind.

---

[44] An extensive overview of possible privacy risks can be found in PrimeLife Heartbeat 1.2.5, see http://www.primelife.eu/images/stories/deliverables/h1.2.5-requirements_selective_access_control-public.pdf

[45] See http://valleywag.gawker.com/5012543/paris-hilton-lindsay-lohan-private-pics-exposed-by-yahoo-hack [last accessed on 9 February 2010].

For example, a university student may use his Facebook account to boast about his partying capabilities by uploading a video of himself involved in (alcoholic) drinking games. A few years later, this action, which seemed a simple prank at the time, may come to haunt him when a potential future employer finds this very video when assessing his suitability for the responsible job for which he applies. Although the debate on whether online screening of job applicants is legal and/or ethical is still under way (cf. Davies and Lee, 2008; Johnson, 2007), the result for this particular young professional might be quite disastrous. For one, he might not get the job since the company may deem him unsuitable for such a responsible position. What's worse, chances are he will not be made aware of the reason why he was rejected which may lead to a repetition of the same mistake in the future. Another example that shows the real-world effects of social network site information spreading to other realms than those envisioned is that of Canadian politician Ray Lam, whose political career ended abruptly when photos of his Facebook account became public. In these pictures he grabbed a woman's breast and people were shown in their underwear.[46]

More and more institutions are using the abundance of information on social network sites to satisfy their informational needs. Examples are tax authorities that use a social network sites such as LinkedIn to check whether the professional activities a citizen lists on his tax form match those he listed on his profile page (cf. McDonagh, 2008), or announcements made by police forces in several countries to use social network sites to investigate (perceived) criminals and their online networks (Aleo-Carreira, 2009; BBC_News, 2009; Nederlands_Dagblad, 2008).

In general, users consider this type of infraction of their personal data an unintended but not insurmountable consequence of the use of social network sites. Research findings "*show little to no relationship between online privacy concerns and information disclosure on online social network sites*." (Tufekci, 2008: 1). Rather than restricting the amount of information within the profile, the visibility of the profile is adjusted, which, as we have argued above, does not protect users from information being copied and stored outside of the social network site.

Even when the visibility of the profile is adjusted, which appears to be the preferred coping strategy of most social network site users, risks are still looming. Third parties may actively try to gain access to private information through the network of trusted contacts. Friends or friends of friends may install applications within their profile that harvest data from the available network without the concerned user being aware.[47] While the Terms of Use of most social network sites state that this practice is illegal, and while it may damage the trust someone has placed in his or her online contacts, the fact remains that this is a viable possibility to lose one's personal information. This issue is all the more problematic in light of the fact that users are quite indiscriminate in whom they befriend, as we saw in section 2.4.2. In that section we saw that peer pressure and mechanisms on social compliance may move users to accept contact that they do not know (well enough), or even to accept anyone they do not "*actively dislike*" (boyd, cited in Gross and Acquisti, 2005: 73). When composing a list of contacts that is littered with individuals the user does not know well (if at all), he runs the risk that those contacts may harm his privacy through installing applications that harvest data from their network of friends. The potential for data loss through these means should not to be underrated, therefore.

What this description reveals is that a number of privacy issues may arise *for* users – and *between* users – in social network sites. Taking things to a more general level, one can categorize them into five groups: (1) users do not have enough of an overview of who their audience is; (2) users

---

[46] See http://www.cbc.ca/canada/bcvotes2009/story/2009/04/20/bc-election-lam-facebook.html [last accessed on 3 March 2010].

[47] See http://aclunc.org/news/press_releases/aclu_launches_facebook_privacy_quiz,_calls_for_stronger_privacy_defaults.shtml [last accessed on 3 March 2010] for more information about what can be harvested by applications on Facebook.

cannot show different sides of themselves to different audiences; (3) information persists online and hence can cause problems for users years down the line; (4) users can use social network sites to snoop on others, to gossip and spread negative information about others, thus damaging their reputation and possibly revealing personal information about those others; and (5) users do not have full (or even enough) control over their personal information. In some respects these issues overlap with themes we have encountered in previous chapters, when discussing social interaction in online worlds in general, and in collaborative workspaces in particular. However, in social network sites these themes come together in a particular way. We will discuss each of them in turn.

5.2.1 Who is the audience?

In social network sites, "*audiences are no longer circumscribed by physical space; they can be large, unknown and distant*" (Palen and Dourish, 2003). It is difficult for users to know who sees their information exactly. The audience, to phrase it differently, is not transparent. Partially this is caused by the structure of social network sites themselves. Currently, most social network sites provide limited options for making one's profile or the content contained in it (in)visible for specific others or specific collections of others. Generally, the options a user can choose from are limited to: (1) 'visible to everyone' (that is, all members of the social network site), (2) 'visible only to friends' (i.e. all of the user's contacts![48]), (3) 'visible only to friends and friends of friends', and in some cases (4) 'invisible to everyone'[49]. While some social network sites encourage users to change the visibility settings of information that is deemed intimate (such as their phone number or address) to 'visible to friends only', the default privacy settings are usually set to 'public', which means that individuals' profiles and the information contained therein can be viewed by anyone accessing the social network site. This means, Acquisti and Gross conclude, "*that the network is effectively an open community, and its data effectively public*" (Acquisti and Gross, 2006: 3).

Moreover, even if users do choose to protect their information using these four different options to differentiate between what audiences may see, the option 'visible to friends and friends of friends' is a tricky one. Users may think that when choosing this option their information is relatively protected, but disclosing information to friends of friends may extend the audience significantly without the users' (full) awareness. While the phrase 'friends of friends' appears to refer to a very limited audience, in fact some basic calculus reveals that it may easily consist of a significant group of people (that is, easily consisting of several hundreds of individuals), many of whom are probably unknown to the user[50].

But the lack of overview that users may have with respect to the audience that has access to their information is not just due to their unawareness, which is strengthened by these sites' architectural design. Another issue, which we will look into in detail below (sections 5.3 and 5.4) revolves around the fact that both the providers of social network sites and, in some cases, third parties gain

---

[48] See our critical remarks with regard to the use of the term 'friends' (rather than contacts) in section 2.4 of this deliverable.

[49] This applies, for instance, to one's e-mail address.

[50] If user A has 20 contacts in his contact list (which most people in social network sites easily have), and each of these have 20 contacts in their contact list, this means that when A makes a piece of information on his social network site accessible to his friends and their contacts 400 (20 x 20) users have access to this information. The average number of friends people have on Facebook is 130 (see http://www.facebook.com/press/info.php?statistics [last accessed on 1 March 2010]), which total the audience to 16.900 users (!) according to the math presented.

access to the information displayed on profile pages, thereby further complicating the users' grasp of who is watching the content he or she shares.

5.2.2 Context collision or the lack of audience segregation

Another key element of the fact that users do not have complete control over, or full awareness of who sees the information they post in a social network site is what Raynes-Goldie has called '*context collision*'. When she conducted research on the disclosure of information in Facebook, participants told her they were very frustrated by the fact that in this social network site (and in many others) all contacts are clustered into a single group, without distinction between the myriad of social relations and the various levels of intimacy one has with different contacts in real life. This leads to a "*flattened Friend hierarchy, where by default, everyone is given access to the same personal information. As a result a user's teetotaller boss sees the same things as their best friend, the party animal. This can cause problems when trying to decide what to share about yourself, or trying to manage how people from different life contexts might perceive* [information]. *What is appropriate for a user's friends to see may not be appropriate for their employer*" (Raynes-Goldie, 2010: 2).

Context collision entails that individuals are no longer able to meet the various behavioural requirements of the many different social settings in which they normally operate, since one and the same audience sees all of their behaviours. Whereas individuals can keep various social settings separate in real life, for instance because these social settings are connected to distinct physical places (work, home, public space, etc.), in virtual worlds such as social network sites "*intersections of multiple physical and virtual spaces, each with potentially differing behavioral requirements*" may arise (Palen and Dourish, 2003) (also see Meyrowitz, 1985, 2003, 2005).

Tufekci gives a very simple, yet illuminating example: "*…a person may act in a way that is appropriate at a friend's birthday party, but the photograph taken by someone with a cell phone camera and uploaded to MySpace is not appropriate for a job interview, nor is it necessarily representative of that person. Yet that picture and that job interview may now intersect*" (Tufekci, 2008: 22). That this issue may be a real problem for users becomes clear from an example presented by boyd and Heer, describing a dilemma that a 26-year old teacher from San Francisco encountered: "*She created her Profile when all of her Burner*[51] *friends joined the service. After a group of her students joined the service, they approached her to question her about her drug habits and her friendship with a pedophile. Although her Profile had no reference to drugs or even to Burning Man, many of her friends had both. Furthermore, one of her friends had crafted a Profile that contained an image of him in a Catholic schoolgirl uniform with Testimonials referencing his love of small girls. While his friends knew this to be a joke, the teacher's students did not. The teacher was faced with an impossible predicament. If she removed her Profile or disconnected to her friends, she admitted guilt. Yet, there was no change she could make to her Profile and it was inappropriate to ask her friends to change theirs. Although teachers keep strict physical distance from their students during off-hours, it may prove impossible to maintain a similar distance in online environments*" (boyd and Heer, 2006).

When phrased in the vocabulary of the twentieth century sociologist Erving Goffman, whose perspective on identity we discussed in Chapter 2, what users in social network sites lack are

[51] 'Burner' refers to the Burning Man Festival, an annual festival held in the Black Rock Desert in Nevada (USA), which "*is described by many participants as an experiment in community, radical self-expression, and radical self-reliance*", the Wikipedia lemma on the festival reads (see http://en.wikipedia.org/wiki/Burning_Man [last accessed on 8 Febraury 2010]). Burning Man is known to attract an audience of freethinkers, artists, political and social activitsts etc.

means for '*audience segregation*' (Goffman, 1959). As we have seen above, expressing and constructing identities, according to Goffman, revolves around the idea that whenever individuals engage in interactions with others, they *perform roles*. The goal of these performances is to present an image of themselves which is favourable. To Goffman, then, *impression management* is key in such self-presentations. As we have pointed out several times in previous chapters, each person performs a wide variety of roles in his everyday life, relating to both the places he or she visits, and the other people present there. The presentation of selves, then, is *situated* or *contextual* – it relates to *where* one is, and *who else is there* (cf. Meyrowitz, 1985, 2005; Van den Berg, 2008a, 2008b, 2009).

Audience segregation revolves around the idea that when enacting various – possibly conflicting – roles in their everyday lives, individuals need to keep the different audiences that see each of their role-performances separate, "*…so that the individuals who witness* [them] *in one of* [their] *roles will not be the individuals who witness* [them] *in another of* [their] *roles*" (Goffman, 1959: 137). With segregated audiences for the presentation of specific roles performers can 'maintain face' before each of these audiences. Their image will not be contaminated by information from other roles performed in other situations before other audiences, particularly not by information that may *discredit* a convincing performance in the current situation (Goffman, 1959: 137)[52].

Context collision and context collapse in social network sites are caused by users' lack of means for audience segregation. When the audience consists of individuals from many different contexts of an individuals' life, brought together in one group to view all of the individuals' behaviours in a social network site, then it is clear that this diminishes the individuals' chances of protecting and maintaining his various 'faces'. Moreover, it may lead to minor or more serious privacy risks.

5.2.3 The persistence of information for future audiences

As we have seen several times above, "*the recordability and subsequent persistence of information, especially that which was once ephemeral, means that audiences can exist not only in the present, but in the future as well*" (Palen and Dourish, 2003). This also applies to social network sites. Information posted on one's social network site profile may be accessed by (known and unknown) individuals in years to come. Moreover, since information can be copied, saved and stored easily and indefinitely, information placed on one's profile in a social network site at any particular moment may come back to haunt the individual years down the line. This means that the audience is not only unlimited in terms of its size and makeup (in contrast to audiences in the physical world), but also in terms of temporality. In the words of Tufekci, the temporal boundaries shift in such a way that "*the audience can now exist* in the future. […] *Not only are we deprived of audience management because of spatial boundaries, we also can no longer depend on simultaneity and temporal limits to manage our audiences*" (Tufekci, 2008: 22, emphasis in the original).

Since information and communication technologies and especially web 2.0 applications are relatively new, individuals still need to learn the consequences of their information sharing with

[52] One obvious question raised by this perspective is the fact that at times there is *overlap* between the audiences for whom we perform roles. When I invite my colleagues to dinner at home, for instance, and my family is present there as well, this means that my colleagues will see part of my 'private face', whereas my family members will see part of my 'work face'. In Goffman view, however, in a situation such as this one doesn't show a *mixture* of two existing and formerly separate faces, but rather a *different*, new kind of self-presentation. After all, when inviting colleagues into my home I apparently have reached a level of intimacy with them that will invite me to show more of myself than I would to colleagues and work partners who are not invited. This means, also, that when at work again the next day my 'work face' will have changed for that particular group as well.

respect to these facts. boyd and Heer write: "*Profiles, negotiating public/private boundaries, and dealing with digital architectural features such as replicability, searchability, and persistence suggest that people are still only learning how to interpret performative digital contexts to communicate meaningfully online*" (boyd and Heer, 2006). And safely, we would add.

5.2.4 Peer surveillance, snooping and gossiping

Once an individual has become a member of a social network site and has created a contact list, he can search for others' profile pages or navigate through them using his contact list. Depending on the visibility settings of each profile page, quite a significant amount of information about others may thus be gleaned. Navigating the profile pages of other users in this way possibly invites socially undesirable or even harmful behaviours. For one, gossiping and snooping are facilitated by it. As Hough points out "[t]*oday, technology enables us to gossip or otherwise exchange information with millions of people instantaneously.* […] *Social networking sites such as Facebook, reunion.com, and classmates.com enable the resurrection of those embarrassing youthful escapades and awkward photographs we all wish would stay buried. Often, the postings are captured on camera-enabled cellphones without the knowledge of the subjects and uploaded without their consent, leading to instant notoriety, long-lasting embarrassment, and a loss of reserve that may never be recaptured*" (Hough, 2009: 409).

Moreover, rules of etiquette that tend to dictate individuals to avoid information that can be considered embarrassing or harmful to others in real life do not apply in online worlds such as social network sites. Quite the opposite is true there: as we have seen in some of the examples described in this deliverable (for instance that of the 'dog poop girl' or of celebrities such as Paris Hilton and Lindsay Logan) users massively flock to information that is discrediting or harmful to these individuals. When there is a fight between two users, others warn their network to come and see the brawl. In real life there is a social norm of what Goffman has called '*civil inattention*' when encountering others in public spaces such as a train or a street. This means that individuals consciously withdraw their attention from others to leave them their space. Goffman describes civil inattention as "*withdrawing one's attention from* [other persons present in the same place] *so as to express that* [they do] *not constitute a target of special curiosity or design*" (Goffman, 1963: 84).[53] In social network sites this practice appears to be absent, at least for a significant number of users. The personal information, stories, pictures and interactional details of others are a source of interest to many.

This has led some researchers to conclude that social network sites are breeding grounds for surveillance between peers. For example, Adam Joinson writes that "*social networking sites like Facebook may* […] *serve a surveillance function, allowing users to 'track the actions, beliefs and interests of the larger groups to which they belong'* […]. *The surveillance and 'social search' functions of Facebook may, in part, explain why so many Facebook users leave their privacy settings relatively open* […]. *If 'social searching' is a public good, then reciprocity rules would dictate that by enabling a degree of surveillance of oneself, one* […] *should also be able to engage in reciprocal surveillance of others*" (Joinson, 2008: 2). Social network sites offer users a "*unique affordance* […] [to] *view other people's social networks and friends* […]. *This ability to find out more about one's acquaintances through their social networks forms another important surveillance function, and may also be a method for increasing the size of one's own social network*" (Joinson, 2008: 5). Peer surveillance, snooping and nosing around may all lead to privacy issues for the parties subjected to them.

---

[53] Granted, this behaviour was probably more common in Goffman's time (the late 1950s) than it is today.

5.2.5 Who controls a user's information?

In our description of social network sites in Chapter 2, we have explained that in these domains users can create a user profile on which they can present themselves and that also forms the starting point for setting up connections with other users within the same environment. On the profile page, users can choose what information to share about themselves and, to some extent, who can view this information (i.e. everyone, friends only etc.). Therefore, in theory at least, users have some control over the image they create of themselves on their profile page. As research has shown, especially young people perceive themselves to have a considerable degree of control over their disclosure of personal information online, and it turns out that they share such information in full awareness of the associated risks, because they have a high degree of confidence in their ability to manage potentially negative outcomes (Bryce and Klang, 2009: 3)

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

Moreover, as Bryce and Klang point out, users have control over what information they choose to share on their profile pages, but "*low control over the potential use of that information by others*. […] *...the commercial uses of personal information for data mining and targeted advertising as specified in Terms of Service policies can potentially infringe online privacy where access to, or understanding of these policies is absent or low*" (Bryce and Klang, 2009: 4). We will now turn to this issue in more detail when discussing the second angle: the provider's perspective.

5.3 The provider's perspective

The previous section focused on the user perspective of privacy in social network sites, be it the owner of a profile, a connection in his network, or a third person who has access to the public elements of the profile. Another perspective is offered when we consider the point of view of the provider. The provider has access to three types of information.

First, there is all the information that users store on their profile pages, ranging from personal information such as names, education or work history, to content such as uploaded photos or videos, to the connections the users establish with other users on the social network site. Thus, the information stored in the social network site can either be factual information about one single user, or information concerning the relationship between two or more social network site members. The latter can take the form of an established connection between the two, or of a piece of content in which two or more social network site users appear, such as a photograph or a posting.

In principle, users also have access to this information. However, the difference is that the provider can extract information from the system through technical means on a scale and with a frequency and efficiency that the user cannot. Moreover, the provider can add secondary data to the information supplied by users, such as time and date-stamps on social network site use, technical data concerning the connection with the social network site ('which webpage did the user visit prior to the login page of the social network site?'), and data on the IP address of the

computer the individual is using when accessing the social network site. The combination of the user-supplied information with these types of secondary data results in a far richer information profile than the user would initially expect, or is generally aware of, since this enriched data is not actively presented to him. Finally, the provider is able to store all changes that a user applies to his online information for an indefinite period. This could concern changes to his profile, the content he or she posts there, or the development of the number and type of connections over time.

The third type of information that providers can gather revolves around advanced data mining techniques, in which the entire pool of collected and enriched data of all collective members of the network is used as a starting-point for exploration. The opportunities for data mining objectives are only limited by the ingenuity of the provider. Some examples are:

- Create profiles for targeted advertisements based on keywords in user profiles and show these to both the users and their connections;
- Use the IP addresses of users' computers to establish relevant geographical groups for targeted advertising, perhaps in real time using online analytical processing (OLAP);
- Specific unwanted consequences of the access to information from the provider's perspective for the privacy of users of social network sites are hardly documented, since they take place within the confines of the organisation. However, it is clear that the raw material for substantial unexpected and unwanted privacy violations is readily available. A number of incidents have shown the impact unexpected use of personal information could have, one of which will be discussed below.

At the end of 2007, Facebook introduced so-called Beacon technology, which allowed the collection of data on activities a user performs on the web. By adding a few lines of code on any website, data on the interaction of the user with that particular site (for instance, buying a product, registering for a service or placing an item on a wish list) would be sent to Facebook. In turn, Facebook would make this data available to associated trusted third parties in order to come up with targeted advertising. These so-called 'social adverts' would build upon the social networks already established in Facebook: someone would be informed that their connection had acquired a certain product or service.

The Beacon technology contained a number of unpleasant surprises (cf. Chew *et al.*, 2008). First, the data was collected from users even when they were not logged into Facebook. In Facebook's Terms of Use, a user gives consent to this practice when establishing an account, but when confronted with the actual result, most users felt it to be too intrusive.[54] The cartoon below succinctly depicts their key objection.

[54] See for instance the cartoon at

Figure 13: A cartoon on Facebook's Beacon by Geek and Poke.[55]

Even when the particular account was not visited or updated for a longer period (for instance, half a year), Facebook still maintained the right to collect personal information during this period. Second, the targeted advertising was not only aimed at the user himself, but also at his Facebook connections as described above, who could infer the type of online activities one of their contacts had been engaged in. Finally, Facebook asserted that the user had a final say in whether the information collected on affiliated websites would be made available for advertising purposes. However, when a user opted out of the scheme during the visit of an affiliated website, this information would still be sent to Facebook. Although no advertising would be based upon that particular visit, nevertheless the information was collected and stored by Facebook.

After substantial outcry from privacy advocates, in December 2007 Facebook made changes to Beacon so that "*users had to explicitly 'opt in' to having their details published by the Beacon system*" (Edwards and Brown, 2009). Facebook's founder, Mark Zuckerberg said: "*If you select that you don't want to share some Beacon actions or if you turn off Beacon, then Facebook won't store those actions even when partners send them to Facebook.*"[56]

5.4 Third parties' perspective

In section 5.2 we discussed an example of the way in which third parties, both commercial and non-commercial ones, can access user data through network infiltrations. The focus of that particular example was on private user information that perpetrators were targeting. This section concentrates on social network site information at a higher aggregation level, that is, not only

[55] Source: http://geekandpoke.typepad.com/geekandpoke/images/2007/12/26/tw2007p4b.jpg [last accessed on 3 March 2010].
[56] See http://blog.facebook.com/blog.php?post=7584397130 [last accessed on 11 February 2010].

personal information pertaining to individual users, but information about their connections, thus leveraging the network information inherent in social network sites. For this purpose, third parties normally use automated processes or applications. A number of different application categories can be discerned.

5.4.1 Combining social network sites

The first category consists of applications that combine publicly available information in different social network sites by means of so-called 'mash-ups'. A mash-up is a web application that combines data from more than one source into a single integrated tool; an example is the use of cartographic data from Google Maps to add location information to real estate data, thereby creating a new and distinct web service that was not originally provided by either source.[57] The number of mash-ups with a particular focus on social network sites is on the rise. As social network sites proliferate, a growing need has emerged for information sources to be combined into one concise presentation. Examples include http://wieowie.nl/, http://www.yasni.de/ and http://www.wyczajka.pl.[58] All these sites tap into different social networks and search sites and present the information in one location.

The mash-ups described above present personal information from social network sites in a new setting, but the site itself is just a presentation platform on which interested people can get a combined view of available information about a specific person. The same type of solution is offered by a site like http://friendfeed.com/, which allows users to bring all their social network environments together in one location. It enables the user to present all his online expressions (e.g. Twitter, blogs, Flickr, last.fm) in one place. A key difference to the first type of mash-up presented is that the user is actively involved in publicizing all information, in which he also is able to disclose information that previously was only available to his online connections in each separate network.

Until recently, the technology to connect different social network sites had to be developed separately for each social network site. This changed with Google's introduction of the so-called 'Social Graph API' in February 2008. API stands for Application Programming Interface, which is a collection of definitions on the basis of which a computer program can communicate with another program. It can be viewed as an interface description between two pieces of software[59]. The Social Graph API enables website developers to incorporate social network information in their sites. When a user signs up at a new site or to a new service, the developer can use this API to show the user with whom he is already connected on another site. These connections can be added to the new site, thereby easing the burden on users who can move the social network they already established in one particular social network site to a new social network site without having to build a new network from scratch (Gijzemijter, 2008). Also, the Social Graph API is attractive to website developers because they get an easy means to give their sites a social dimension, thus generating traffic and critical mass.

To further clarify the potential of the Social Graph API, consider the difference with a feature that many social network sites already incorporate: the address book import. When registering at a new social network site, one of the first tasks a new user can perform is populating his network with friends. To ease the burden of checking the presence of friends in this social network environment,

---

[57] See http://en.wikipedia.org/wiki/Mashup_(web_application_hybrid) [last accessed on 11 February 2010].
[58] All sites on this page: last accessed on 11 February 2010.
[59] See http://www.pcmag.com/encyclopedia_term/0,2542,t=API&i=37856,00.asp [last accessed on 12 February 2010].

the sites almost invariably offer a tool to check whether people listed in an existing address book (for instance in MS Outlook (offline) or Yahoo! Mail (online)) are already a member of that particular social network site. The result of the address book import is that the user is presented with a complete inventory of all acquaintances that already have an account, based on corresponding e-mail addresses. The entire batch can be sent an invitation to establish a connection within the realms of the social network site, thus building an extensive network within minutes.

Whereas the tool described above uses an address book as a data source, the Social Graph API uses the entire social network of a user as a source for new connections. Through this mechanism, all existing connections of the user in all social networks to which he is associated become instantly available in each new social network site he joins, as long as that particular social network site uses Google's Social Graph API.

In principle, the API respects the privacy of individual users. The API returns web addresses of public pages and publicly declared connections between them. The API cannot access non-public information, such as private profile pages or websites accessible to a limited group of friends.[60] However, a potential problem arises when users have carefully constructed a number of different contexts for their online personality, in an attempt at recreating the practice of audience segregation, which we've discussed above, in online worlds. For instance, when a user has a professional profile in LinkedIn and a leisure profile on MySpace, both the mash-up technology and solutions like the Social Graph API suddenly combine these contexts into one. This may not be the user's intention, nor be in his or her best interest, although – as mentioned – Google specifically states that only publicly available information is accessible for the Social Graph API.

5.4.2 Using information in social network sites

In the previous section, the key issue under review was the migration or combination of all of the 'social' information of individual users, that is all the information relating to their connections in a social network site. This information, as we have seen, was embedded into or even transferred to a new environment, be it an external website or even a new social network site. But there are other means to employ information stored in social network sites in new settings as well.

OpenSocial[61], another Google initiative, permits website owners to include code on their pages which allows visitors to share the activities they perform on that particular site with their social network connections. This is interesting for website owners, since they make their site more attractive for visitors and create viral attention for the site. It can also be interesting to website visitors, since it becomes easy to share newly found websites with friends. And for application or widget developers it is interesting as well, since popular widgets will be used by many websites. OpenSocial can be considered as a tool that can be utilised to offer social network features to formerly more static websites. It is crucial, however, that the user himself decides which connections from his social network he wants to introduce to a new service: OpenSocial itself just offers the building blocks for such types of interaction. It is therefore less intrusive if it comes to combining different social contexts automatically; the applications in this category are more transparent to the user in their approach and consequences.

One last initiative that needs to be mentioned in this category is dataportability.org[62], which is also designed to share and combine information from different contexts. The idea behind

[60] See http://code.google.com/apis/socialgraph/ [last accessed on 12 February 2010].
[61] See http://code.google.com/apis/opensocial/ [last accessed on 12 February 2010].
[62] See http://www.dataportability.org/ [last accessed on 12 February 2010].

dataportability.org is that the user carries his or her context along to new web environments, which would save the user the trouble of building up a new profile at every new site you register with. The drawback is that the website that you sign up to will immediately have a full-fledged background on you, with information of your latest internet purchases at Amazon (if Amazon supports dataportability.org), or your music taste (if last.fm were to join as well). Dataportability.org is not so much an social network site feature, but an effort by a group of volunteers and internet application vendors to promote the capability to control, share, and move data from one system to another.

The relevance of this initiative has not been lost on social network sites, however. The idea of carrying along one's personal information ecosystem from one environment to another made the involvement of social network sites imperative; no social network site can afford not to incorporate data portability features in its site, which explains the list of web industry players that have shown interest until now.[63] In January 2008, several major web companies joined: Google, Facebook and Plaxo, followed by Drupal, Netvibes and Mystrands, and then LinkedIn, Flickr, Six Apart and Twitter, as well as Digg and Microsoft. This is quite an impressive list for an initiative that was only launched in November 2007.

5.5 Data dissemination in social network sites

In the previous sections we have looked at three perspectives from which we can understand privacy issues in social network sites: the user's perspective, the provider's perspective and third parties' perspective. However, it is also worthwhile to look into which *data* are disseminated in social network sites, on a more general level, and in which general cases disclosure proves to be a privacy problem. This is what we will look into in this section.

When addressing the privacy issues surrounding social network sites, it is important to establish which types of data are actually being discussed. Data may come from different sources, and may carry different levels of privacy sensitivity. This sensitivity is dictated to a large extent by the consistency between the originally intended audience of certain information, and the audience that eventually ends up being confronted with the information, that is whether information is deemed sensitive or not is largely related to the *context* in which it is disclosed. We have seen examples of this when discussing Nissenbaum's ideas on privacy as contextual integrity in Chapter 3 (see section 3.1.3). In social network sites contextual integrity is a key to understanding sensitivities with regard to the spread of personal information as well. For example, it would not cause great distress if holiday pictures that were originally meant to be shared with direct family members end up being viewed by some close friends, even if these close friends were not the intended audience for these pictures. However, it may be much less pleasant if the exact same pictures end up on the computer of one's manager.

The following overview addresses the different types of data:

- *Private data*: data that a user has decided to keep to himself, for instance his marital status or political preferences;
- *Shared or semi-public data*: data that a user wants to share with some other people, for instance with his family, a close group of friends, or his colleagues;
- *Public data*: data that is available to anyone.

[63] See http://en.wikipedia.org/wiki/DataPortability [last accessed on 12 February 2010].

5.5.1 Data dissemination

Fundamental to social network sites is the fact that data is shared between different users of the social network site. Privacy issues may arise when other users disseminate data meant for one particular group to other – unintended – audiences. The different combinations of sharing information with others are depicted in the diagram below.

		Someone else treats this information as…		
		Private	**Shared**	**Public**
A user deems information he has shared…	**Private**	(1) not relevant	(2) possible privacy violation	(3) possible privacy violation
	Shared	(4) no privacy issue	(5) possible privacy violation	(6) possible privacy violation
	Public	(7) no privacy issue	(8) no privacy issue	(9) no privacy issue

Table 7: Data dissemination and privacy issues in social network sites.

Before addressing the different combinations, one remark should be made. Until now we have discussed the sharing of social network site profile information by parties who have '*played by the rules*'. Whether we agree with the rules is another question, but social network site users, providers, and third parties have been assumed to act in accordance with the legal provisions that govern social network sites. These rules may be codified in the Terms of Use, in End User License Agreements, in data protection laws, or in any other source of applicable law.[64] However, unfortunately, we cannot rely on everyone observing the law, and this leads us to cell 2 and cell 3 in the matrix. These cells represent information that the user has designated as private, but that is being treated by (dishonest) others as either shared or public information. When a user profile is hacked, and an outsider gains access to private information, the acquired information can be shared with a small group or with the public at large. When the latter occurs, as is represented by cell number 3, embarrassment and shame may result. When information is released to a small group (cell number 2), situations like blackmail or identity theft may occur. Although the privacy issues resulting from these types of security breaches are significant, we will not investigate them further here. In the rest of this chapter, the privacy issues under review will *not* be the result of a breach of any legal or technical barriers protecting the social network site user information.

Let us turn to a discussion of the other cells of this table instead. Cell number 1 is not relevant with respect to privacy issues: after all, when you have defined information as private, someone else will not have access to your information in the first place. The conception of someone else treating your information as private therefore does not have any practical meaning. The other extreme occurs when you have defined your data as public, that is, accessible to anyone. It is possible that another person treats this data as private, shared or public information, but since the data owner already has defined the data as public in the first place, the subsequent decision on its further dissemination by someone else is inconsequential in terms of privacy violations. The bottom three cells (numbers 7, 8, and 9) do not involve privacy issues, therefore. The same holds

[64] For a detailed discussion of legal issues in social network sites: see the next chapter.

for cell number 4: if someone else decides to treat information that you have shared with him as private, no privacy issues will ensue.

The situation changes if you have released information to a particular group, for instance to your close friends, and one of these friends decides to make this information publicly available (cell number 6). This would constitute a privacy breach from the perspective of the information owner. Cell number 5 merits some more attention, because it potentially contains two different situations. First, information shared with a certain group may be treated as shared between members of the *same* group by someone else. In that case, no harm is done, because this is in line with the objective of the data owner. However, if one of the group members decides to share this information with (members of) *another* group, it reaches an audience the data owner never intended. In that case, the effect may be equivalent to the dissemination of information from the shared environment to the public environment described above in cell number 6, when the information is released to the public domain without limitations. The effect is less intrusive if it is shared with another group and as such not completely up for grabs for anyone. However, it is still an unintended data release from the perspective of the data owner.

5.5.2 Data types

In the previous section, sharing of data between different members of a social network site was addressed. This section will discuss the *types* of data that can be discerned in social network sites, whereby the main focus will be on the *origin* of the data. The distinction between the different types of data is relevant, since protective measures for each data type may vary.

When we assess data stored in social network sites, the first classification is to whom the information relates:

- Data *about individual users*, whereby each single data element is *assignable to exactly one user*. An example of this type of data is the real name or social security number of a social network site member;
- Data about *relationships between users*, whereby each data element contains information relating to more than one user. A picture showing two social network site members is an example of this type of data. Another type in this category is a connection between two users in the same social network site;
- Data about *others*. An example of this type of data is a picture displaying two individuals, of which at least one is not member of the social network site.

The authors of the ENISA position paper on security in online social network sites propose to divide the different types of data in social network sites a different way: they distinguish between '*factual data*' and '*secondary data*' (Hogben, 2007):

- *Factual data* are directly supplied by the users to the social network site. Examples are all data entered on profile pages, or the content of messages exchanged between two members within the realm of the social network site. Note that this category includes all three of the categories we have distinguished above: data about individual users, about relationship between users, and about others;
- *Secondary data* is all information that the members of social network sites disclose to the network provider while using the network itself: data such as date and time on which the social network site was accessed and the duration of connections, but also the location (IP address) from which the connection was made, and so on and so forth.

All items and types of information discussed above can be found within the boundaries of the social network site, whether they were put there intentionally or may be derived from the use that members make of the social network site. The last category we have to consider is information from *outside* the realms of the social network site, which we will call '*additional information*'. These types of information can be used to enrich the data sets generated within the social network site, thus creating an even more detailed picture of the individual social network site member, his interests, habits, socio-economic situation, and so on.

5.6 Privacy protection goals for social network sites

Now that we have established the various types of data stored in a social network site (either explicitly by users and their connections, or implicitly through using the network itself), we can turn to a discussion of the protection of this data[65]. In the previous chapter we formulated a list of '*privacy protection goals'* when we addressed privacy issues in collaborative workspaces. Table 3 on page 62 summarized these goals. We can also study these same goals with the context of social network sites. Based on the work of Wolf and Pfitzmann (2000) we have formulated four privacy protection goals for social network sites and present them in the table below.

Privacy protection goal:	**Description:**
1. Confidentiality	Personal data is *confidential* if nobody other than the owner of the data and parties explicitly selected by the owner of the data (e.g. other users, the provider) are able to access these data. In the context of social network sites this entails that data is protected against undesired access of others, both from inside the social network site and from outside.
2. Integrity	*Integrity* of personal data ensures that nobody is able to retrospectively modify the data or circumstances of disclosure, or that everybody can notice such an illegitimate modification. In the context of social network sites this means that data is protected against unsolicited changes made by other users, the provider or third parties.
3. Availability	*Availability* of resources, services and systems ensures that a user can access his/her personal data on the system whenever he/she wants. In the context of social network sites this means that data is protected against (temporary) disappearance from the social network site due to actions of other users, the provider or third parties.
4. Unlinkability	*Unlinkability* ensures that it cannot be distinguished whether two or more items are related to each other or not, and in

[65] As said, in the next chapter we will look at the legal issues with respect to privacy in social network sites in great detail. This discussion is only intended to be a first introduction to that theme.

Privacy protection goal:	Description:
	particular whether they are connected to the same natural person or not. In the context of social network sites this means that information on the social network site can only be derived from other sources with the explicit consent of the data owner. This is in stark contrast with the current situation, in which the social network site provider has unlimited access to the raw primary data stored within the network, and to secondary data generated when members use the social network site.

Table 8: Privacy protection goals for social network sites.

All of these goals aim to prevent the loss of control of personal information: one of the key ingredients of trustworthy use of social network sites (and, for that matter, of any computer-supported network) is that the user stays in control of the information stored in the network. User control is one of the key ingredients to maintain what we have called 'audience segregation' above (see section 5.2.2). When this control is lost, the confidence users place in the social network site is undermined and users may restrict their further use of the system or even abandon them entirely. Potential benefits of social network site use will thus be lost on their members. In section 5.5.1 we discussed an example of such a breach of confidentiality: the loss of personal data due to a hacked profile (cells number 2 or 3 in Table 7).

The last privacy protection goal in Table 8 above, unlinkability, deserves special attention. As we have argued in the table it is relevant whenever information about or relating an individual user can be derived within the context of the social network site. Note that the issue of unlinkability is not limited to the combination of information from *outside* the social network site with information from *inside* the social network site. Rather, when using a particular social network site, different types of information are created, which might ultimately be linkable to a certain social network site member. It may, however, not be in the user's interest that this combination of information is made. For instance, if someone makes use of a particular social network site for both leisure and business uses, statements and expressions directed at one audience may not be appropriate for the other audience. This process of separated contexts that collapse was discussed in section 5.2.2. The use of information from one context in another context that was never intended by the information owner is also known as 'decontextualization'. The result of this process may be devastating for the individual concerned: an observer could derive unwarranted conclusions about an individual based on out-of-context information.

Moreover, the combination of factual data and secondary data as introduced above may not be in the interest of the user. For example, it would be possible to combine the fact that the private profile of a user (factual information) has been updated from behind a computer at the office during working hours (secondary information). These combinations can currently be deduced with the information available to the social network site provider. Unlinkability issues should thus also be considered within each particular social network site, and refer to both factual and secondary types of information.

5.7 Requirements for privacy-enhanced social network sites

We will now turn to formulating a number of requirements for privacy-enhanced social network sites. We will base these requirements on the privacy protection goals as stipulated in Table 8 above. With all of these requirements it is important to remember that people have compelling social reasons to use social network sites, and those same social factors (may) lead them to misunderstand the privacy risks involved. Because of the social relevance of this new form of online interaction and self-presentation, 'solutions' that focus exclusively on restraining practices of sharing of personal information miss the point that people use these networks *because* they enable them to share personal information in the first place (boyd, 2008c; boyd and Ellison, 2007; Grimmelmann, 2009).

We have gathered a set of requirements of privacy-enhanced social network sites in Table 9 below.

Privacy protection goal:		Requirement:	Description:
1. Confidentiality	→	**a. Awareness of the potential audience**	There is a wide variety of social network sites available, and using social network sites is very popular. As we have sketched in this chapter one of the problems with using social network sites in their current form is that members lack an overview of the (potential) audience to which they are disclosing information. They post information on their profile pages assuming that only their 'friends' can see it, whereas in fact oftentimes a much wider audience has access to it (i.e. other users, providers, third parties, outsiders). Making users aware of the broad potential audience supports the realisation of the right to control to whom personal data is disclosed. *Social network sites should provide features to raise the awareness of users with respect to the potential audience of what they share in these environments.*
	→	**b. Choosing the potential audience**	Even if users would be aware of the potential audience, in the current generation of social network sites users have very limited means to define who has access to what they disclose within the social network environment. They can define privacy settings for items on their profile page (for instance, their telephone number or address), but most social network sites do not enable users to set the accessibility of *each* item of information they post online. *Social network sites should provide options for users to define who has access to each item of content they disclose in this environment.*
	→	**c. Facilitating multiple contexts**	One of the most important difficulties with respect to self-presentation in the current generation of social network sites is the issue of 'context collision': a user's contacts are clustered together into a single audience, thereby preventing him to show different sides of himself to different audiences (as individuals tend to do in everyday real-life contexts). Audience segregation is thus inhibited, which undermines individuals' freedom to express themselves and may cause privacy problems.

Privacy protection goal:		Requirement:	Description:
			Social network sites should provide options for users to disclose different sides of themselves (work, private, hobby, etc.) within separate contexts in the same social network, thus more accurately mimicking the rich texture of everyday social life and respecting the various degrees of intimacy in it.
	→	**d. 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 social network sites everyone within a particular social group is attributed the same 'intensity', that is, everyone is treated the same with respect to access to a user's information. Moreover, once contacts have been added to a user's contact list, the only way to remove them from it is through using the (socially highly awkward) mechanism of 'defriending'. *Social network sites should provide users with options to manage relations in ways that more accurately mimic the ways in which relationships wax and wane in real life. For instance, contacts a user has not disclosed any content to for a substantial amount of time could be made to fade away from the contacts list.*
2. Integrity	→	**Protection of integrity**	In current social network sites users can add and modify content on their own profile page, but they can also add content to the pages of other users, or they can tag content and thus disclose information about others. Providers have access to all of the information placed online within the social network environment and can remove content if it is deemed harmful for individuals or the provider itself. Third parties sometimes have access to users' information as well, for instance through applications offered within the social network site. *If other users post information about an individual in the social network environment, the provider should make the individual aware of this fact. If information is removed or accessed by third parties, the social network site should notify the user.*

Privacy protection goal:		Requirement:	Description:
3. Availability	→		Users wishing to delete accounts from existing social network sites often learn that it is difficult enough to remove one's own account and profile page, but almost impossible to remove secondary information linked to their profile such as public comments on other profiles but also data on an individual's use of the platform, time stamps, surfing behaviour etc. Platform providers have an incentive to keep the profiles (even if they are dormant) for economic reasons. *Social network sites should enable users to easily remove their profile pages and accounts and provide them with options to view (preferably at a glance), change and delete secondary information*.
4. Unlinkability	→	**a. Protection against surveillance**	Awareness that one is being watched can lead to "*anxiety and discomfort,* […] *self-censorship and inhibition*," (Grimmelmann, 2009). Social network sites should offer users mechanisms that enable them to see who has accessed their information.
	→	**b. Protection against profiling**	Profiles on social network sites can be downloaded and stored by third parties, thus enabling these third parties to use these profiles to create a digital dossier of personal data. *Social network sites should prevent the possibility of unauthorized downloading of profile information.*
		c. Protection against the panoptic provider	The platform provider has a reasonably comprehensive snapshot both of who the user is and of who he knows. This information is used for targeted advertising and other profiling uses. *The infrastructure of social network sites could make it impossible for the social network*

Privacy protection goal:		Requirement:	Description:
			site provider to have access to all of the data of its users (both factual and secondary data). Alternatively, as a minimum requirement, it should adhere to auditable processes that safeguard user data from inappropriate access and uses.

Table 9: Requirements for privacy enhanced social network sites.

In this chapter we have provided an overview of a wide array of privacy issues as these emerge in existing social network sites. We began by listing a variety of parameters that are relevant in this respect, viz. the architecture of social network sites – which invites users to view them as a 'walled garden', when in fact they are rather open platforms – and the fact that users feel there is safety in the huge numbers of other users active in these environments. Then we went on to categorize privacy issues in social network sites by looking at them from three different perspectives: (1) the individual user's perspective; (2) the provider's perspective; and (3) the perspective of third parties. We listed causes for privacy violations and risks with respect to all three of these perspectives. Then we turned to a discussion of the types of data that are disclosed in social network sites, and we distilled a list of privacy protection goals, similar to the one we developed in Chapter 4 with respect to collaborative workspaces. We ended the chapter with an overview of requirements for privacy-enhanced social network sites, based on the privacy protection goals we formulated.

Using these privacy protection goals and the requirements that stemmed from them we have built a demonstrator of a privacy-enhanced social network site, in which we have implemented the requirements formulated in Table 9. We will present this social network site demonstrator, which we've called Clique, in Chapter 7, together with the other demonstrators within Work Package 1.2. However, before doing so we must delve a little further into the *legal* aspects of privacy protection in social network sites. This is what the next chapter is about.

Chapter 6

Legal aspects of social network sites and collaborative workspaces

After analyzing the privacy issues in social network sites we will now turn to a legal analysis of the problems emerging from the use of social network sites and collaborative workspaces. In the next sections we will describe the implemented European legislation and its applicability to social network sites and collaborative workspaces (sections 6.1 - 6.7). In section 6.8 we will address a number of specific problems concerning social network sites, such as the End User License Agreements (EULAs) and Terms of Use (ToUs) used by the providers of these sites. The chapter will end with a number of concluding thoughts.

One important point needs to be made at the beginning of this chapter. In this chapter we have chosen to address both the legal issues that arise in social network sites, and those that arise in collaborative workspaces, that is, at least where these *overlap*, which is, in fact, the case most of the time. Social network sites, as such, raise more, and more far-reaching legal issues than collaborative workspaces, since in these environments users actively share personal information, which may cause privacy problems that need to be addressed from a legal perspective. Moreover, in social network sites a wide variety of services are combined for members to use, each having their specific legal consequences. This leads to a complex and multi-faceted legal problem.

In collaborative workspaces, by contrast, the possible privacy violations that may arise are more straightforward (if not equally devastating to the users on the receiving end of them). In collaborative workspaces users tend to disclose less personal data. Moreover, the variety of services offered by each single collaborative workspaces is less broad, and hence possible privacy risks are more easily defined in legal terms (if not more easily solved in technical terms).

Therefore, throughout this chapter we will discuss legal issues and legislation with respect to both social network sites and collaborative workspaces, but at times we will discuss aspects of the former in much greater detail.

6.1 Relevant European legislation and its applicability to social network sites and collaborative workspaces

In the European Union legislation on privacy and identity management is mainly enclosed in a set of directives focused on data protection. The package consists of (1) the general Data Protection Directive 95/46/EC[66], which forms a data protection framework; (2) e-Privacy Directive 2002/58/EC[67]; and (3) the Data Retention Directive 2006/24/EC[68]. All of them provide important definitions together with specific legal requirements for privacy and data protection. Other regulations that are considered to be important for the subject of social network sites can be found in the e-Commerce Directive 2000/31/EC[69], and the Copyright Directive 2001/29/EC.[70] We will discuss each of these items of regulation in relation to social network sites in turn.

6.2 The Data Protection Directive (95/46/EC)

Social network sites and collaborative workspaces, in general, fall under the regime of the Data Protection Directive. Providers of those services have an obligation to comply with its rules on privacy protection irrespective of how a particular social network site or collaborative workspace is structured.

The main goal of the Data Protection Directive is to promote the free movement of personal data within the European Union, and to ensure a high level of protection of both the right to privacy, and the fundamental rights and freedoms of the individuals with regard to the processing of personal data in all Member States (Recital 3 of the Directive). The Preamble of the Directive explicitly states these two objectives of ensuring that personal data can move unrestrictedly within the Single Market of the European Union on the one hand and that a level of protection of the individual's rights on his personal data is uniform within the whole EU on the other. This feature is of great relevance for social network sites and collaborative workspaces because very often users take advantage of the lack of borders in an online environment and participate in all sorts of social networks, irrespective of the geographic and national boundaries.

6.2.1 The scope of the Data Protection Directive

[66] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L281, pp. 31-50 (23 November 1995).
[67] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Official Journal L201, pp. 37-47 (31 July 2002).
[68] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, Official Journal L105, pp. 54-63 (13 April 2006).
[69] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), Official Journal L178, pp. 1-16 (17 July 2000).
[70] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, Official Journal l 167, pp. 10-19 (22 June 2001).

The scope of the Directive, described in Article 3, covers the processing of the personal data wholly or partially by automatic means, as well as the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system. A 'personal data filing system' is defined in Article 2(c) DPD and it refers to any structured set of personal data that is accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis. This definition describes perfectly any social network service, which in fact is always a set of personal data organized in a way that allows communicating with other users within a bounded system that facilitates viewing and transversing their list of connections. In order to fulfil the points of the acquired definition, the social network will have to use some structure to make the data accessible.

The Directive does not apply to the processing of personal data in the course of the activity that falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security and the activities of the State in areas of criminal law. Additionally, the Directive does not apply to the processing of personal data by a natural person in the course of purely personal or household activities. This particular exception plays a significant role for the use of social network sites or collaborative workspaces. It could easily eliminate the usage of these types of web 2.0 environments from the scope of the Directive if one decides that it concerns 'personal use'. This area of exemption was examined in the Lindquist case, crucial for the subject, which will be discussed further in this below.

6.2.2 The definition of roles

For the purpose of the discussion on the legal aspects of social network sites and collaborative workspaces, the basic concepts of data protection, introduced in the Directive, should be emphasized. According to the Article 2(a) DPD, personal data is any information related to an identified or identifiable natural person, who in this sense becomes a data subject. The notion of 'personal data' is very broad as it normally applies to all text, sound and image data – therefore, the Directive foresaw some exceptions. Recital 16 of the Directive provides that the processing of sound and image data, like video surveillance, does not fall under the scope of the Directive if it is carried out for the purposes of public security, defence, national security or in the course of State activities relating to the area of criminal law or of other activities which do not come within the scope of Community law. According to Recital 17, when the processing of sound and image data is carried out for purposes of journalism or the purposes of literary or artistic expressions, in particular in the audiovisual field, the principles of the Directive should apply in a restricted manner, but only if it is necessary to reconcile the right to privacy with the rules governing freedom of expression – which is specified in Article 9 DPD.

As explained in Article 2(a) DPD, for the Directive an 'identifiable person' is every person who can be identified, either directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. According to Recital 26 of the Directive, in order to determine whether a person is identifiable, account should be taken of all the means likely to be used either by the controller or by any other person to identify the said person. This is an expansive approach, as all data that could be linked to an identifiable individual will fall under the scope of the Directive. In result, data will be equivalent with 'personal' as soon as it will be possible to identify the person, to whom the information refers.

Recital 15 of the Directive states that processing of data is only covered by the Directive, if it is automated or if the data processed are contained in a filing system structured according to specific criteria relating to individuals, so as to permit easy access to the personal data in question. The

definition of the 'processing' itself is equally broad. It refers, according to Article 2 (b) DPD, 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. This list contains, basically, any possible activity that could be performed on personal data. For example, even a single consultation or retrieval of a file containing personal data constitutes a processing and requires application of the provisions of the Directive. It is actually difficult to imagine any operation performed on personal data that is not included in this definition. Just the mere storage of personal data on a server should be qualified as processing, despite the fact that nothing is really done with the data. Without a doubt, any provider of a social network site or a collaborative workspace will be involved in usually more than one of the named activities and will be rendered to process personal data. For the operation of social network sites and collaborative workspaces, actions such as the collection of data, storage, organisation, as well as blocking and erasure are the minimum necessity without which functioning of such sites would not be possible. Also, all three actions of disclosure by transmission, dissemination or otherwise making available seem to be an indispensable factor for the existence of these web 2.0 environments, as they allow searching for profiles of friends and connecting with them, or searching for postings and comments, which, at the end of the day, are what these web 2.0 environments were created for.

The Data Protection Directive also provides several other relevant definitions. In the context of data protection, 'controller' means every individual or entity who determines the purposes and means of the processing of the data. Depending on the situation, the actual data controller can vary, and sometimes more than one responsible controller can appear. The situation of joint control arises when the decision about the data is made together by different entities. There is a possibility that for the same action of data processing the provider of the service and the user will be in position of co-controllers (Van Alsenoy *et al.*, 2009). Additionally, the term of 'data processor' was introduced by the Directive. A data processor is a third party who merely processes personal data on behalf of the data controller. The fact is that due to technological development, since the enactment of the Directive, the number of parties participating in processing of data has increased. Additionally, the processing became, very often, a highly automated activity. It has resulted in blurred situation sometimes and currently the distinction between controller and processor is not always easy to make (Kuner, 2007: 71-72). Such a differentiation, between 'data controller' and 'data processor', is crucial in order to define the liability for violations of the Data Protection legislation. As a general rule, the data controller is the one to take the responsibility for any irregularities or infringements. Another important term is 'data recipient' which, according to Article 2 (g) DPD, is any person to whom the data is disclosed, whereas a 'third party' is any person other than the data subject, the controller, the processor and anybody else who is authorized to process the data.

All these notions are essential for the user-provider relationship within a social network site and a collaborative workspace. Depending on the particular situation and the person performing an activity, the status might be changing, and very often the same person will play more than one role at the same time – but not necessarily for the same data and the same activity. A user of a social network service can, for example, be a data subject – for his own data –, and at the same time a data controller – for somebody else's data –, if he is the one processing personal data and deciding on the purposes and means of such processing. The extent to which someone is processing someone else's data will be the decisive factor when assessing the person of the controller. A certain level of decision-making power on the purposes and means must be exercised by an entity to be qualified as a controller. Of course, it should not be forgotten that the power of the user to determine the means of processing is limited. As we have seen in the previous chapter, the user can normally adjust some features or settings to his wishes, but he does not have any power over the manner in which the processing is conducted (Van Alsenoy *et al.*, 2009). This aspect of the service is non-negotiable and depends entirely on the provider. The technical functionality of a

service relies on commercial intermediaries providing the service (Wong and Savirimuthu, 2008). However, the user exercises a decision-making power on whether or not he wants to provide a particular piece of information and which application he decides to use. Therefore, the *roles* of the entities in the processing of information should be distinguished with regard to a specific processing operation.

Note that a distinction should be made between the decision-making power regarding the overall structure of an application, its security features, generic purpose etc. on the one hand, and the decision-making power over the input of specific personal data on the other (Van Alsenoy *et al.*, 2009). If both of these decisions are made by the same actor, there will, most likely, be a single controller. Otherwise there will be multiple controllers. Nevertheless, they might not always be in the positions of co-controllers or be jointly liable for the same processing operations. To the contrary, each participating entity can be considered a controller for separate actions that occur (Van Alsenoy *et al.*, 2009). To conclude, the user of the social network site or a collaborative workspace can be qualified as the controller but only of those processing operations for which he can really determine the purpose and means. This means that the user can be attributed the controllership with regard to the information he decides to provide and the processing operations he initiates (Van Alsenoy *et al.*, 2009).

To clarify this conclusion let us take a look at the very popular practice of 'tagging' pictures on the social network site Facebook.[71] In this case the parties involved could be:

- Facebook;
- Individual A, a member of Facebook who uploads a picture of a friend who is not a member of Facebook himself;
- Individual B, a member of Facebook who is in A's contact list, and who tags the picture; and
- Individual C, a non-member (or outsider) whose picture is uploaded by A and tagged by B.

Facebook, who provides the technical functionality, is a controller since it determines the purposes and means of processing data by providing the technical functionality. The same goes for person A, who is the only one with the power to remove the tag after it appears on his profile (in the described situation[72]). Person B is also a controller as he provides the name (and possibly also an e-mail address) of C. The only one who has *no* control over the processing of his own data in this scenario is C, who is merely a data subject. If he still refuses to register for the service, which would give him the power to de-tag, his only solution is to ask A to do it for him. After sending a notification e-mail to C, informing him about being tagged, Facebook stores his name and e-mail address for its own purposes. This constitutes a new activity for which Facebook will be a controller.

The question whether a user can be considered a data controller has not been answered until the Lindquist case[73]. In this case one of the questions raised was whether the act of referring, on an internet page, to a person and identifying that person by name or by other means, for example by giving their phone number or information regarding their working conditions or hobbies (which was declared to be an act of processing of personal data wholly or partly by automatic means) is covered by the exception of personal use from Article 3(2)(b) DPD. The European Court of

[71] The practice of tagging in social network sites will be discussed in more detail in section 6.8.2.
[72] If the tagged person would be another Facebook user, he would be able to remove the tag as well. See section 6.8.2.
[73] ECJ, C-101/01, 6 November, 2003, available at: http://curia.europa.eu/jurisp/cgi-bin/gettext.pl?lang=en&num=79968893C19010101&doc=T&ouvert=T&seance=ARRET [last accessed on 16 February 2010].

Justice ruled that this particular exception must be interpreted as relating solely to activities carried out in the course of the private or family life of individuals, for instance in correspondence or the holding of records of addresses, as mentioned in recital 12 of the Directive. The court ruled that this is not the case when the processing of the data consists in publication on the internet, which makes such data accessible to an indefinite number of people.[74] According to this decision it could be argued that the unrestricted use of social network sites and collaborative workspaces does not fall under the exception of Article 3 (2)(b) DPD and therefore, that the Directive is applicable to both of these types of web 2.0 environments.[75]

6.2.3 Applicability of the EU data protection law

An analysis of the circumstances under which the national data protection laws of the Member States should apply (Art. 4 DPD) results in a conclusion that EU data protection law in general is applicable to service providers who have their place of establishment outside of the EU in two situations: 1) if the processing of personal data in the context of establishment occurs within the EEA; 2) if the data is processed outside of the EEA but with the use of equipment based within the EEA. If the controller has no establishment in a Member State to guarantee privacy protection for individuals in the European Union the Directive clarifies that it is applicable nevertheless when the controller uses equipment for the processing of personal data, which is situated on the territory of a Member State. The term 'equipment' covers all possible means for data processing, such as computers, telecommunication devices, impression units, etc. As an exception to this rule, mentioned in Article 4, the Directive does not apply when the equipment is used only for the purposes of transit of personal data through the territory, such as cables or routing equipment. Additionally, the regulation provides that if the means for processing personal data are located on the territory of a Member State, a representative established in the aforementioned Member State should be designated by the controller. The provisions of Article 4 were introduced to avoid any possibility of circumvention of the protection granted by the DPD, and also to avoid having data subjects left without protection (Terwangne and Louveaux, 1997), which is explained in more detail in recital 20 of the Directive.

In the first case, if the processing of data takes places within the territory of the EEA, it is important to note that the providers of various internet services often have their establishment outside of the EU. According to Google's Response to the Article 29 Working Party Opinion on Data Protection Issues Related to Search Engines[76] this situation will exclude them from the scope of the Directive. Even though Google has branches in some locations in Europe (Ireland, Belgium, the Netherlands), in their Response they claim that, in order to fall within the scope of the EU data protection law, these branches would have to be involved in the actual processing of personal data, and, above that, do it as a controller. It is important to acknowledge that activities performed by the EU-based branches of Google may not necessarily be involved in the processing of user data. One example of such an activity is the practice of selling targeted advertising, which does not require the actual processing of user data, as Google explains in the Response. However, if the data was processed by an EU-based entity, for example by one of the data centres, it is still Google Inc. making all decisions regarding the purpose and means of the data processing activities, which makes them the controller of the data. Since the EU-based Google branches are not acting as controllers of the data and do not determine the purpose and the means by which the user data is

[74] See the previous footnote.
[75] We will return to the Lindquist case in more detail below.
[76] Response to the Article 29 Working Party Opinion On Data Protection Issues Related to Search Engines, 8 September 2008, available at: http://blogs.taz.de/ctrl/files/2008/09/google.pdf [last accessed on 16 February 2010].

processed, it is argued that the EU data protection law will not apply to them. The question should be asked what would happen in a situation when data processed outside the EU comes back to European users in the form of targeted advertising.

In the second case, if the data is processed outside the EEA but with the help of equipment within the EEA, it is important to consult Article 29 Working Party opinion WP 56[77]. It states that if cookies are placed on a user's hard disc, the law of the Member State in which the computer of the user is located will be applicable. Consequently, service providers that are established outside of the EU, who use cookies to deliver their services, will need to apply the EU data protection law. In their Response to this Article Google admits that this practice is acknowledged in its Privacy Policies, in which Google explains that it sends cookies when the user visits their website.[78] For that reason, Google falls within the scope of DPD.

A third scenario arises when Google Inc., which is located in the US, has access to their global network of data centres, some of which are situated in the EEA. In that case Google will, undoubtedly, use equipment placed in the EEA.

Now, how do these regulations apply to social network sites and collaborative workspaces? Once again a nuanced analysis is required. In certain situations, such as described in Article 4(1)(a), application of the DPD would depend on whether a particular provider of a social network site or a collaborative workspace has a place of establishment in the EU. If it doesn't, and the data is processed outside of the EU, a situation similar to the one of Google will occur. In order to find out whether this is the case, it is necessary to check the privacy policies and Terms of Use of individual social network sites and collaborative workspaces. It is very likely that the controller will not have his establishment in the EU. Some of the most popular social networks sites are provided by entities located in the US, and the same goes for collaborative workspaces such as Wikipedia. Nevertheless, they very often have additional branches in Europe. Most of the time, however, it is the headquarters of the company that decides about the means and purposes of data processing. For instance, Facebook's Privacy Policy states that the data obtained by them is being transferred to and processed in the United States[79], which is relevant information.

If both the place of establishment and of data processing is outside of EU, the use of jurisdictional rule provided in Article 4(1)(a) will not bring the service provider within the scope of the application of EU data protection law. If equipment is used within the territory of the EU, the situation resembles the one of Google described above. This is so because use of cookies is a common practice among service providers. In its Privacy Policy Facebook clearly states that it uses "…*cookies (small pieces of data* [they] *store for an extended period of time on* [a user's] *computer, mobile phone, or other device) to make Facebook easier to use, to make* [their] *advertising better, and to protect both* [the user] *and Facebook. For example,* [they] *use them to store* [the user's] *login ID (but never* [his] *password) to make it easier for* [the user] *to login whenever you come back to Facebook. We also use them to confirm that you are logged into Facebook, and to know when* [he is] *interacting with Facebook Platform applications and websites,* [their] *widgets and Share buttons, and* [their] *advertisements.*"[80] MySpace announces that it uses "*cookies to identify your Internet browser, store Users' preferences, and determine whether you have installed the enabling software needed to access certain material on the MySpace Services. Data in cookies may be read to authenticate user sessions or provide*

[77] Article 29 Working Party Opinion WP 56 Working document on determining the international application of EU data protection law to personal data processing on the internet by non-EU based web sites, available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp56_en.pdf [last accessed on 16 February 2010].
[78] See the Response to Article 29… cited in an earlier footnote.
[79] Facebook Privacy Policy, available at: http://www.facebook.com/policy.php; Google Privacy Policy, available at: https://checkout.google.com/files/privacy.html [both websites last accessed on 16 February 2010].
[80] Facebook Privacy Policy, available at http://www.facebook.com/policy.php [last accessed on 16 February 2010].

services."[81] Because of this service providers will be bound by the EU data protection regulation, which is in line with the opinion of the Article 29 Working Party.

As for the third scenario described by Google, which revolves around their establishment in the US and access to data through data centres located in the EEA, the answer depends on the design and organization of each specific social network site and each specific collaborative workspace. The main question will be whether such a service provider, whose place of establishment is outside of the EU, will be running branches, for example data centres within the territory of EU. Moreover, they will also have to access to the resources of those branches. If the answer to this question is yes, then the EU data protection law will be applicable.

6.2.4 Principles of data processing

The DPD also introduces specific principles essential for lawful data processing. These principles are sometimes described as the constitutional law of data protection as they set out the core regulation regarding the processing of personal data (Blume, 2002: 30). They simply have to be fulfilled in order to declare the data processing legal and lawful. The addressee of these principles is the 'data controller'. In several articles of the Data Protection Directive principles are presented for the lawful processing of data. In the table below we have summarized them, together with the DPD article number in which they are to be found.[82][83]

Principle:	Article #:	Description:
1. The principle of fair and lawful processing	6	This is a primary requirement since all the others stem from it.
2. The principle of finality	6	This means that data should be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.
3. The principle of data minimisation	6	This means that data has to be adequate, relevant and not excessive in relation to the purposes for which they are collected.
4. The principle of data quality	6	This specifies that data must be accurate and, where necessary, kept up to date.
5. The principle of data conservation	6	This means that data should be kept in a form which permits identification of data subjects for no longer than is necessary.

[81] MySpace Privacy Policy, available at: http://www.myspace.com/index.cfm?fuseaction=misc.privacy [last accessed on 16 February 2010].
[82] All descriptions are quoted or paraphrased from the text of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L281, pp. 31-50 (23 November 1995).
[83] For a more extensive discussion of the principles and their place in European privacy legislation see for example the second chapter of (Cuijpers, 2004).

Principle:	Article #:	Description:
6. The principle of security	17	This means that the controller must implement appropriate technical and organizational measures to protect personal data against accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.
7. The principle of notification to the supervisory authority	18	This means that the Member State or controller must notify the supervisory authority before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes.

Table 10: The principles of data processing as stipulated in Directive 95/46/EC.

Moreover, the Directive also lists the rights of the data subject. These are listed in the table below, again with their accompanying article number.[84]

Data Subjects' Rights:	Article #:	Description:
1. The right to information	10	When a data controller or his representative collects a data subject's personal information, the controller or his representative must provide the data subject with at least the following information: - the identity of the controller or his representative (if any); - the purposes of processing; - further information such as the recipients of the data, whether replies to questions are obligatory or not, that the data subject has the right of access and the right to rectify data concerning him (both of these rights will be discussed below).
2. The right to object	14(a)	This means that the data subject can always object to the collection of his data on compelling legitimate grounds. If the objection is justified his data will be excluded from the collection.
3. Right of access	12	This means that the data subject has to right to obtain from the controller, without constraint at reasonable intervals and without excessive delay or expense: - confirmation as to whether or not data relating to him are being processed, and information at least as

[84] In this table, too, all descriptions are quoted or paraphrased from the text of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, Official Journal L281, pp. 31-50 (23 November 1995).

Data Subjects' Rights:	Article #:	Description:
		to the purposes of the processing, the categories of data concerned, and the recipients to whom the data are disclosed; - communication to him of the data undergoing processing and of their source; - knowledge of the logic of automatic processing involved.
4. The right to rectify, erase or block the data	12	This means that the data subject has the right to rectify, erase or block the processing of his data if it does not comply with the rules for data processing stipulated in the Directive, in particular because of the incomplete or inaccurate nature of the data.
5. The right to seek legal relief	22	This means that Members States must provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question.

Table 11: The rights of data subjects as stipulated in Directive 95/46/EC.

Special attention should be paid to the provisions of Article 7, which describes when it is allowed to process data. Article 7(a) states that personal data may be processed only if the data subject has unambiguously given his consent. According to the definition provided in Article 2(h) of the Data Protection Directive the 'data subject's consent' means any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed. This provision is of particular importance for the users of social network services, who agree to have their data processed through Terms of Use and privacy policies.

Users of Facebook, registering to the service agree that they "will not provide any false personal information on Facebook, or create an account for anyone other than [themselves] without permission. [Moreover, users agree to keep their] contact information accurate and up-to-date." Furthermore, they consent to "having [their] personal data transferred to and processed in the United States"[85].

When signing up for MySpace and agreeing to its Terms of Use a user is also accepting MySpace's privacy policies. That way he provides his consent to data processing. MySpace writes: "*MySpace collects your email address, first and last name, postal code, gender, and date of birth from you in order to register you as a Member ("Registration Data"). MySpace cannot register you as a Member without this information. All other information you provide during the MySpace registration or that you post on the MySpace website is voluntary. MySpace may also collect PII* [i.e. personally identifiable information] *from you if you choose to participate in MySpace Services activities like sweepstakes, contests, and surveys, because you want us to furnish you with products, services, newsletters, or information, or in connection with content or suggestions you submit to MySpace for review. In addition, MySpace collects other Related Data*

[85] See http://pl-pl.facebook.com/terms.php [last accessed on 17 February 2010].

and non-PII including IP address, aggregate user data, and browser type. This data is used to manage and improve the MySpace Services, track usage, and for security purposes. MySpace Members may also choose to provide or store non-PII information and Related Data in their profiles, including but not limited to date of birth, interests, hobbies, lifestyle choices, groups with whom they are affiliated (schools, companies), videos and/or pictures, private messages, bulletins or personal statements (collectively "Profile Information"). The Profile Information in a Member's profile is provided at his or her sole discretion. Please be aware that your Profile Information, as well as any information posted to any public forum, can be accessed by the public. Profile Information located on private profiles can be accessed by MySpace at all times and, in limited cases, by certain third parties authorized by MySpace for purposes of ensuring compliance with My Space's Terms of Use".[86]

Despite all the information provided to users oftentimes it is doubtful whether the users' acceptance of the Terms of Use truly constitutes unambiguous consent. As the International Working Group on Data Protection in Telecommunications points out, some users, only interested in obtaining the service, do not actually read Terms of Use or the privacy policy (2008). Others read them but do not always understand them. Therefore, the Working Group correctly argues that in order to make sure that users provide a truly informed consent the information should be tailored to the specific needs of the targeted audience. In the ENISA Position paper on online social networks it is even argued that Terms of Use should be replaced by user-friendly community guidelines (Hogben, 2007). Hogben *et al.* write that they should use accessible language to allow users to understand the rules of the site, which in turn would stimulate users to comply with them. However, some specialists argue that such a solution will not be very helpful, since users need to read the conditions or privacy policies and this problem is not solved by simply making them more accessible (cf. Grimmelmann, 2008).

6.2.5 Transfer of data to third countries

If data is processed outside the EU the rules on the transfer of personal data to third countries come into play. The Data Protection Directive provides these rules in Article 25 and lists derogations from the normal procedure in Article 26. Mainly, Member States should warrant that when personal data are transferred to a third country for (intended) processing, this may take place only if the third country ensures an adequate level of protection (Art. 25(1)). When we look at this issue in more detail, it turns out that this will not be the case with social network sites or collaborative workspaces. Articles 25 and 26 were introduced into the Directive in order to ensure an equal level of protection for data subjects from the EU, when their data is processed outside of the EU. This has to be taken care of in case the rules of the Directive do not apply. If the Directive is fully applicable itself, such an additional measure of protection is irrelevant. Entities involved in processing the transferred data will have to comply with all the provisions of the Directive anyway. This will occur in the discussed situation. As explained in the paragraph above, due to the use of cookies, social network sites and collaborative workspaces will fall within the scope of the DPD. This means that the additional layer of protection is not required.

[86] MySpace Privacy Policies, available at: http://www.myspace.com/index.cfm?fuseaction=misc.privacy [last accessed on 16 February 2010].

6.3 Focus on social network sites: Information society services and/or electronic communication services?

As we have argued at the beginning of this chapter, social network sites raise more, and more complicated, legal issues than collaborative workspaces, since social network sites are actively used by their members to disclose personal information. While many of the legal issues discussed in this chapter apply both to social network sites and collaborative workspaces, in this section we focus on social network sites alone, since they raise an interesting legal question with respect to the *kind* of service they are. Are social network sites electronic communication services, or are they information society services instead? Correct application of the appropriate Directives depends on the answer, so it is important to establish what kind of service these network sites are.

6.3.1 Social network sites as information society services

The definition of an 'information society service' is provided by Directive 98/34/EC.[87] Article 1(2) of the 98/34 Directive states that an information society service is characterized as any service normally provided for remuneration, at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, and at the individual request of a recipient of a service. When analyzing the individual elements of this definition, we can see that a social network site fulfils all of the necessary requirements to be qualified as an information society service. Social network sites are paid services, although, most of the time it is not the users who pay for the service. Nevertheless, it still is an economic activity performed to gain profits, which is the vital point of the definition. This particular requirement is not restricted to the users, or the recipients of the service, and therefore it is perfectly acceptable for other parties to remunerate the provider for his service (Lodder and Kaspersen, 2002: 67-93). Remuneration could be offered, for example, via advertisements or through direct marketing.

Recital 18 of the e-Commerce Directive clarifies that information society services are not solely restricted to services giving rise to on-line contracting but also, in so far as they represent an economic activity, extend to services that are not remunerated by those who receive them. Further, it enumerates some examples that cover services such as those offering on-line information or commercial communications, or those providing tools allowing for search, access and retrieval of data. Information society services also include services consisting of the transmission of information via a communication network, of providing access to a communication network or of hosting information provided by a recipient of the service.

Social network sites also deliver their services at a distance, while the parties are not simultaneously present. Having in mind the way a social network site works, it is obvious that face-to-face contact is not possible. The same has to be said about the remaining two components of the definition, which require a service to be delivered by electronic means and at the individual request of a recipient. The former means that electronic equipment must be used to send and receive the service, while the latter entails that the service has to be delivered on demand – which is always the case when typing the URL or following a link (Lodder and Kaspersen, 2002). We conclude that when analysing of all the elements of the definition of the information society service it turns out that labelling social network sites as information society services is justified.

---

[87] Directive of 22 June 1998, which lays down a procedure for the provision of information in the field of technical standards and regulations and of rules on information society services as named by Directive 98/48/EC of 20 November 1998 on the legal protection of services based on, or consisting of, conditional access.

6.3.2 Social network sites as electronic communication services

The terms 'public communication network' and 'electronic communication network' are defined in the Framework Directive,[88] which, however, does not provide a definition of publicly available communications services. A public communications network, according to Article 2(d) of the Framework Directive, is an electronic communications network used wholly or mainly for the provision of publicly available electronic communications services. An electronic communications network (Art. 2(a)) refers to transmission systems and switching or routing equipment and other resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed. An electronic communications service (Art. 2 (c)) is a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services. It does not include information society services, as defined in Article 1 of Directive 98/34/EC, which do not consist *wholly or mainly in the conveyance of signals on electronic communications networks.*

The explanation of what it means for a service to be 'publicly available' can be found in recitals 4 and 5 of the Universal Service Directive 97/33/EC[89], although there is no explicit reference to these provisions in Article 2 of the Framework Directive. According to the Universal Services Directive, the notion of 'publicly available' does not cover services available only to a specific end-user or to a closed user group. Moreover, the same Directive specifies that 'public' does not refer to ownership, nor does it refer to a limited set of offerings designated as 'public networks' or 'public services', but means any network or service that is made publicly available for use by third parties.

6.3.3 Further issues

After this analysis we may conclude that the most popular types of a social networks fulfil the criteria given by the definition of the information society service. However, some social network sites offer e-mailing options as well, which are functionally equivalent to web-mail. At this point it is useful to take a look at the Article 29 WP Opinion on data protection issues related to search engines.[90] As this document explains, services providing or exercising editorial control over content are explicitly excluded from the scope of the definition of an 'electronic communications

---

[88] Directive 2002/21/EC of the European Parliament and of the Council on a common regulatory framework for electronic communications networks and services (Framework Directive), Official Journal L 108 , pp. 33-50 (24 April 2002).

[89] Directive 97/33/EC of the European Parliament and of the Council of 30 June 1997 on interconnection in Telecommunications with regard to ensuring universal service and interoperability through application of the principles of Open Network Provision (ONP), Official Journal L 199 , pp. 0032 – 0052 (26 July 1997).

[90] Article 29 Data Protection Working Party, Opinion 1/2008 on data protection issues related to search engines, WP 148, adopted 4 April 2008, available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp148_en.pdf [last accessed on 17 February 2010].

service'. This is the reason why search engines do not fall within the scope of that definition. Nevertheless, the document states, "*a search engine provider can offer an additional service that falls under the scope of an electronic communications service such as a publicly accessible email service which would be subject to e-Privacy Directive 2002/58/EC and Data Retention Directive 2006/24/EC*."[91]

Even though the opinion refers to search engines, the similarity with social network sites is obvious. Providers of social network sites may offer additional functionalities such as web-mail. And this partial service will fall under the scope of both e-Privacy and Data Retention Directive. This means that although social network sites primarily constitute an information society service, examination of additional functionalities offered is also relevant.

To conclude, it should be noted that every social network site could be in a different position, depending on its design and the partial services it provides. For that reason, each particular social network site should be analyzed separately in a case-by-case manner to decide what type of services it covers. Appropriate assessment will allow for application of the correct laws.

6.4 The e-Privacy Directive (2002/58/EC)

The rules provided by the Data Protection Directive also apply to electronic communications, apart from the services placed in the scope of the DPD. More specific rules for the processing of personal data in electronic communications are contained in the e-Privacy Directive. The list of requirements, introduced by the DPD, is complemented and adjusted to the needs of the electronic communications sector, which results in the addition of specific principles, such the principle of confidentiality, and requirements for processing data and the location of data.

In principle the e-Privacy Directive will not apply to social network sites, once again, because of the type of service it covers. As explained above, social network sites fit in the definition of an information society service (see section 6.3.1 above). However, particular social network sites (and collaborative workspaces, too) may be offering extra functionalities, such as web-mail, which fall within the definition of an 'electronic communications service'.[92] Providers of these services will have to comply with the provisions of the e-Privacy Directive. As already mentioned in the conclusion of the previous section, each time a nuanced analysis will be required. This is why the provisions of the e-Privacy Directive will be described below.

6.4.1 The scope of the e-Privacy Directive

The e-Privacy Directive applies only to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks within the Community. As explained in recital 6 of the e-Privacy Directive, publicly available electronic communications services over the internet open new possibilities for users but also new risks for their personal data and privacy. Furthermore, according to recital 7, in the case of public communications networks, specific legal, regulatory and technical provisions should be made in order to protect the fundamental rights and freedoms of natural persons and the legitimate interests of legal persons, in particular with regard to the increasing capacity for automated storage and processing of data relating to subscribers and users.

---

[91] See the Article in the previous footnote.
[92] See the Article in footnote 90.

In the Preamble it is mentioned that with the advent of new advanced digital technologies in public communications networks within the Community, specific requirements concerning the protection of personal data and privacy of the user are being raised. The development of the information society is characterized by the introduction of new electronic communications services. Access to digital mobile networks has become available and affordable for a large public. These digital networks have great capacities and possibilities for processing personal data. The successful cross-border development of these services is partly dependent on the confidence of users that their privacy will not be at risk. This is particularly important for the so-called location-based services (LBSs), on which the e-Privacy Directive focuses.

6.4.2 Location-based services

These services, introduced in the Directive as 'value added services', refer to any service which requires the processing of traffic data or location data other than traffic data beyond what is necessary for the transmission of a communication or the billing thereof (Art. 2(g)). As explained in recital 15 of the Directive, traffic data may include any translation of the communication information – that is, any naming, numbering or addressing information provided by the sender of a communication or the user of a connection to carry out the communication – by the network over which the communication is transmitted for the purpose of carrying out the transmission. Location data may refer to the latitude, longitude and altitude of the user's terminal equipment, to the direction of travel, to the level of accuracy of the location information, to the identification of the network cell in which the terminal equipment is located at a certain point in time and to the time the location information was recorded.

In order to perform their task, location-based services require processing of location data. Basically, according to the given definition, this refers to any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service. In simple terms, the relation is such that in digital mobile networks, location data giving the geographic position of the terminal equipment of the mobile user are processed to enable the transmission of communications. And such data are traffic data covered by the Directive (recital 35). Very often, digital mobile networks may have the power to process location data more precisely than is necessary for the purpose of transmission of communications. Accurate data like that is used for the provision of value added services such as, for example, services providing individualised traffic information and guidance to drivers. For these services to be allowed, the consent of the subscriber is obligatory. Furthermore, even after giving their consent, subscribers should be permitted, in a way that is easy and free of charge, to temporarily or permanently object to the processing of location data (recital 35).

6.4.3 Confidentiality of communications

Another important regulation provided by the e-Privacy Directive concerns confidentiality of communications. As stated in the Preamble (recital 21), measures should be taken to prevent unauthorised access to communications. The reason is the protection of the confidentiality of communications, including both the contents and any data related to such communications, by means of public communications networks and publicly available electronic communications services. Article 5 of the Directive calls on Member States to ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. Particularly, they should prohibit listening, tapping, storage or other kinds of interception or surveillance of

communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorized to do so in accordance with Article 15(1). However, this stipulation should not prevent technical storage, which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.

6.4.4 SPAM

The e-Privacy Directive also introduces a provision on unsolicited communication that could be of relevance to social network sites and collaborative workspaces. The aim of the regulation is to protect subscribers from intrusions on their privacy by any form of spam, which may impose a burden and/or cost on the recipient. Additionally, the Preamble of the Directive explains that for the purpose of the harmonization of the single market a common approach to ensure simple and consistent Community-wide rules is necessary. Article 13 replaced Article 7 of the e-Commerce Directive and it states that the use of automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may only be allowed with respect to subscribers who have given their prior consent. However, when a customer provides his electronic contact details for electronic mail, when purchasing a product or a service, the same natural or legal person who provided the product or the service may use these electronic contact details for direct marketing of its own similar products or services. It is possible under the condition that customers are clearly and distinctly given the opportunity to object to this practice, free of charge and in an easy manner. There is no need to prevent such communication in case of an already existing customer relationship, as it may result in providing the service desired by the customer in a better and faster way. Apart from these provisions, spam that is free of charge is not allowed either without the consent of the subscribers concerned or in respect of subscribers who do not wish to receive these communications. The choice between these options should be determined by national legislation. In any case, sending spam that disguises or conceals the identity of the sender, or without a valid address to which the recipient may send a request that such communications cease, shall be prohibited. The goal of this rule is to facilitate the effective enforcement of Community rules on spam.

6.5 The Data Retention Directive (2006/24/EC)

The Data Retention Directive is another EU piece of legislation with a possible impact on social networks sites and collaborative workspaces. Its scope, described in Article 1(1), is to ensure that traffic and location data will be available for the purpose of investigation, detection and prosecution of serious crimes. The crimes to which the retained data will be applicable are not explicitly mentioned in the Directive and should be defined by each Member upon the implementation of the Directive into national law. The list of crimes should be kept consistent, therefore, to prevent a completely different interpretation of the term 'serious crime' the European Council urged the Member States to have due regard to the crimes listed in Article 2(2) of the Framework Decision on the European Arrest Warrant[93] and crimes involving telecommunication[94].

[93] Council Framework Decision on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA) (13 June 2002).
[94] Council of the European Union, Statements, Council doc. 5777/06 ADD 1 (10 February 2006), available at http://register.consilium.eu.int/pdf/en/06/st05/st05777-ad01.en06.pdf [last accessed on 17 February 2010].

6.5.1 The scope of the Data Retention Directive

The crucial point of the Directive is that the data shall be retained by the providers of publicly available communications services or public communication networks. As it was shown above, social network sites as such fall into a category of information society services. The same is true of mobile social networks. These still fall under the definition of an information society service, apart from the fact that they use location based service applications to operate. It is important to realize that, in this case, provision of a social network and provision of a location-based service will be considered as two separate activities falling under two separate regimes. Since social network sites are not considered to be electronic communication services in general, the rules on data retention will not apply to them. However, if the social network site provides additional functionalities which constitute 'electronic communications services', the provider will have to comply with the Data Retention Directive as well. The same goes for collaborative workspaces. To prevent any ambiguities, an analysis of a particular social network service or collaborative workspace under discussion should be recommended. Such a solution seems to be a safe approach that would allow assessing the character of each specific social network site or collaborative workspace – an action that is necessary in order to determine whether a provider of that web 2.0 environment should comply with the Data Retention Directive. If the answer to such a question is positive, basic rules of data retention will be presented in the next part of this chapter.

6.5.2 Data to be retained

There are specific categories of traffic and location data that need to be retained, as well as data necessary to identify a subscriber or registered user. Content data shall not be retained. Moreover, traffic data relating to web browsing are not to be retained, since when it comes to internet data, the directive only asks for the retention of data relating to internet access, internet e-mail and internet telephony. Even though no content data may be retained, the question about what is to be done with regard to traffic data that can reveal private information about individual users remains vital.

Article 5 of the Directive provides a detailed list of the categories of data to be retained. They are summarised in the table below.

Categories of data to be retained:
Data necessary to trace and identify the *source* of a communication
Data necessary to identify the *destination* of a communication
Data necessary to identify the *date*, *time* and *duration* of a communication
Data necessary to identify the *type* of communication
Data necessary to identify users' *communication equipment* or what purports to be their equipment
Data necessary to identify the *location* of *mobile* equipment

Table 12: Which data must be retained, according to the Data Retention Directive?

It should be noted that Article 3(2) of the Data Retention Directive clarifies that not all the data that fall under the abovementioned categories have to be retained, but only those that are generated or processed and stored (as regards telephony data) or logged (as regards internet data) by providers of publicly available electronic communications services or of a public communications network within their jurisdiction in the process of supplying the communication services concerned. This solution leads to the idea that complying with the Directive will not require any extra effort from the provider. Such an impression may appear due to the fact that the Directive calls for the retention of data that are already generated or processed in the process of supplying their communications services (Art. 3(1) DRD) by the providers. However, according to Article 6 of the e-Privacy Directive, presently the providers are obliged to retain data necessary mainly for billing purposes.

The retention *period* provided in the Directive (Article 6) should be not shorter than 6 months and not longer than 2 years from the day of the communication. In the end, the retention period within a particular Member State will depend on the choice made during introduction of the Directive into national law.

6.5.3 Provision to authorities

The retained data shall be provided only to the competent national authorities in specific cases and in accordance with national law. To avoid confusion regarding which authorities fall under the term 'competent national authorities' Article 29 Working Party proposed the creation of a list of designated law enforcement services that should be made public.[95] Such a clarification seems to be necessary as the list of authorities within different countries varies strongly. For example, in France the access to data is allowed only to judicial authorities and the police, while in the UK the number of official bodies with permission to such access is much bigger (Pimenidis and Kosta, 2008).

6.5.4 Security

Security obligations that are imposed on the providers in the Data Retention Directive are very rigorous. To be retained, the data do not need to be of evidential quality, but they shall be of the same quality and subject to the same security and protection as those data on the network. Moreover, the data shall be subject to appropriate technical and organizational measures to protect them against accidental or unlawful destruction, accidental loss or alteration, or unauthorized or unlawful storage, processing, access or disclosure. Additionally, appropriate measures shall be taken in purpose of ensuring that they can be accessed solely by specially authorized personnel. Finally all other data shall be destroyed at the end of the period of retention – except, of course, those that have been accessed and preserved. The deletion of data should occur upon expiration of the retention period chosen in the national legislation. It is clear that the data should be stored in such a way that will allow their transmission upon request to the competent authorities, without delay. To summarize, it should be said that the storage of the data, their authenticity, accuracy and security, for the prevention of loss of the data as well as for their timely and proper transmission to

[95] Opinion 3/2006 on the Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (25 March 2006), available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp119_en.pdf [last accessed on 17 February 2010].

the competent authorities is all the responsibility of the provider. As the Directive does not describe the way of transferring of the retained data to the competent authorities, the European Telecommunications Standards Institute (ETSI) prepared a document on the 'Handover Interface for the request and delivery of retained data' (ETSI, 2007).

6.6 The e-Commerce Directive (2000/31/EC)

Another piece of legislation vital for legal analysis of social network sites and collaborative workspaces is the e-Commerce Directive. First, it should be emphasized that the e-Commerce Directive does not apply to issues relating to information society services covered by the Data Protection Directive and the e-Privacy Directive (Art. 1(5)(b)). As we explained above these two Directives constitute a legal framework for the Community data protection. This means that providers of information society services that fall within the scope of these Directives have an obligation to fully comply with them. These issues will not be addressed here again.

6.6.1 Applicable law

Another interesting point that should be raised in light of the discussion on the e-Commerce Directive and social network sites and collaborative workspaces is the 'country of origin principle' and the exceptions it allows for when dealing with consumers. As explained in recital 22, information society services should be supervised at the source of the activity – that is, the country of origin –, in order to ensure an effective protection of public interest objectives. Further on, recital 22 says that in order to effectively guarantee freedom to provide services and legal certainty for their suppliers and recipients, such information society services should in principle be subject to the law of the Member State in which the provider is established. To simplify, the principle states the a service provider has to fulfil the requirements that are regulated in the country of his establishment. The introduction of the principle caused some intense discussions[96], which resulted in the agreement that under certain circumstances – for example if consumers are involved – the freedom of providing information society services should be restricted. Due to a greater need for consumers' protection, the regulation was adjusted to stay in line with the Rome convention[97] and its Article 5[98], which introduced a country of destination principle. In effect, in

[96] Public hearing in Brussels, November 1999.
[97] Rome Convention of 1980 on the law applicable to contractual obligations.
[98] Article 5 of Rome Convention on certain consumer contracts reads: (1). This Article applies to a contract the object of which is the supply of goods or services to a person ('the consumer') for a purpose which can be regarded as being outside his trade or profession, or a contract for the provision of credit for that object. (2). Notwithstanding the provisions of Article 3, a choice of law made by the parties shall not have the result of depriving the consumer of the protection afforded to him by the mandatory rules of the law of the country in which he has his habitual residence: - if in that country the conclusion of the contract was preceded by a specific invitation addressed to him or by advertising, and he had taken in that country all the steps necessary on his part for the conclusion of the contract; or - if the other party or his agent received the consumer's order in that country; or - if the contract is for the sale of goods and the consumer travelled from that country to another country and there gave his order, provided that the consumer's journey was arranged by the seller for the purpose of inducing the consumer to buy. (3). Notwithstanding the provisions of Article 4, a contract to which this Article applies shall, in the absence of choice in accordance with Article 3, be governed by the law of the country in which the consumer has his habitual residence if it is entered into in the circumstances described in paragraph 2 of this Article. (4). This Article shall not apply to: (a) a contract of carriage; (b) a contract for the supply of services where the services are to be supplied to the consumer exclusively in a country other than that in which he has his

Article 3 (3) of the e-Commerce Directive contractual obligations concerning consumer contacts are excluded from its scope. This means that for contracts concluded electronically a consumer may apply the law of his home country (Lodder and Kaspersen, 2002: 11). Recital 55 of the Directive explains, to support such opinion, that the regulations of the Directive do not affect the law applicable to contractual obligations relating to consumer contracts; accordingly, the Directive cannot have the result of depriving the consumer of the protection afforded to him by the mandatory rules relating to contractual obligations of the law of the Member State in which he has his habitual residence. Of course, we have to bear in mind that for most social network sites and collaborative workspaces, their Terms of Use (ToU) will contain a provision on applicable law, which will not allow for differentiation according to the consumer's country. For example, in its Terms of Use (recently renamed 'Statement of Rights and Responsibilities') Facebook declares: "*You will resolve any claim, cause of action or dispute ("claim") you have with us arising out of or relating to this Statement or Facebook exclusively in a state or federal court located in Santa Clara County. The laws of the State of California will govern this Statement, as well as any claim that might arise between you and us, without regard to conflict of law provisions. You agree to submit to the personal jurisdiction of the courts located in Santa Clara County, California for the purpose of litigating all such claims*"[99]. In Netlog's Terms of Use, it is Belgian law, also without regard to its conflicts of law provisions.[100] This particular problem is an issue of an international private law and the rules on conflicts of law. Also a discussion on the enforceability of Terms of Use or End User License Agreements is required. This will be done in section 6.8.1.

6.6.2 Liability of Internet Service Providers (ISPs)

Other provisions of the e-Commerce Directive important for social network sites and collaborative workspaces are contained in Articles 12, 13, and 14 and they cover the liability of intermediary service providers. The e-Commerce Directive distinguishes between levels of liability based on the type of service that is being provided. In case of mere conduit, where the role of the provider is solely a passive transmission of the information, or provision of access to a communication network, the provider is not held liable if he doesn't initiate the transmission, doesn't select the receiver of the transmission and, additionally, he doesn't select or modify the information contained in the transmission. It is clarified that the above-mentioned acts consist of automatic, intermediate and transient storage, which means that the information cannot be stored for longer than reasonably necessary for the transmission. Therefore, from the side of the provider of the service, there is neither knowledge nor control over the transmitted or stored information. Such service is often compared to postal services, which cannot be held liable because of letters or packages containing illegal material (Lodder and Kaspersen, 2002: 67-93). This particular provision is not applicable to social network sites and collaborative workspaces since providers of these services store the acquired information for much longer than described above.

Article 13 of the e-Commerce Directive addresses providers of caching services. It covers liability regarding copies that are stored only temporarily and, similar to the case of mere conduit, in an automatic, intermediate and a transient way. Although in this case the storage is longer and its purpose is to make the transmission of information delivered at the request of recipients more efficiently, it does not apply to social network sites or collaborative workspaces, which, in order to perform their tasks, have to store the data for the entire duration of the relation between the user

---

habitual residence. (5). Notwithstanding the provisions of paragraph 4, this Article shall apply to a contract which, for an inclusive price, provides for a combination of travel and accommodation.

[99] See http://www.facebook.com/terms.php?ref=pf [last accessed on 17 February 2010].

[100] See http://en.netlog.com/go/about/legal/view=general [last accessed on 17 February 2010].

and the provider of the service. A provider of a caching service is not liable on the condition that he does not modify the information, complies with conditions on access to the information, complies with rules regarding the updating of the information, and does not interfere with the lawful use of technology to obtain data on the use of the information. Moreover, a caching provider is obliged to promptly remove or disable access to information if he obtains knowledge that the information at the initial side of the transmission has been removed from the network, or the access has been disabled, or that a court or an administrative authority has ordered such removal or disablement.

According to Article 14 of the e-Commerce Directive, hosting services consist in the storage of information provided by the recipient of the service. This is exactly what is happening in the web 2.0 environments under scrutiny in this deliverable, and especially in the case of social network sites fed with information by their users. Such information is stored for the length of time in which a user maintains his relation with the service, and sometimes even longer than that. This is definitely not a temporal storage. There are two conditions under which a provider of such a service is *not* held liable. First of all, he cannot have actual knowledge that information or an activity is illegal. Furthermore, he cannot be aware of facts or circumstances from which the illegal activity or information is apparent. The second condition requires that in case of obtaining such knowledge, he will act immediately to remove or block access to such information. This clearly means that if a user of a social network site or a collaborative workspace puts illegal information on his account, the service provider is not liable for any infringement as long as he is not aware of the misconduct. However, this will no longer be the case when somebody informs the provider about the illegal content of the profile. From that point on, the information has to be removed or access must be blocked. The removal or disabling of access, when it's required, has to be undertaken with respect to the freedom of expression and to the procedures established at the national level (recital 46). Moreover, Member States are allowed to introduce specific requirements that shall be fulfilled immediately prior to the removal. There are some concerns about a possibility of an unjustified notice, which would lead to a blockage of information that in fact was never illegal in the first place. That is why the second provision of Article 14 is sometimes found to be quite problematic. Some argue that the fear of providers to be held liable could result in a misuse of this piece of regulation (Lodder and Kaspersen, 2002: 67-93). Moreover, we can imagine a situation in which the provider will find himself trapped in a state where he will have to choose between the following two: on the one hand he could be held liable for not removing the information, and on the other, he could be held liable by the recipient of the service for removing the material that was not at all illegal.

For the issue of the Internet Service Provider (ISP) liability, the crucial aspect is the editorial control over the content. Only the lack of such control allows for exemption provided in the described articles. Otherwise, the situation of ISPs resembles the one of publishers and invites a similar level of liability. Therefore, the main question is whether the ISP "*exercises sufficient editorial control to render it a publisher with the same responsibility as a newspaper for filtering content*" (Bernstein and Ramchandani, 2002). As Bernstein and Ramchandani explain, the discussion is ongoing with case law going into two opposite directions. In European legislation the provision on monitoring is helpful to resolve the question of liability.

6.6.3 Monitoring

It should be emphasized that according to the e-Commerce directive providers do not have a general obligation to monitor the information that is being transmitted or stored (Article 15). They also have no obligation to actively seek facts or circumstances indicating illegal activity. This means that no cyber-patrolling is required from the service providers. The Preamble in recital 47

states clearly that Member States are prevented from imposing such monitoring obligations on service providers, but only with respect to obligations of a general nature. For specific cases, however, this prohibition is not valid. Also, the prevention from the monitoring obligation does not affect orders that could be issued by national authorities to the service providers in accordance with national legislation.

In light of the presented opinion that Internet Service Providers can be exempted from liability only if they do not exercise editorial control over the content, it is worth noting that ISPs are advised to be careful. The accepted opinion is that ISPs that monitor the content on their servers will be treated as publishers of the information. This puts them at greater risk of being held liable.[101] It appears that very often providers consider it safer not to control and monitor the content in order to use the exemptions provided in the Directive.

6.7 The Copyright Directive (2001/29/EC)

The Copyright Directive[102] is relevant with respect to social network sites and collaborative workspaces as well. Its scope is the legal protection of copyright and related rights in the framework of the internal market, with a particular emphasis on the information society. It does not apply to the legal protection of computer programs, rental right, lending right and certain rights related to copyright in the field of intellectual property, copyright and related rights applicable to broadcasting of programmes by satellite and cable retransmission, the terms of protection of copyright and certain related rights, and the legal protection of databases. As the Copyright Directive covers issues closely related to those from the scope of the e-Commerce Directive, such as liability issues, it should be emphasized that the Copyright Directive is without prejudice to those provisions, i.e. the ones on liability from the e-Commerce Directive.

The Preamble of the Directive, in recital 9, states that protection of copyrights helps to ensure the maintenance and development of creativity in the interests of authors, performers, producers, consumers, culture, industry and the public at large. Moreover, in recital 22, it is highlighted that the objective of proper support for the dissemination of culture must not be achieved by sacrificing strict protection of rights or by tolerating illegal forms of distribution of counterfeited or pirated works. Additionally, according to recital 38, Member States should be allowed to provide for an exception or limitation to the reproduction right for certain types of reproduction of audio, visual and audiovisual material for private use, accompanied by fair compensation.

6.7.1 Sanctions and remedies

As for the sanctions, the Directive provides Member States with the right to introduce effective sanctions and remedies for infringements of rights and obligations as set out in the Directive. All necessary measures should be taken to ensure that those sanctions and remedies are applied. The sanctions thus provided for should be effective, proportionate and dissuasive and should include the possibility of seeking damages and/or injunctive relief and, where appropriate, of applying for seizure of infringing material (recital 58).

---

[101] See http://www.out-law.com/page-431 [last accessed on 18 February 2010].
[102] Directive 2001/ 29/ EC of the European Parliament and the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society.

With respect to social network sites and collaborative workspaces, recital 59 is of particular importance. It states that in the digital environment, the services of intermediaries may increasingly be used by third parties for infringing activities. In many cases such intermediaries are best placed to bring such infringing activities to an end. Therefore, without prejudice to any other sanctions and remedies available, right holders should have the possibility of applying for an injunction against an intermediary who carries a third party's infringement of a protected work or other subject-matter in a network. This possibility should be available even where the acts carried out by the intermediary are exempted under Article 5. The conditions and modalities relating to such injunctions should be left to the national law of the Member States. In fact, the possibility described above is very often used by the IP right owners who prefer to sue site owners over the end users, which is generally not economically viable (Osborne, 2008).

6.7.2 User generated content

Social network sites and collaborative workspaces, with their vast amounts of user generated content (UGC), such photographs, text, videos, music or blogs, constitute a major threat in the sense that some of this content will constitute an infringement on rights of copyright holders. In social network sites such as MySpace and Facebook, it is extremely popular to upload content that is not exactly generated by the particular user, for example videos of favourite music bands. Generally, music labels sue the providers of social network sites for the content posted on their sites by users but without permission of the copyright holders. This happened in the suit filed against MySpace by UMG Recordings, which claimed that the popular platform "*encourages, facilitates, and participates in the unauthorized reproduction, adaptation, distribution and public performance*"[103] of copyrighted works. In the suit, plaintiffs actually described the content of MySpace as 'user-stolen' instead of 'user-generated', and claimed to believe that MySpace is "*a willing partner in that theft*"[104]. The Terms & Conditions of MySpace, state that "[b]*y posting any Content on, through or in connection with the MySpace Services, you hereby grant to MySpace a limited license to use, modify, delete from, add to, publicly perform, publicly display, reproduce, and distribute such Content solely on, through or in connection with the MySpace Services, including, without limitation, through the MySpace Services to applications, widgets, websites or mobile, desktop or other services which are linked with your MySpace account (collectively, "Linked Services"), including, without limitation, distributing part or all of the MySpace Services and any Content included therein, in any media formats and through any media channels…* [At the same time,] *MySpace assumes no responsibility for monitoring the MySpace Services for inappropriate Content or conduct. If at any time MySpace chooses, in its sole discretion, to monitor the MySpace Services, MySpace nonetheless assumes no responsibility for the Content, no obligation to modify or remove any inappropriate Content, and no responsibility for the conduct of the User submitting any such Content*"[105]. As for the protection of copyrights specifically, the Terms of Use Agreement stipulates that "*MySpace respects the intellectual property of others, and requires that our users do the same. You may not upload, embed, post, email, transmit or otherwise make available any material that infringes any copyright, patent, trademark, trade*

---

[103] For example: UMG Recordings et al v MySpace Inc. No 06-cv-07361. See: http://www.afterdawn.com/news/archive/8145.cfm, http://news.findlaw.com/hdocs/docs/ip/umgmyspace111706cmp3.html and http://www.jenner.com/files/tbl_s69NewsDocumentOrder/FileUpload500/4094/UMG%20Recordings%20v.%20MySpace.pdf [all sites last accessed on 18 February 2010]. Also see (Osborne, 2008).

[104] See http://news.findlaw.com/hdocs/docs/ip/umgmyspace111706cmp3.html [last accessed on 18 February 2010].

[105] See http://www.myspace.com/index.cfm?fuseaction=misc.terms [last accessed on 16 February 2010].

secret or other proprietary rights of any person or entity"[106]. If users violate this rule, "[i]*t is MySpace's policy to terminate, in appropriate circumstances, the membership of repeat* [sic!] *infringers*"[107].

6.7.3 Rights under protection

The right to reproduction is protected under the regime of the Copyright Directive, through its Article 2. According to its provision, Member States shall provide for the exclusive right to authorize or prohibit direct or indirect, temporary or permanent reproduction by any means and in any form, in whole or in part for authors, for performers, for phonogram producers, for the producers of the first fixations of films, and for broadcasting organizations. Right of communication is protected in Article 3, which reserves the exclusive right to authorize or prohibit any communication of the works to the public for their authors. It is made clear that this provision applies to any communication to the public, by wire or wireless means, including the making available to the public of their works in such a way that members of the public may access them from a place and at a time individually chosen by them, which basically means – on demand. Article 4 of the Directive covers the distribution right. In respect of the original of their works or copies thereof, authors are granted the exclusive right to authorize or prohibit any form of distribution to the public by sale or otherwise. This provision is particularly relevant in case there is a possibility to download copyrighted work from somebody's profile on a social network site, or through publication in a collaborative workspace.

Article 5 of the Directive provides a list of exceptions and limitations to regulations on rights of reproduction and communication to the public. For the subject of social network sites and collaborative workspaces, the most important exception seems to be the one of Article 5 (2)(b), which allows for reproductions on any medium made by a natural person for private use and for ends that are neither directly nor indirectly commercial, on condition that the right holders receive fair compensation, which takes account of the application or non-application of technological measures.

6.8 Specific problems in social network sites

In the remainder of this chapter we will discuss a number of particular legal problems that are relevant for social network sites. While some of these may also apply to collaborative workspaces, we have chosen to focus on social network sites alone, due to the (legal) complexity of these environments and the fact that users are explicitly invited to share personal data on social network sites.

6.8.1 Terms of Use

When registering for a social network site, before actually receiving the service, the user has to give his consent to the Terms of Use and the privacy policy. Offering and accepting the service creates a contractual relationship between the user and the provider of the service. Accepted

[106] See the previous footnote.
[107] See footnote 105.

Terms of Use and privacy policies constitute part of the contract. Such contracts are always subordinate to mandatory regulations. This means that even though the Terms of Use are drawn unilaterally by the providers of these services, without any power of the user to negotiate on the provisions (Edwards and Brown, 2009: 15), they will not be absolutely dependent on the wish of providers.

Together, the Terms of Use (ToU) and the End User License Agreement (EULA) are a kind of shrink-wrap or 'click-wrap' agreement in which the 'I accept'-button has to be clicked in order to receive the service. Such situations, in which one of the parties has a much stronger bargaining power and imposes contract terms on the other party, can be typically seen in contracts of adhesion (Edwards and Brown, 2009: 19).

When signing up for a social network site, the user will have to accept a contract with sometimes interesting provisions, or otherwise the service will not be delivered. For example, when accepting Facebook's Terms of Use, the user agrees that Facebook "*If you violate the letter or spirit of this Statement, or otherwise create possible legal exposure for us, we can stop providing all or part of Facebook to you. We will notify you by email or at the next time you attempt to access your account*"[108]. Violations include being under 13 years of age or being a convicted sex offender.

Of course, as with most Terms of Use and End User License Agreements, the user must accept the fact that the provider waives all types of responsibility. For example (spelled in capitol letters): "*WE TRY TO KEEP FACEBOOK UP, BUG-FREE, AND SAFE, BUT YOU USE IT AT YOUR OWN RISK. WE ARE PROVIDING FACEBOOK "AS IS" WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. WE DO NOT GUARANTEE THAT FACEBOOK WILL BE SAFE OR SECURE. FACEBOOK IS NOT RESPONSIBLE FOR THE ACTIONS, CONTENT, INFORMATION, OR DATA OF THIRD PARTIES* […]. *WE WILL NOT BE LIABLE TO YOU FOR ANY LOST PROFITS OR OTHER CONSEQUENTIAL, SPECIAL, INDIRECT, OR INCIDENTAL DAMAGES ARISING OUT OF OR IN CONNECTION WITH THIS STATEMENT OR FACEBOOK, EVEN IF WE HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. OUR AGGREGATE LIABILITY ARISING OUT OF THIS STATEMENT OR FACEBOOK WILL NOT EXCEED THE GREATER OF ONE HUNDRED DOLLARS ($100) OR THE AMOUNT YOU HAVE PAID US IN THE PAST TWELVE MONTHS*"[109].

Apart from that, the Terms of Use usually state that they can be modified at the discretion of the service provider. For instance, Facebook's Terms of Use Agreement reads that they "*can change this Statement if we provide you notice (by posting the change on the Facebook Site Governance Page)…*". In its latest version Facebook added the phrase "*…and an opportunity to comment*", probably in light of the public outcry that previous versions of the ToU have generated.

Also, the Terms of Use of many social network sites stipulate that the continuous use of the service constitutes user's agreement. For instance, in its Terms of Use MySpace provides that it "*may modify this Agreement from time to time and such modification shall be effective upon posting by MySpace on the MySpace Website.* […] *Your continued use of the MySpace Services following any such modification constitutes your agreement to be bound by and your acceptance of the Agreement as so modified*"[110].

Due to these factors the enforceability of such Terms of Use and End User License Agreements is sometimes questioned before the court. However, depending on the court, the outcome may be different. Some courts have declared such shrink-wrap license agreements to be invalid. This

[108] See http://www.facebook.com/terms.php [last accessed on 17 February 2010].
[109] See the previous footnote.
[110] See http://www.myspace.com/index.cfm?fuseaction=misc.terms [last accessed on 16 February 2010].

decision builds on the fact that ToUs and EULAs are in fact contracts of adhesion, and courts have declared them unconscionable and/or unacceptable. Other courts have determined that the shrink-wrap license agreement is valid and enforceable. However, no court has ruled on the validity of EULAs generally – decisions are limited to particular provisions and terms.

6.8.2 Tagging

The concept of tagging was already introduced in section 6.2.2 above, when we discussed the complication surrounding the role of the data controller, but it is a phenomenon that merits some attention in its own right. Tagging photographs is one of the features offered by many social network sites, but the most famous provider allowing it is Facebook. It enables 'signing' the pictures with the names of people that appear on them but also with additional metadata such as a link to their social network site profile or e-mail address (Hogben, 2007: 10). What is particularly relevant is that anyone with a Facebook account can add tags, not just the data subjects themselves. However, no consent of the person being tagged is required. This leads to situations in which users can put compromising pictures of somebody else on his profile, and additionally explicitly mention the name of the depicted person. It has become a common practice among the users of Facebook to go through the profiles of their 'friends' and to see if they should de-tag themselves anywhere after every event that might have resulted in 'inappropriate' pictures. In July 2008 Lisa Guernsey of *The New York Times* wrote: "*De-tagging — removing your name from a Facebook photo — has become an image-saving step in the college party cycle. 'The event happens, pictures are up within 12 hours, and within another 12 hours people are de-tagging,' says Chris Pund, a senior at Radford University in Virginia.*" (Guernsey, 2008).

The data subject of this activity can de-tag pictures about him or her, but only if he is a member of Facebook as well. This is very important since it allows other Facebook users to respond to tags and remove them from the picture, but it does not grant the same possibility to non-users, outsiders who deliberately chose not to participate in this social network site. Such non-users will get an e-mail notifying them of the fact that they have been tagged (if their e-mail address is provided by the person tagging them!), but they will only be able to de-tag the picture after registering to the service themselves. The e-mail will provide them with a link to the tagged picture, which is a recent change. The Facebook Help Center states: "*You can tag anyone in a photo, regardless of whether they have a Facebook profile. While tagging your photos, if you type in the name of someone who is not on your Friend List, you have the option of listing their email address. When you are done tagging, they will receive an email that provides a link to the image. They will be able to see the photos in which they are tagged, but nothing else on the site unless they register*"[111].

Previously, it wasn't even possible to see the picture without registering. Note that if the user who tags a non-user does not provide an e-mail address of this non-user, the latter may never find out about it.

Another interesting point is that the data subject can de-tag himself on a picture or video if he is a member of the social network site as well, but he or she cannot remove the picture or video from somebody else's profile entirely. For instance, on the question of how to remove a video in which a users appears against his will or without his consent the Facebook Help Center says: "*View the video and click the 'remove tag' link next to your name. It will no longer be linked to your profile.* […] *If you are having problems with someone constantly tagging you in embarrassing videos, just remove them as a friend… If you don't want the video to be shown at all, please talk to the person*

[111] See http://www.facebook.com/help/?faq=12562 [last accessed on 18 February 2010].

who posted it. They should be respectful enough to remove unwanted videos. Unfortunately, Facebook CANNOT make people remove videos that do not violate our Terms of Use"[112].

Note that there is a possibility to adjust the default settings in such a way that it becomes impossible to be tagged by third parties. However, the problem with this option is that it is deeply hidden in privacy settings, which means that most of users never even manage to discover it.[113] Those who do, ignore it most of the time (Edwards and Brown, 2009: 13). We can conclude that, without a doubt, the practice of tagging in social network sites greatly facilitates violating privacy of others. It is no longer enough for users to be careful with what images they post on a social network site, they also have to keep in mind that their privacy might be endangered by others (Hogben, 2007: 10).

6.8.3 Private or public space?

The amount of highly personal data revealed by users on social network sites is enormous, as we have discussed several times in previous chapters. The majority of the user profiles contain data ranging from birth names, addresses, phone numbers, and pictures to 'sensitive' data such as sexual preferences, relationship status, political views, and health information (Gross and Acquisti, 2005). As we have seen above, users often do not realize that this information could be accessed by their parents, teachers, and many others. It appears that some users are still not aware of just how public their profile can be. Media coverage of privacy violations in social network sites has increased in recent years, and hence the privacy awareness of most users has changed as well. However, there are plenty of instructive cases reporting the behaviours of users of social network sites that show just how fragile this awareness still is.

In July 2007 proctors of Oxford University turned to Facebook to look for evidence of students breaking the University's disciplinary rules (Edwards and Brown, 2009). They found a vast amount of pictures taken during post-exam parties, many of which could easily be called 'compromising'. In consequence, a number of disciplinary sanctions were taken. This incident shocked many students – they considered it to be an outrageous intrusion into their privacy.

Another case involved a student who lost an opportunity for a summer internship after the president of the company saw his Facebook profile, in which he claimed that one of his interests was "*smokin' blunts*" (Finder, 2006). Yet another one involved a participant of a beauty pageant, who was blackmailed by someone who threatened to send her racy pictures, taken from her private Facebook album, to the contest officials unless she surrendered the crown (Fenner, 2007). As we have seen in earlier chapters, it has become a generally acknowledged practice for future employers to check the social network site profiles of job applicants before hiring them. Other institutions and organisations have started doing the same, for instance universities screening students before admission (Shepherd and Shariatmadari, 2008), police officers have started looking for information on social network sites profiles (Aleo-Carreira, 2009), and tax authorities control job descriptions and compare them with tax declarations (McDonagh, 2008).

All these cases lead to the (legal) question of whether social networks sites constitute 'private' spaces, in which a reasonable level of privacy could be expected, or 'public' spaces, in which there is no place for such expectations (Edwards and Brown, 2009). As we have seen in Chapter 5 users tend to believe that everything they post on their profile page can only be accessed by their

---

[112] See http://www.facebook.com/help/?faq=12419 [last accessed on 18 February 2010].

[113] The editors of this document put considerable effort into finding this option in early February 2010, but were unable to locate it in the current version of Facebook. This could mean one of two things: (1) the option is, in fact, very, very well hidden; or (2) it has been removed. We cannot be certain which of the two is the case.

intended audience (Grimmelmann, 2008). Despite the fact that users provide considerable amounts of personal information themselves, they expect their privacy to be protected from invasions. This phenomenon is known as the 'privacy paradox' (Barnes, 2006; Norberg *et al.*, 2007). It appears to be extremely difficult to assess the default level of privacy protection that users should be able to expect or demand (Edwards and Brown, 2009).

The answer to a lot of problems appears to be in privacy settings. These can be adjusted by users in social network sites, which could eliminate a certain amount of unwanted disclosures. However, as indicated by Gross and Acquisti in their study, very few users decide to change their privacy preferences (Gross and Acquisti, 2005). Some of them are not even aware that it's possible.

From the legal point of view, it should be noted that the validation for privacy violations in social network sites depends on the type of profile and on what is being done with the collected information. If information was acquired from a profile that was set to 'public', normally there would be no problem with lawfulness of such an action. However, if the profile or information on it were set to 'friends only', with access strictly limited to a defined group of people, the legality of the action could be questioned. Apart from that, it seems that there would be no problem with the initial gathering of information, for example for forensics, from every available source, also a public profile on social network site. However, it is unclear whether such information could be used as evidence later on. That would also depend on the type of information. In some court cases pictures that had been found on Facebook, and that proved that a crime was committed by the person standing trial, were accepted by the court and, in effect, lead to a conviction (Perez, 2007).

To conclude this section, it should be noted that the users of social network sites have considerable power over the access to their profile pages. Adjusting the privacy settings to their profile pages can result in improving privacy protection. Therefore, the ENISA Position Paper recommends that users should be educated about (among other things) (1) the fact that the size and type of audience may be different than in offline circle of friends, (2) that images can give away private data as well, especially when tagged with metadata, and (3) that profile information may appear in search results even when believed to be private (Hogben, 2007).

6.9 Concluding thoughts

This chapter presented an overview of the existing legal framework regarding social network sites and collaborative workspaces and discussed some important legal issues that arise with respect to this new, budding type of online environment. However, it goes without saying that many questions still remain. Moreover, with the current pace of technological development, new ones will keep appearing. Providers of social network sites (and, to a lesser degree, collaborative workspaces) keep offering new functionalities and applications, which may have a strong impact on the privacy of users, as was evidenced, for instance, in the case of picture tagging in social network sites. Apart from practical problems that they may cause in the everyday lives of users, they also raise questions of a legal nature. The problem of data control and mainly the question whether such control could be attributed to users is one of the main issues regarding the protection of personal data in Europe. This question could also have an impact on how European courts may address future conflicts as these may that arise in the context of social network sites and collaborative workspaces. The long-debated issue of the applicability of EU data protection law becomes crucial with respect to these new web 2.0 environments. Due to the lack of boundaries on the internet and the increasing number of available services originating from other countries, assigning the correct law is not always an easy task. According to the Article 29 Working Party, however, the use of cookies on the terminal equipment of European users implies the applicability of the European data protection legislation to both social network sites and collaborative

workspaces. Therefore, with respect to both of these web 2.0 environments it seems that European users will be protected most of the time, based on this reasoning.

Furthermore, with respect to social network sites, the qualification of these sites as an 'information society service' or an 'electronic communication service' might cause additional problems. A social network site as such fulfils the criteria of the former, but things get more complicated due to the extensiveness of extra services offered. The only solution that seems to provide a correct answer is a careful analysis of each particular social network site under review on a case-by-case basis. Only then can a full picture of a specific social network site be obtained.

Last, the presented analysis emphasized the value of user awareness. It is not possible to tackle the legal problems in relation to social network sites or collaborative workspaces without the cooperation and willingness of the users. Educating users should be undertaken by corporate and political decision-makers, as well as social network site providers. The PrimeLife project has also contributed in this education process, by developing its own alternative social network site, called Clique, in which users find a number of tools to control and protect their privacy, and its own tools for privacy management in a collaborative workspace, phpBB, as well. These demonstrators that we have developed to contribute to a privacy-enhanced web 2.0, will be discussed in the next chapter.

Chapter 7

Towards a privacy-enhanced web 2.0

In this deliverable we have looked at two focal technologies within the landscape of web 2.0, viz. collaborative workspaces and social network sites, and we've investigated which issues arise in these domains with respect to privacy and identity management. In the PrimeLife project we attempt to turn our analysis of issues such as these in existing online environments into demonstrators that may help provide solutions for (some of) them. Thus, in response to and based on the findings that we have presented in the first six chapters of this deliverable we have set out to build three different demonstrators, which we will discuss in this chapter. Each of these focuses on a different set of issues and/or applies to a different web 2.0 domain. In the table below we introduce the three demonstrators, their domain of application and the key issues that they set out to solve. In this chapter we will discuss these demonstrators in detail.

Demonstrator:	**Area of application:**	**Key contributions:**
1. The phpBB extension	Collaborative workspaces: specifically, phpBB forum software.	a. providing users with fine-grained, privacy-respecting access control; b. safeguarding contextual integrity in forums
2. Clique	Social network sites	a. providing users with the option to create their own 'collections' in which social contacts can be clustered; b. providing users with the option to create multiple 'faces' to mimic the practice of audience segregation in real life; c. providing users with fine-grained

Demonstrator:	Area of application:	Key contributions:
		options to define the accessibility of their postings and content in social network sites, thus mimicking the rich and varied texture of relationships in real life.
3. Scramble!	Social network sites and collaborative workspaces	'Scrambling', i.e. encrypting, any message sent from one user to another in social network sites or collaborative workspaces, thus protecting users from either providers or third parties accessing their content.

Table 13: The three demonstrators in WP1.2.

7.1 Contextual integrity in collaborative workspaces: The phpBB extension

As we have seen in Chapter 4, the content of collaborative workspaces that is created by users may contain personal data in the sense of personal information, personal ideas, thoughts and personal feelings. Think, for instance of posts in a forum, in which users share personal thoughts on a given topic. In contrast to explicit profiles in which, for example, the date of birth is a specified data item ('date of birth: 22 February 1980'), the same personal information can be stated in a forum post that says 'I got a new car for my 30th birthday yesterday!' and that is automatically tagged with the date of writing (23 February 2010). In the latter case, it may not be immediately obvious to the user that she has disclosed her date of birth on the internet.

From a privacy perspective, the disclosure of personal data in collaborative workspaces is critical, yet from a social perspective such disclosure is fundamental, since the exchange of information, both personal and non-personal, is the key feature of this kind of environment and the reason why people use it. Hence, when building an extension for more privacy-friendly participation in a collaborative workspace, it was not our objective to prevent the disclosure of personal data in collaborative workspaces per se. Rather, we aimed at increasing people's awareness with respect to their privacy and at enabling them to more selectively specify to whom they want disclose their data.

As we have shown in Chapter 4, the access settings of currently available forums are specified by the provider (including its technical administrators and moderators), and cannot be changed by individual users of these forums. Thus, the user can only decide to disclose information to the groups specified by the provider – and in the worst case, this means disclosing to the public at large – or, alternatively, not to disclose anything at all. Since the first option is not preferable from a privacy perspective and the second option is not preferable from a social perspective, our objective was to develop a *user-controlled selective access control system* for collaborative workspaces. The user should be able to decide who has access to her contributions. That is, a user who wants to share her happiness about her birthday present with some other users (for instance,

other owners of the same brand of cars) should be able to specify appropriate access control rules to her post in the forum. Users should be able to protect their privacy through safeguarding their contextual integrity: information that is disclosed before an intended audience, should not spill over into other contexts and hence possibly have damaging consequences.

With the prototype we have built we aim at demonstrating in which way an existing collaborative workspace application can be extended with privacy-enhancing functionality while preserving the main principles of the original system. We have chosen to build an extension for the popular forum software phpBB (version 3.0.4), which was also part of our analysis of privacy issues in Chapter 4 (see section 4.4). The phpBB software is available with a so-called 'copyleft license'[114] and is developed and supported by an Open Source community [php]. With respect to the technical realization of our selective access control extension, we have relied on mechanisms (credentials, access control policies) that were previously developed in the PRIME project, mainly with a focus on user-provider-scenarios, and have investigated whether they are also applicable in an existing forum platform as an instance of a collaborative workspace application.

Besides the development of purely technical means, we repeat that it is also necessary to sensitize the users of collaborative workspaces with respect to privacy in order to find a comprehensive solution. Therefore, as a central goal in the direction of privacy-enhancing access control for collaborative workspaces we aimed at raising awareness of the issue in users. Therefore, in cooperation with Work Package 2.2 we also integrated a tool that supports the privacy-awareness of forum users in the demonstrator.

The prototype that we have developed fulfils two purposes. First, it serves as a proof-of-concept, that is, the implementation demonstrates that it is feasible to extend an existing application for collaborative workspaces with a component for privacy-enhancing and fine-grained access control. Second, the prototype is also an instrument to collect data from (real) users in order to address further research questions.

For the prototype, we have relied on a forum that allows users to participate without the need for registration, but to contribute under a unique pseudonym. Users do not posses explicit member profiles in phpBB. However, different posts from the same user are linkable and we have investigated how to protect such contributions that contain personal data (that is, personal information, expressions of thoughts and feelings from users). As we have argued in earlier chapters of this deliverable, it is important that users themselves can decide what they deem to be sensitive or intimate information, rather than what is evaluated as such by third parties such as lawyers or computer specialists (Adams, 1999). This is why we argue that users themselves need to be given control over the audience to whom they disclose information, and hence need to have access control mechanisms in collaborative workspaces.

7.1.1 Before we begin: A note on terminology in phpBB

In forums content is always structured in a specific way to make it easily accessible, easy to use, and searchable. In this section we discuss the content structures of phpBB platform. The top level of this platform is the forum itself, which is assigned a title and presented to the user when he first enters the platform. The administrator is responsible for managing all general issues of that forum. |The forum is subdivided into *topics* that each address a different subject matters for discussion. Moderators are responsible for assuring compliance of the content with ethical quality in each topic. Thus, they have the possibility to change subjects or content of posts, to lock or even to delete posts.

[114] GNU General Public License (GPL).

Within a topic (or a sub-topic), individual discussions focusing on particular aims are called *threads*. These are created with the submission of a starting *post* to which users can reply by submitting replying post.

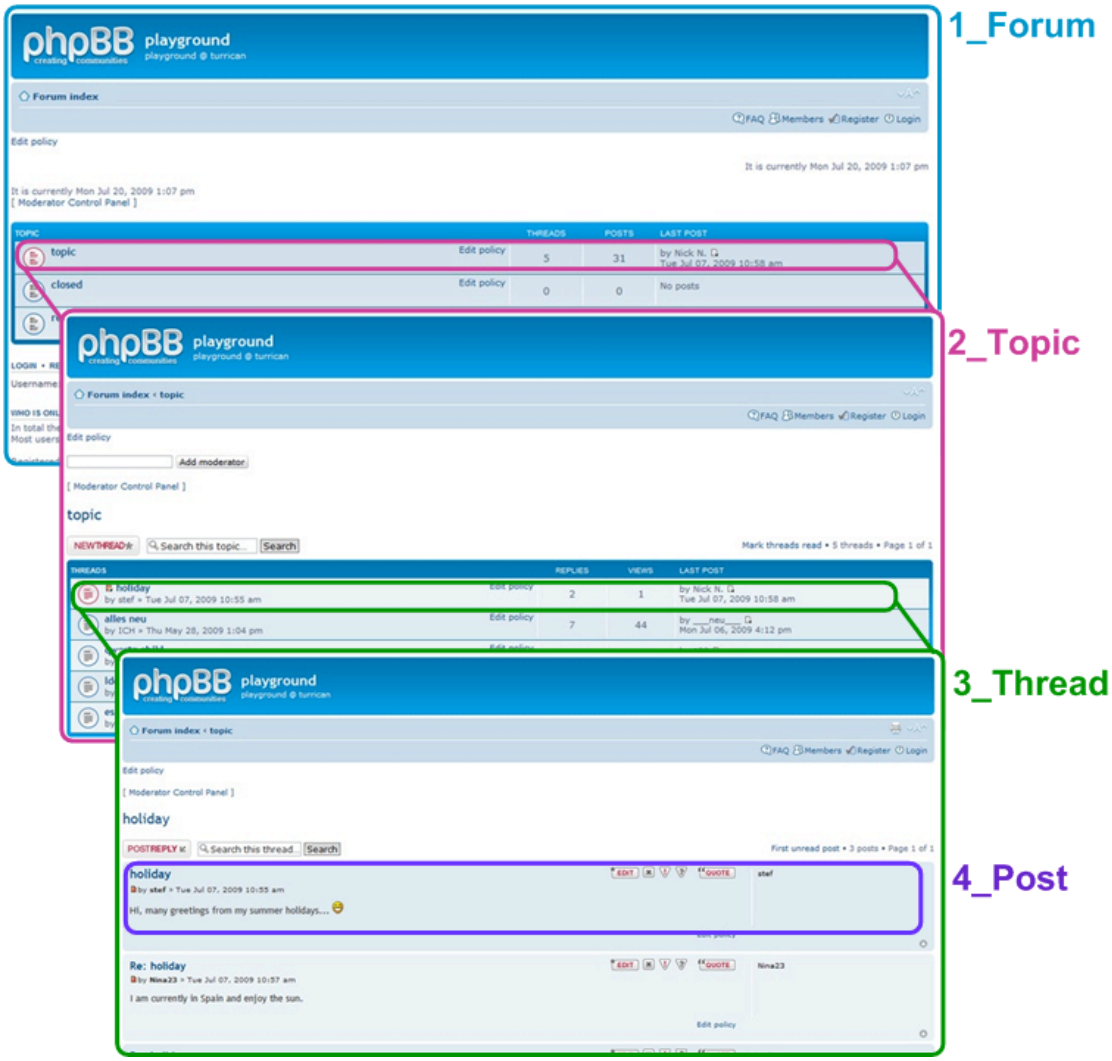


Figure 14: Overview of the hierarchy of a phpBB forum.

7.1.2 Approach to realizing selective access control through the phpBB extension

Selective access control that supports privacy-preservation in collaborative workspaces requires mechanisms that do not base on the knowledge and existence of particular identity information. In such environments, it has to be assumed that people are not required to disclose identifying personal data. Rather, they must prove the possession of a particular property that represents a prerequisite to access a certain resource. As we have seen in Chapter 4 the most common approaches to access control include the access control 'list model', the 'role-based' and the 'group-based' access control approaches. All three require a central instance that defines lists,

roles, or groups based on user names (i.e. identifiers of user accounts) (cf. Pötzsch and Borcea-Pfitzmann, 2010).

However, social and collaborative interaction, such as working on new ideas in a wiki or exchanging experiences or knowledge in forums, does not necessarily require an association of the contacts by their names, but by particular properties. To give an example, someone sets up a wiki dealing with research questions addressing the field of 'Privacy and Identity Management in Social Software Environments'. In this case, it is not possible for this person to assess the real level of expertise of the user authenticating himself as a 'Privacy Expert'. The wiki page owner actually needs to learn if the user who claims to be a privacy expert really possesses the knowledge in order to contribute to the knowledge base on the level of expertise he proclaims to have. For this, that user is required to prove the possession of this knowledge in a way that it is assured. In order to realize such kind of access control, which would be based on *certified properties*, we rely on using access control policies (or ACPs for short) and credentials provided by the PRIME framework.

One of our main objectives while realizing privacy-enhancing selective access control for the phpBB forum was to not to alter the actual functionality of the forum platform. Instead, the add-on we built needed to fit the existing infrastructure. This means that users of the current ('official') release of forum software phpBB should be able to act according to their usual workflows when adding and reading contributions. The add-on we have built provides them with the possibility to selectively specify access rules for postings. These rules are part of ACPs that will be assigned to a contribution (resource) owned by the respective users. The access rules indicate certain attributes a resource requester has to possess.

Accordingly, permissions specified for a resource always relate to certain properties (described as attributes within the assigned ACP), which users (requesters) have to prove they possess in order to get access to this resource. Such properties may be phpBB-related or may be not. That is, a rule in an ACP might ask for a proof of a particular role, for instance 'administrator', 'moderator', 'owner', or 'user', which would be a phpBB-connected property of the user. Also, the rule might indicate that, to get access to the resource, the user needs to be, for example, a citizen of Dresden.

Permissions that should be modelled within the PRIME-enabled phpBB are the following:

- Read contribution;
- Add contribution;
- Edit contribution;
- Delete contribution; and
- Edit policy.

On the one hand, resources for which permissions can be specified using ACPs reside within the different levels of content hierarchy within the forum (see our discussion of this hierarchy in section 7.1.2 and Figure 14). On the other hand, they may also be access control policies themselves, that is:

- Forum;
- Topics;
- Sub-topics;
- Threads;
- Posts; and

- Access control policies.

Initially, each creator of an item of content – that is, a forum, topic, thread, or post – can specify access control policies with respect to this item of content. Additionally, the administrator of the forum has the possibility to define the access control policies for topics and sub-topics. A similar procedure applies to the privileges a moderator has within the topic; the moderator credential which the according user has to possess, that is, a proof of being a moderator, enables this person to read, edit, and delete the according topic as well as all underlying threads and posts, independently from the policy settings a user might make to a resource she owns within that topic.

Table 14 summarizes all of the default rules that are defined for our prototype.

		Right / Privilege				
Level	*Role*	**Read content**	**Create content**	**Edit content**	**Delete content**	**Edit policy**
Forum	**administrator**	X	X	X	X	X
	forum owner	X	X	X	X	X
	user	X	-	-	-	-
Topic	**administrator**	-	-	-	-	-
	topic owner (= moderator)	X	X	X	X	X
	user	X	-	-	-	-
Thread	**administrator**	-	-	-	-	-
	moderator	X	X	X	X	-
	thread owner	X	X	X	X	X
	user	X	X	-	-	-
Post	**administrator**	-	-	-	-	-
	moderator	X	-	X	X	-
	post owner	X	X	X	X	X
	user	X	X	-	-	-

Table 14: Default rules for access control policies in the phpBB extension.

At this point, it is necessary to mention that phpBB originally does not provide the possibility to assign permissions for threads or individual posts. Thus, a solution is required to extend access control to these two levels of the content hierarchy. Three different approaches are possible, all of which have their advantages and disadvantages:

- All processes of access control are adjusted by adding PRIME-related source code and, if required, modifying the original phpBB code;
- All processes of access control are delegated to the according PRIME module (which is the PrimeAuth class), which runs in parallel to the phpBB service. This module recognizes the kind of action that should be conducted and in accordance with those actions it performs the checks of permissions;
- An additional hook being integrated into the phpBB system is developed, which recognizes the kind of action that should be conducted and performs the related checks of permissions.

The biggest advantage of the second and third approaches is that changes or adjustments of the original phpBB code are not required, since access control processes are externalized. However, new modules or at least interconnectors have to be developed, which potentially are prone to errors. In comparison to these, the first option would be a clear-cut solution. However, it would require to open up a parallel version management of phpBB code. Follow-up versions of the original phpBB would have to be adjusted each time a new version of phpBB is released. Since this is not a reasonable way to offer privacy-enhancing access control on a selective way to phpBB users, a combination of the second and the third approach has been realized, which is in the focus of the prototype realization described in this section.

7.1.3 Message exchange between the phpBB extension and the PRIME modules to realize privacy-enhancing access control

In this section we will shortly illustrate the process of message exchange between the client and server components of the phpBB platform and the PRIME framework.

1. The user asks to access a phpBB resource and calls the according web page (for instance, https://example.org/phpBB/posting.php?mode=edit&f=6&p=18). On the client side – i.e. in conjunction with the user's web browser –, a proxy[115] is running, which specifically deals with PRIME-related messages. As the proxy does not know whether the called web page belongs to a PRIME-enabled site, the request is passed without any modification;

2. The application extension supporting privacy-enhancing access control, which is realized with help of a phpBB hook, maps this access to a specific resource (for instance, `urn:phpBB:6:5:18:edit`) and asks the server-side PRIME middleware whether the user is allowed to access it. At this point, it does not pass any handle (cf. step (11));

3. The server-side PRIME middleware checks the access control policies. It will establish a lack of information (for instance, the user has to verify that she is permitted to edit the resource) if the policy does not state that all users are allowed to edit the resource. Also, if the request has been made the first time within the current session, the server PRIME returns an 'ask' decision.
   If the request requires the application to check access control policies for more than one resource (for example to display multiple posts on the requested web page) then steps (2) and (3) are executed at least once for each single resource;

4. The application extension returns two HTTP headers:
   - X-PRIME indicates the location of the server-side PRIME middleware (for instance https://example.org:9907);
   - X-PRIME-Protected-Resource contains the resource identifier (for example `urn:phpBB:6:5:18:edit`).

[115] For users of the Firefox browser, a special add-on is available, called the 'PRIME Interceptor, which deals with PRIME-related requests.

5. If the application has to check access rights of multiple resources, then the response contains X-PRIME-Protected-Resource fields for each resource whose policy check returned 'ask'. To give an example:
   - X-PRIME: https://example.org:9907/
   - X-PRIME-Protected-Resource: `urn:phpBB:6:5:1:read`
   - X-PRIME-Protected-Resource: `urn:phpBB:6:5:5:read`
   - X-PRIME-Protected-Resource: `urn:phpBB:6:5:18:read`

6. If none of the resource access checks returns an ask (i.e., the requested resource is not assigned an access control policy or the access control policy states 'allowed for everybody') then no X-PRIME header field is returned and the client-side PRIME middleware will not be called. If access to the superior resource of the requested resources is not allowed then an 'access denied' is returned. If the web page consists of multiple access-controlled resources, then only those whose check returned 'allow' are put into the page;

7. The proxy inspects the response from the server and detects the X-PRIME headers. It caches the originally requested URL and calls the function `accessRemoteResource` in the client-side PRIME middleware to initiate data disclosure;

8. The client-side PRIME middleware calls the server-side PRIME's function `accessData` to retrieve a `ClaimRequest` that would fulfil the policy;

9. The client-side PRIME function checks whether the requested `ClaimRequest` can be fulfilled and, if necessary, asks the user for permission (in form of an `AskSendData` (ASD) dialogue) to send the requested data or to fill in missing data, respectively;

10. The server-side PRIME middleware stores the fulfilled claim together with a randomly generated session identifier (`sessionID`[116]) in the so-called 'PII database'[117]. `sessionIDs` are used as subjects within the PRIME modules. These may also be referred to as `handle` or `session handle`.
    If several resources are requested for a web page – i.e. their resource identifiers are passed to the `accessRemoteResource` function– the sequence of steps (6) - (8) is performed for each individual resource.[118] All these sequences use the same `sessionID` returned by the first `storeData` call.

11. The `sessionID` is returned to the proxy as result of the `accessRemoteResource` call. If the user decides not to disclose any PII within step (7) then the page returned by step (4)

---

[116] The `sessionID` is handled as a shared secret between the server and the client.
[117] The PII database securely stores privacy-sensitive information of the users, that is, their *Personal Identifiable Information* (PII).
[118] In the future, for usability reasons, the implementation needs to be enhanced to avoid multiple popups of the `AskSendData` (ASD).

will be displayed, consisting only of resources whose `accessData` call returned 'allow' and the following steps are not performed;

12. The proxy reloads the original URL in the client's browser, but this time, passing the `sessionID` as X-PRIME-Handle HTTP header;

13. The application extension asks the server-side PRIME middleware again, passing the handle obtained from the client (cf. step (2)).

The server-side PRIME middleware retrieves the necessary information from the PII database and performs the policy evaluation again. In contrast to step (3), this time, it uses the data stored under the handle to fulfil the policy requirements. If the user had disclosed the correct data to the server in step (5), `checkAccess` now returns 'allow'. If the web page has multiple resources, the sequence (11) – (12) is performed once for each individual resource. If access is granted, the application returns the corresponding content to the client. Steps (1) – (13) are also summarized in the figure below.

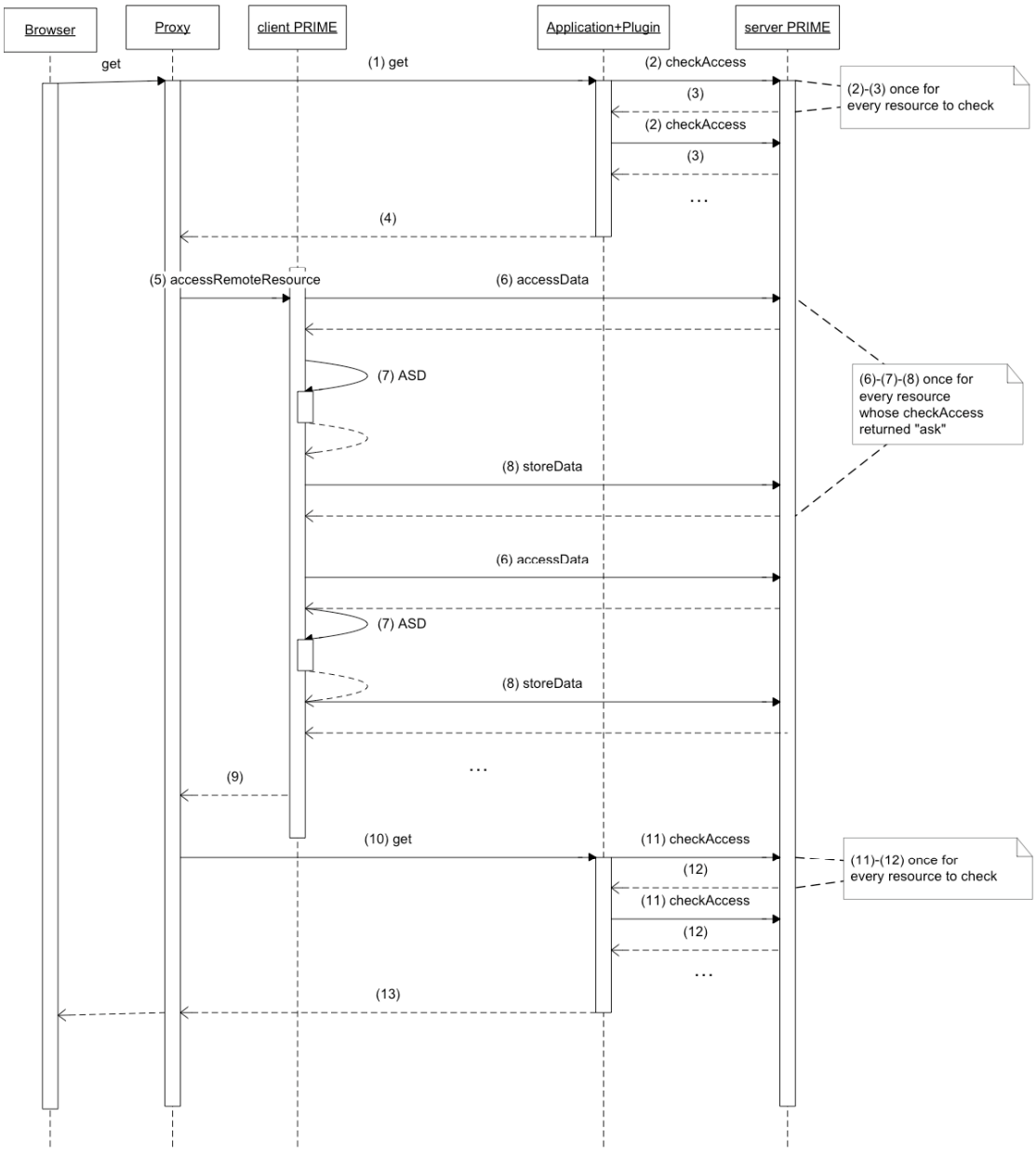


Figure 15: Sequence diagram of message exchange during the access control process.

7.1.4 Integration of privacy-enhancing access control into phpBB

The connector between phpBB and the PRIME framework, which shall overtake the tasks of access control, is realized as a hook. The concept of hooks is suggested by phpBB and allows the integration of additional code that will be executed by the phpBB application. The PRIME module for access control is integrated into phpBB through the file `hook_prime.php`, which is located in the directory `./includes/hooks/` and is automatically found by phpBB. Further files related to the PRIME hook are located in the directory `./includes/hooks/hook_prime/`. The latter contains all PRIME files within the sub-directory `./prime/`. This approach prevented any changes within the original phpBB code except for some ineluctable adjustments of

the style-related files realizing the layout and design of the user interface elements. This means that the files in the directory `./styles/prosilver/template/` have been amended by place holders for additional outputs. The latter reside within another sub-directory `./prime/` of the style directory. Moreover, the directories `./language/en/prime/` and `./language/de/prime/` as well as the corresponding files for PRIME-related internationalized texts have been added.

7.1.5 The process of checking permissions

As mentioned, the extension realizing PRIME-supported access control is included by means of the phpBB hook system. This means that phpBB provides a directory called `./includes/hooks/` in which PHP files created by others (such as the programmers who developed this extension) can be placed. In this way, the phpBB runtime behaviour can be extended or modified respectively.

Access control in phpBB is realized by the class `Auth`. Thereby, an instance of this class is assigned to the global variable `$auth`. Specific access control-related processes in phpBB are executed by calling the corresponding methods on the $auth variable.

PRIME-based access control is realized by class `PrimeAuth`, which extends the class `Auth`. Within the hook, the global variable `$auth` gets assigned an instance of `PrimeAuth` so that all corresponding method calls are now handled by `PrimeAuth` instead of the original phpBB `Auth` or PRIME `Auth` classes.

Figure 16 illustrates the process of access control by showing the single steps. These are marked by numbers and explained below.

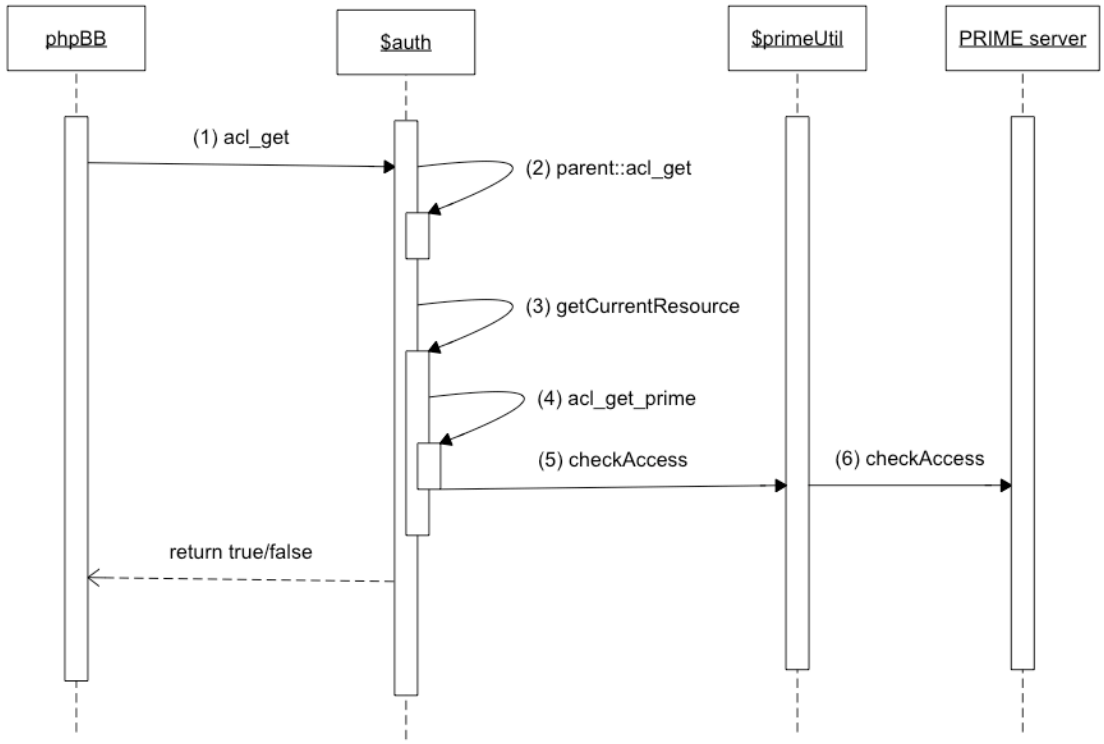


Figure 16: Steps of permission testing of resource access using the PRIME modules.

The main access control method of class phpBB. `Auth` is `acl_get()`, which aims at determining if access to a requested resource can be granted (1). The idea of the extension integrating PRIME is to determine if one of the access control systems (access control lists (ACL) used by phpBB or access control policies (ACP) used by PRIME) would allow the access to the requested resource for the requester. In order to realize the checks, the method `acl_get()` of the extended class performs the following steps:

1. Call the original (ACL-based) implementation to determine whether access is allowed (step 2). This procedure ensures that the originally intended access control mechanism based on ACLs is given priority over the PRIME-based extension. Further, since access control checks based on policies and credentials (i.e., based on PRIME mechanisms) take much more time, an access control process may be completed much faster if the result of ACL check is already a positive one;
2. If a requested access of a resource is not granted according to the corresponding ACLs, then the process of access control policy checks is started. Thereby, two predeterminations have to be made:
   Because of the complexity of the process of access control policy checking, solely the ACPs of the requested action are checked, i.e., checks of the ACPs of other actions on the corresponding resource are performed only when the user requests to execute one of these other actions. This implies that, e.g., user interface elements indicating the possibility to initiate one of these other actions (e.g., 'edit post') are displayed though it is not clear if the user is allowed to perform those actions.
   As mentioned, the privacy-enhancing extension has to handle access control not only on the levels of the forum and topics, but also on the levels of threads and posts. In order to be able to check if the resource requester is permitted to execute the action she initiated, the access control module first needs to determine which action was initiated and which kind of resource is concerned. This is realized as follows:
   - phpBB learns of the action the user initiated by an accompanying return value consisting of the name of the script intended to be called to perform the action as well as parameters indicating the resources involved in the execution of the action.
   - Actions are represented by specific identifiers[119], which are handled as resource identifiers within the PRIME-based access control. If a requested artifact is not assigned its own access control policy, or the access control policy does not contain an access rule for the asked action, then the access control policy is inherited from the next artifact residing on an upper level of the hierarchy and possessing an access control policy that contains access rules for the 'current action'. Accordingly, starting at the phpBB artifact specified by the given resource ID, the artifact hierarchy is searched upwards for an artifact with such an access control policy (step 4). The access control policy found is checked (steps 5, 6).
     If the check's result is positive, i.e., the user would potentially be allowed to perform the requested action, an additional check is performed, which aims at determining if the access rules of upper-lying artifacts (in case of a post, these would be the parent thread and topic as well as the actual forum) grant the user read access to the respective resource. This means, each superior 'read'-access control policy in the hierarchy is checked. If the user has no rights to read-access the artifacts above the requested artifact she is not granted any access.

[119] For example, '`urn:phpBB:6:5:18:edit`' stands for action edit post 18, which is part of thread 5 in topic 6 of the phpBB forum.

If no access control policy is found along the artifact hierarchy including the forum artifact, then access is considered as denied as well.

- If, according to the results of the access check procedure, access is not granted then a mask indicating 'access denied' is shown to the user and the phpBB `login_box` function (step 7) is called.

7.1.6 Displaying privacy-awareness information

Having described these technical details of the privacy-enhancing selective access control so far, in the following we introduce the tool that supports users to be aware of their privacy. The perception of privacy in social settings depends on the anonymity or identifiability of the users on the one hand, and on the available audience, i.e., who may read and reuse the disclosed personal data, on the other hand. Providing privacy-awareness information should help users to assess their level of privacy while interacting with others on the internet and enable them to make informed decisions whether to disclose personal data, for instance in the forum (Pötzsch, 2009).

Therefore, in cooperation with WP 2.2, we extended the phpBB forum with a tool to support the privacy-awareness of users. In the current (first) version, the privacy-awareness tool allows to present the following two items to the users:

- Their current IP address, and
- the potential audience that may access the disclosed personal (and non-personal) data.

The display of the current IP address shows users that they are not completely anonymous on the internet and – in particular – in the phpBB forum, but rather that there is some identifier available. The indication of the potential audience should partly compensate the missing social and context cues in computer-mediated communication (Döring, 2008) and, thus, it reminds users how many people have the possibility to read their posts in the forum.

For the integration of the privacy-awareness tool in the privacy-enhancing version of the phpBB forum, the information about the potential audience is coupled with the setting of the access control policies for read access. If no particular policy is specified for the forum element and the default policy of the upper-lying content element(s) states 'allow everybody', then the tool indicates 'all internet users' as the potential audience for this posting (Figure 17). However, if an access control policy is set which restricts the potential audience, the tool makes users aware of this fact (Figure 18).

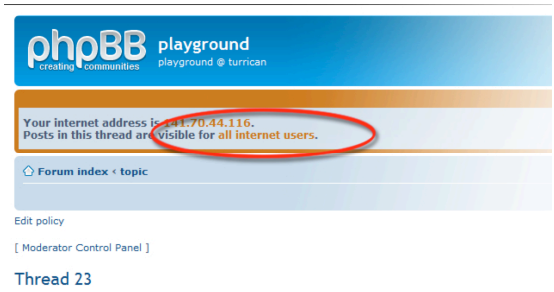


Figure 17: All internet users can see the post in phpBB.

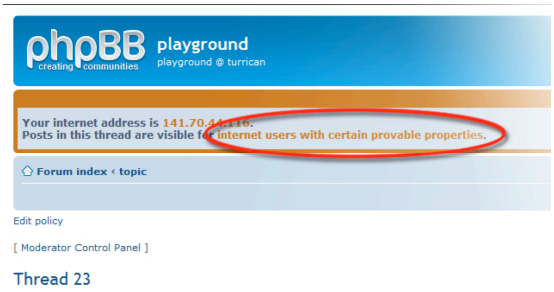


Figure 18: Only users with certain provable properties can see the post in phpBB.

Table 15 provides an overview about the dynamic options of the display of privacy-awareness information in the prototype.

Privacy Awareness Item:	Depends on:	Example output message:
IP address	The current IP address of the user's device	"Your internet address is 141.70.44.116."
Potential audience	Forum element and the settings of the access control policy	"Posts in this forum are visible for all internet users." "Posts in this thread are visible for internet users with certain provable properties."

Table 15: Display options of the privacy awareness component for phpBB.

7.1.7 An example of a scenario of selective access control in phpBB using PRIME middleware

To explain how selective access control based on access control and credentials in the forum as an instance of collaborative workspaces works, we sketch the following scenario: Alice, Bob, Hannes and other people are users of a leisure-oriented forum in which several different topics are discussed. In general, everybody is allowed to contribute with no need for registering at the service, which typically requires users to provide their e-mail addresses and/or further personal data. The forum only requires to indicate a unique pseudonym if someone writes a contribution.

When Bob creates a new thread called 'Fit for summer' under the topic 'Sports and Cars' he wants to encourage men in particular to get in shape and to discuss their weight problems without feeling ashamed due to women around. Therefore, he specifies that only male users should have reading and writing access to this thread. Then, Bob writes an introducing post for the thread and explains that men who plan to start sports and healthy nutrition should contribute to this thread in order to motivate each other. For this post, Bob does not specify additional access rules. Thus, the rule is derived from the thread, that is, only men can read the post. Write access to particular posts is granted to the author himself/herself and the moderator of the topic in the forum by definition.

Hannes, who is a bit overweight, wants to find a buddy for the fitness centre near his home. Therefore, he describes his weight problems, his time constraints due to work and family and which fitness centre he is member of within a new post in the 'Fit for summer' thread. Since Hannes does not want everybody on the internet to know about this information, he only allows people who are already members of the same fitness centre access to his post in order to find a buddy for training together and motivating each other. Thus, Hannes' post can only be read by men who are members of the same fitness centre.

When someone tries to read Hannes' post in the forum, the evaluation of the access control policy is performed according to the hierarchical order of the content elements of the forum (Table 16).

Level:	Access control policy:
1. Forum	[(cred:Admin-Forum) OR (everybody[default])] AND
2. Topic	[(cred:Moderator-SportsAndCars) OR (everybody[default])] AND
3. Thread	[(cred:Moderator-SportsAndCars) OR (cred:Owner-FitForSummer) OR (cred:male)] AND
4. Posts	[(cred:Moderator-SportsAndCars) OR (cred:Owner-PostFromHannes) OR (cred:memberOfFitnessCentreXYZ)]

Table 16: An example of an access control policy.

In the example, step (1) (Forum) of the access policy ensures that someone is allowed to read the forum if he/she is the administrator of the forum or – since we have chosen a public forum for our example – anybody else. Step (2) (Topic) specifies that someone is allowed to read the topic 'Sports and Cars' if he/she is the moderator of the topic or anybody else, since for the topic no restrictions are given in the example either. Step (3) (Thread) ensures that someone is allowed to read the thread 'Fit for summer' only if he/she is the moderator of the topic 'Sports and Cars\' or if he/she is the owner of the thread or if he/she is male. According to the example above, step (4) (Post) determines that someone is allowed to read the post from Hannes if he/she is the moderator of the topic 'Sports and Cars' or if he/she is the owner of the post or if he/she is member of the Fitness centre XYZ.

Read access to Hannes' post is only granted if the whole policy (steps (1) - (4)) is evaluated to be 'true'. Similar to this example for read access, further policies need to be specified in order to add, edit or delete a resource. All users who add a post to a particular thread have the opportunity to further restrict access to their own contribution. However, it is not possible for them to overwrite access control rules from other elements that stand above the post in the hierarchy of the forum elements.

7.2 Audience segregation in social network sites: Clique

In Chapter 5 and 6 we presented a wide variety of issues relating to privacy and identity management in social network sites. In building a demonstrator for PrimeLife we have attempted to contribute to solving some of the most central issues with respect to privacy and identity management that we have encountered in our analysis of existing social network work sites such as Facebook and MySpace. These issues include:

- Users lack overview with respect to who the audience is when posting content in social network sites;
- Users cannot distinguish between different audiences within a social network site. All contacts are collected in a single audience that sees all of a user's postings, thus creating 'context collision' or 'context deflation';
- Information posted in social network sites persists over time – not just the content posted there, but also the relationships users engage in. The only way out of an established connection with another user in a social network site is the socially highly circumspect act of 'defriending';
- Users can snoop on others and engage in peer surveillance;

- Users have limited control over who accesses their data, who stores and copies it, over who adds or removes information about themselves;
- Providers and third parties can use social network sites as an excellent source for information for the creation of profiles and engage in targeted advertising.

In this section we will describe the social network site demonstrator that we built, called Clique.

7.2.1 Before we begin: A note on terminology in Clique

The language used to discuss online communities, the users participating in them, and the connections between these users is often quite fuzzy and imprecise. In our description of Clique we will use the following concepts:

Concepts:	**Description:**
1. Platform	The terms 'platform' and 'social network site' (SNS) (in singular form) will be used interchangeably. We follow the definition of boyd and Donath mentioned in previous chapters – that means that a platform (i.e. the social network site) is a *bounded* system in which users create one or more *profile*(s) and engage in interactions with a *network* of contacts.
2. Face	A person's 'face' is composed of all the personal information that is gathered in a single profile to express an identity. While users currently tend to create only *one* face in social network sites catering specific needs (e.g. dating or professional self-presentation), those catering to several needs, or those catering no specific need at all, might invoke users to create *multiple* faces within the same domain. In such social network sites, then, the personal information making up various identities may be brought together for each individual user.
3. Collections	'Collections' are sets of contacts selected and assigned by the individual from the totality of his network. Collections can consist of anywhere between zero and an unlimited amount of contacts. The individual can assign a name to each collection to identify them as a collection (e.g. 'colleagues' or 'old schoolmates' or 'boring people'). Moreover, each time content is added to the profile, it can be made available for specific collections, or even for specific members of each collection, based on the user's own preferences (more on this below). The management of collections and the content available to them should be dynamic, transparent and open to change at all times.
4. Context	A 'context' is each instance in which a *particular face* and a *particular collection* come together. For instance, a 'work context' is one in which a user presents his 'work identity' (face) to his 'colleagues' (collection). Similarly, a 'reminiscence context' arises when a user presents information

Concepts:	Description:
	(pictures, documents, text in chat relays) (face) regarding his younger years to his 'old school friends' (collection). A third example is that of a person making his holiday pictures available, i.e. information that is often regarded as quite personal (face) to all of his family members (collection) and some individuals from his friends (collection).

Table 17: Key concepts in Clique.

In the picture below we present a graphic depiction of the structures and concepts we distinguish in relation to social network sites.

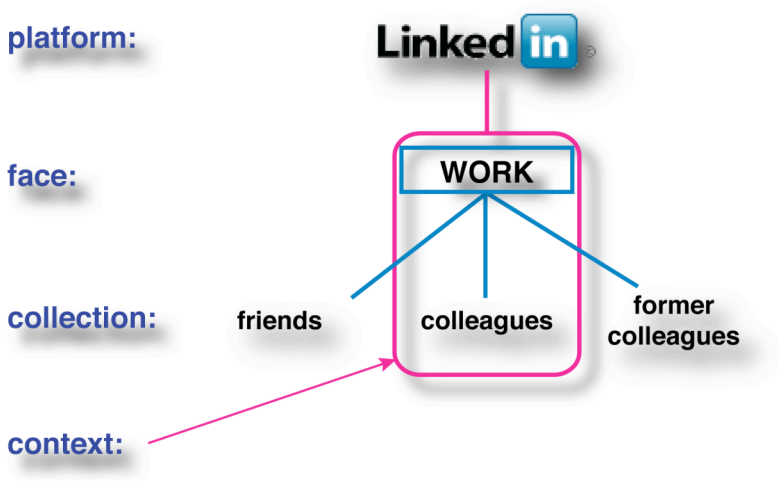


Figure 19: Terminology for social network sites.

In the next sections we will discuss the key features of Clique and the way in which they contribute some of the issues mentioned above.

7.2.2 Clique: An introduction

Within WP 1.2 of the PrimeLife project we have developed our own social network site called Clique (www.clique.primelife.eu) as a demonstrator for audience segregation and privacy-enhanced social networking. With this social network site we hope to accomplish a number of goals:

- To translate the requirements presented at the end of Chapter 5 – which were based on the findings of our analysis on current issues in existing social network sites with respect to privacy and identity management – into concrete, practical and workable solutions;
- To provide pointers for the providers of existing social network sites on how some privacy and identity issues could possibly be solved in their own social network sites;

- To raise awareness among users that privacy and identity management issues exist in current social network sites, that these can be solved, for instance, in the way we did in Clique, and that it is important for users to actively approach providers of existing social network sites such as Facebook and MySpace to ask for tools to solve such issues.

Clique was built using Elgg[120] Open Source software for developing a social network site. It is our goal to make the tools that were developed in Clique available for the (Elgg) Open Source community as well. Below is a picture of the 'dashboard', the opening screen a users sees after logging into the network of Clique.

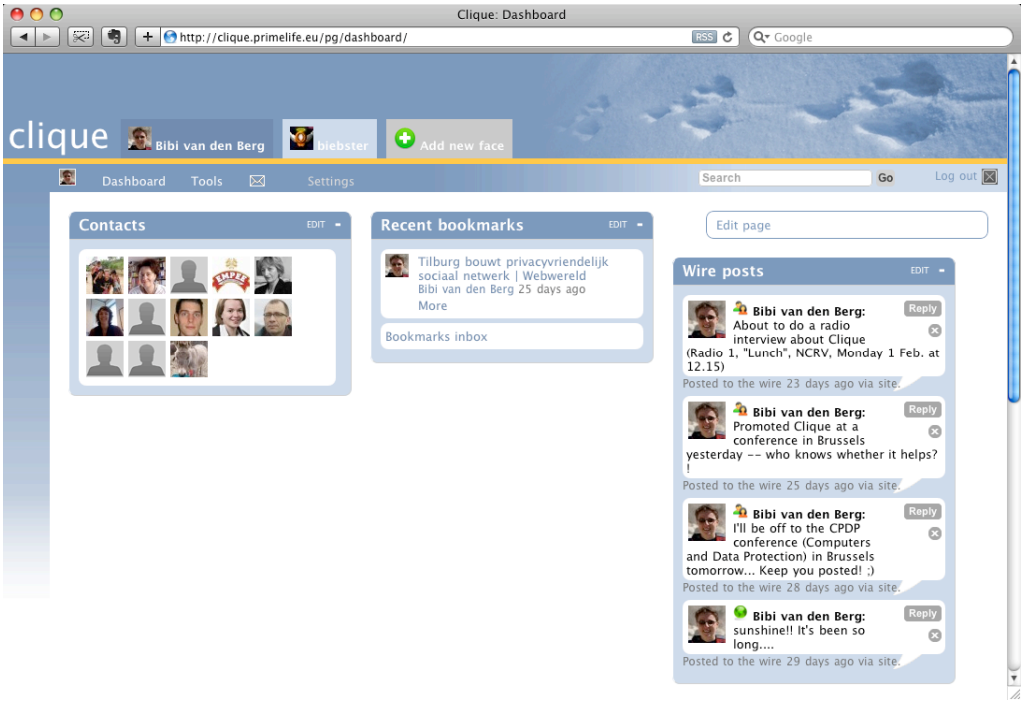


Figure 20: The Clique dashboard.

Clique has a number of features, which will be discussed in detail in the next sections.

7.2.3 Facilitating nuance in users' audience in Clique

The first principle we realized in Clique to enhance users' ability to protect their privacy and to increase their options for adequate and realistic self-presentation was the introduction of *nuance* in connections (also see: Donath and boyd, 2004). By this we mean two things:

- Enabling users to create *multiple 'faces'* within the same social network site, so that they can show different 'sides' of themselves;

[120] See http://www.elgg.com/ [last accessed on 24 February 2010].

- Enabling users to create their own labels for 'collections' in which they may gather one or more of their contacts.

We will begin by discussing the latter – the creation of multiple faces in Clique will be discussed in the next section (7.2.4).

As we have seen in Chapter 5, in most social network sites all contacts in a user's network are lumped together in one category. No distinction is made between the different social spheres a person may participate in, as all of us do in our everyday lives. This means that a) it is impossible for users to hide parts of their network of contacts from other contacts (for instance, I do not want my colleagues to see my friends, or I do not want my mother to see my colleagues); and b) that it is impossible to show particular information to one portion of one's network while hiding it from others. All information displayed on one's profile is there for all to see, at least for one's entire network of contacts.

By allowing users to create 'collections' within their network of contacts, they can cluster social relations according to their own preferences, and thereby mimic the actual practice of building and maintaining separate social spheres in real life in the process. It is important that users can be free in *labelling their own set of collections*, since they themselves know best what the fabric of their own social lives consists of and how it could be divided into relevant and meaningful categories. James Grimmelmann has argued that offering what he calls 'technical controls' to manage the (in)visibility of a person's profile in social network sites is not a workable solution for the following reason: if the provider of the social network site offers the possibility to place contacts in clusters (such as 'family' or friends'), then these clusters are never going to be an adequate representation of the complexity of social relationships in real life. He writes: "*Consider the RELATIONSHIP project, which aims to provide a "vocabulary for describing relationships between people" using thirty-three terms such as "apprenticeTo," "antagonistOf," "knowsByReputation," "lostContactWith," and "wouldLikeToKnow."*[…] *Clay Shirky shows what's wrong with the entire enterprise by pointing out that RELATIONSHIP's authors left out "closePersonalFriendOf," "usedToSleepWith," "friendYouDontLike," and every other phrase we could use to describe our real, lived relationships.* […] *We shouldn't expect Facebook's formal descriptors to be precise approximations to the social phenomena they represent.*" (Grimmelmann, 2008: 27)

Grimmelmann is absolutely right, of course, in claiming that the social network site *provider* can never manage to capture the complexity of individuals' many social spheres and connections. However, we argue that the *individuals themselves* are fully capable of doing so, and this is why we believe it is important to place access control mechanisms, such as creating collections to cluster social contacts, into their hands rather than into the hands of providers and system designers. Users can then choose which labels to use for which collections and also how granulated they want their own set of collections to be. This solves the problem signalled by Grimmelmann above. Having said that, with regard to user-friendliness a number of standard options might be included in the list of collections (e.g. 'family', 'relatives', 'friends', 'colleagues', 'acquaintances', etc.).

Below we present a number of screenshots that show the way in which the creation and management of collections is implemented in Clique. Figure 21 shows the way in which users can add a new collection to their profile page. They begin by typing in a name for the collection, in this case 'My favorite colleagues'. Then individual contacts from the user's contact list – that is, individuals that he or she has befriended beforehand – can be added to the collection by clicking through the alphabet and selecting those individuals the user wants to include in this collection. The letters of the alphabet are bold if there is a contact whose user name starts with that letter, and grey if not. After selecting one or more contacts to add to the collection, the user can click 'save' and the collection is added to his profile. Figure 22 shows an overview of the collections this user has made and outlines how many contacts are in each collection.

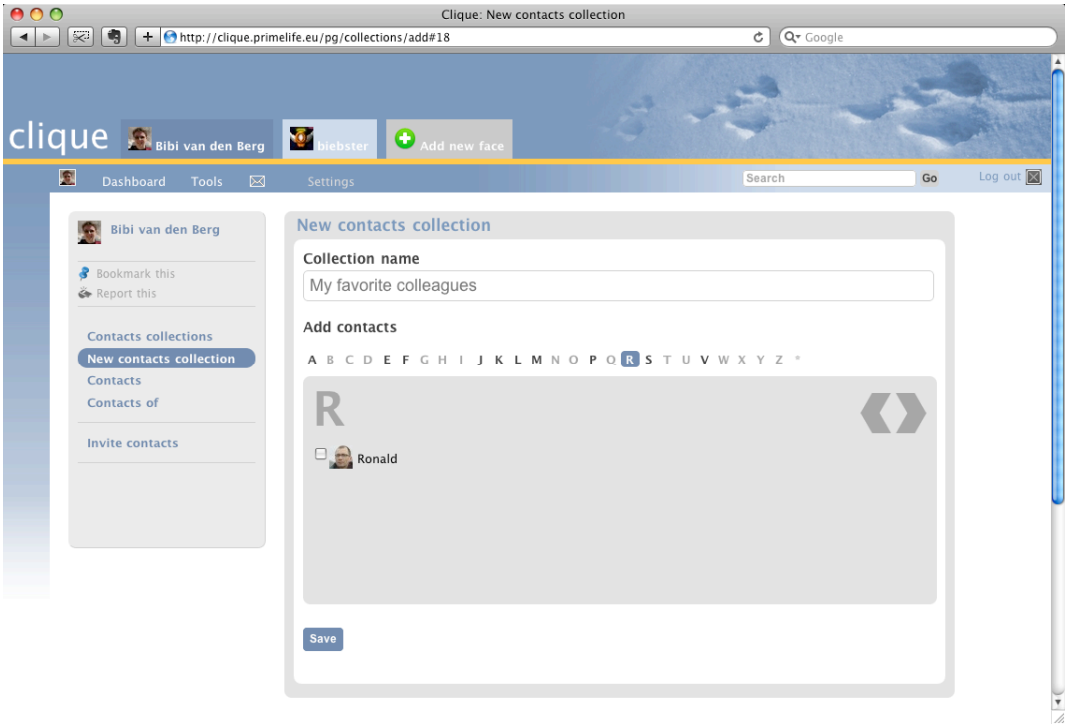


Figure 21: Creating a new collection in Clique.

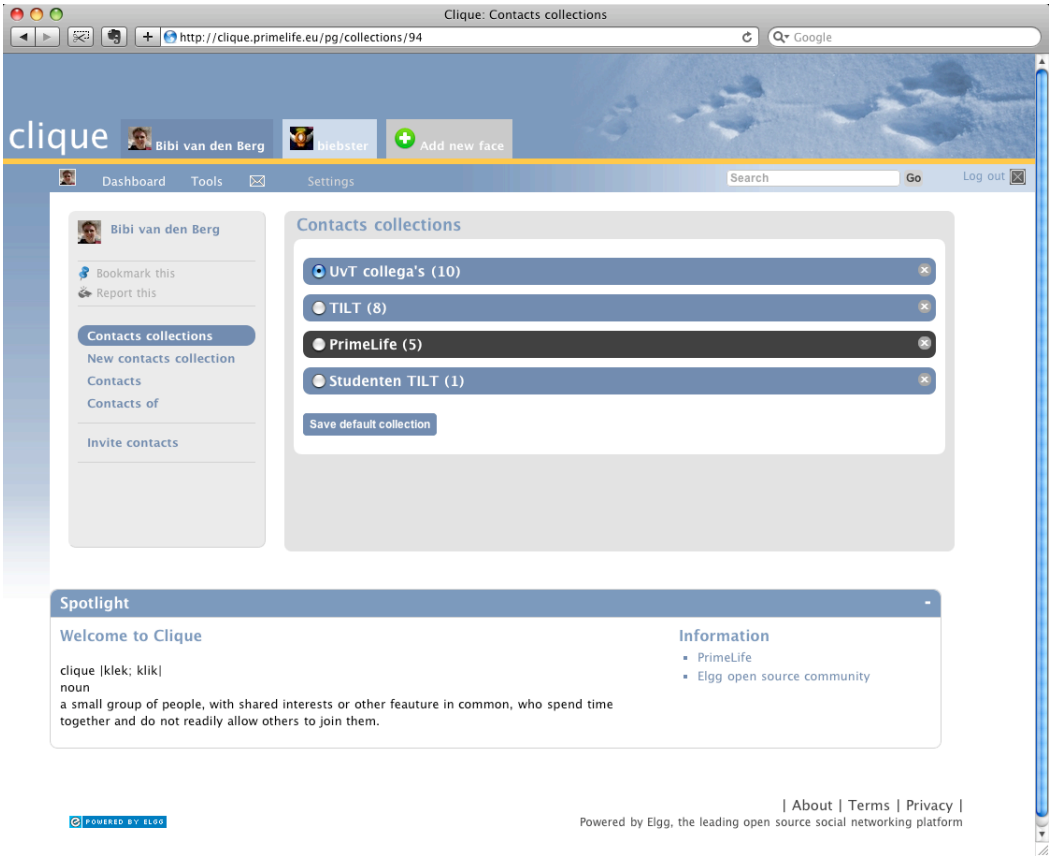


Figure 22: Overview of a user's different collections.

7.2.4 Contextualizing profiles in Clique

The second principle that we focused on in our contribution to realizing privacy-enhanced social network sites aimed at *contextualizing* the user's profile and all the information gathered there. This would solve issues of context collision, context deflation and de-contextualization, which we've addressed in Chapter 5. Currently, in existing social network sites users are allowed to create only one profile per person, and hence can create only one context in which all of their data are gathered. However, in real life individuals move from one context to the next throughout their everyday life – they travel to work, visit a supermarket, have dinner with their family at home, and spend the evening at the gym with friends. Combining all of the different sides of themselves that they normally display in each of these different contexts is a challenge, and we have seen that many users confess they do not manage to do it well, if at all. One solution many social network site users have turned to in order to overcome this challenge is to create different profiles in different social network sites, for instance a work-related profile in LinkedIn and a more personal one in Facebook. While this solves the issue of context collision, it is a time-consuming and cumbersome solution, since users have to log onto different platforms to manage their profiles and keep track of contacts and their activities in each domain.

To solve this issue we developed the following idea in Clique: Users can create multiple '*faces*' in Clique to mimic the various social contexts in which they participate in real life (for instance, a work face, a private face, a face for the tennis club etc.). When a user accesses his profile in Clique, his various faces are visualized with separate tabs. By clicking on the tabs the users can access the page attached to that face. Figure 23 shows a screenshot of the author's two faces in Clique. The first, a face called 'Bibi van den Berg' is a work-related face, in which she presents information about her professional life and is connected to colleagues at the University of Tilburg, within her department, with other members of PrimeLife, and with students of her own department. The other face, called 'Biebster' is her private face, which is only visible to intimate friends and family. Note that the latter do not see the author's professional face. New faces can be added by clicking on the tab at the far right, which reads '+ Add a new face'. As the figure shows, existing faces can be enabled, temporarily disabled or removed entirely. Each of these faces has its own list of contacts and (if the users has created them) its own list of collections. Using tabs to distinguish between different faces is a visually appealing and easy way for the individual to manage his or her own profile and the various faces contained therein. Information added to one of the tabs (e.g. the 'Biebster' tab) is invisible in all other tabs, and hence it is easy for the user to manage who sees what. By simply clicking through the different tabs he or she can see what information is accessible there.

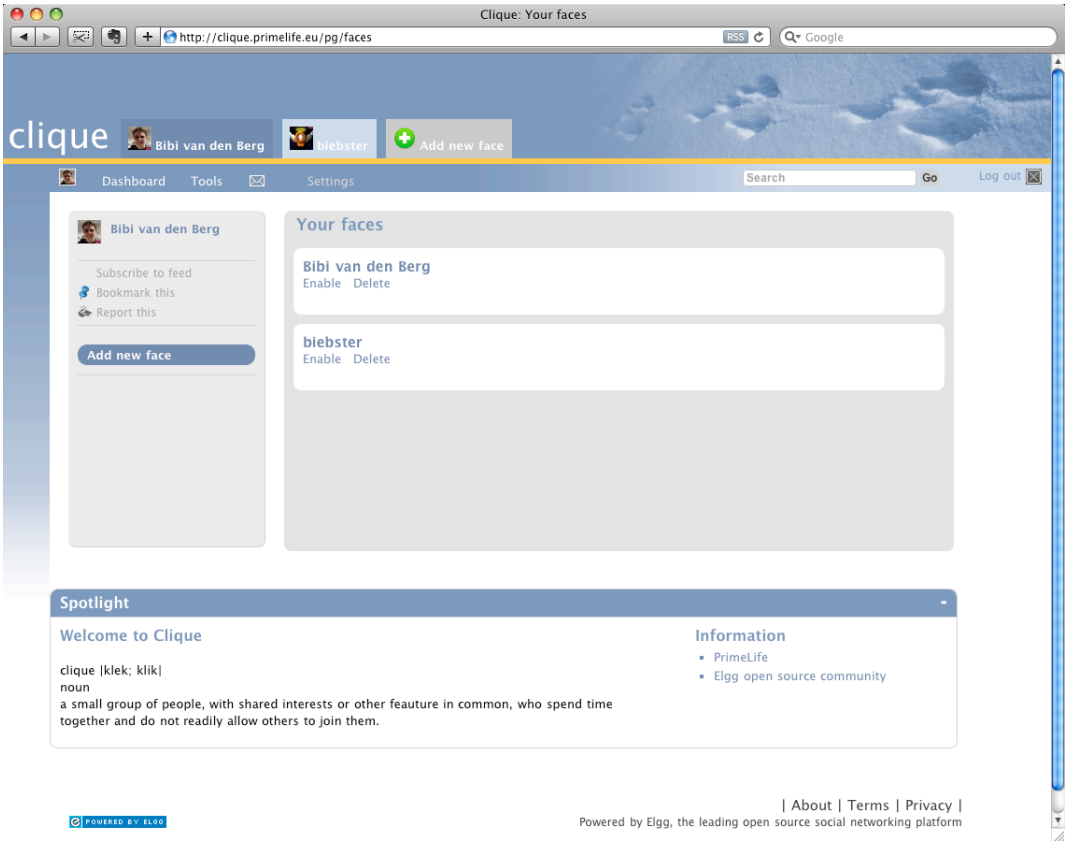


Figure 23: 'Faces' in Clique.

7.2.5 Contextualizing information in Clique

Introducing faces was one way in which we've implemented audience segregation and countered context collision in our social network site Clique. However, it was not the only measure we took to contextualize users' activities. In order so safeguard their contextual integrity we also implemented a tool to contextualize each item of *information* that users add to Clique. Each time users post an item of information, whether this is an item of content (a picture, a blog entry) or personal data (filling in the 'address' field on the profile page, adding a telephone number) the system asks the user 1) in which *face* (context) they want to make it available, and 2) to which collections and/or individual users.

Thus, contextualization in Clique has a number of aspects. First, as we have seen, faces compartmentalize the information a user displays before different audiences, thus countering existing issues of context collision in social network sites. Second, users add contacts and collections to each specific face, for instance 'friends' and 'relatives' to a private face, and 'colleagues' and 'former colleagues' to a work face. This further prevents information spill and information leakage (either accidental or otherwise). Last, each time a user adds an item of information to his or her profile page, the intended face and audience must be specified, which diminishes the risks of information spill even more. In this way users gain control over visibility and/or accessibility of information in relation to particular collections and/or particular individuals. For example, colleagues would be prevented from seeing one's holiday pictures, or acquaintances from reading one's diary entries.

Below is a series of screenshots that depict the implementation of contextualizing information as we've implemented it in Clique. The central principle in realizing access control for social network sites here was to diversify between *public*, *semi-public* and *private postings*. Thus, when users post information within a face, they can choose to display the information to:

- No one (private)[121];
- Specific collections, individual contacts, or a combination of both (semi-public yet more restricted than the following);
- Contacts (that is all the individuals on the user's contact list in that face, i.e. semi-public);
- All members of Clique (public);

Figure 24 shows a screenshot of what uploading a file looks like in Clique. The file is uploaded in the author's 'Biebster' face, as signified by the darker shade of the tab in the top row and the icon and name in the left corner. After choosing a file and giving it a name and description the user can choose which individuals and/or collections can see this holiday picture by clicking on 'Define access rights'. Figure 25 shows the screen that appears when a user clicks this link. By placing individual contacts or collections in the 'Allowed contacts' or 'Denied contacts' box the file that is about to be posted on the profile page is made accessible (or not) to the individuals added to each box. In this case, the contacts in two collections ('My best friends' and 'Friends') can see the holiday picture, except for one person: 'Sandra', who is a member of the collection called 'Friends' – as is signified by the tag underneath her name – has been moved to 'Denied contacts' box, and will therefore not be able to see this picture, despite the fact that she is in the 'Friends' collection. After setting the access rights to this picture the user clicks 'OK' and the file will be uploaded and made accessible to the intended audience. The user can always adjust the access rights at a later stage as well, and can see who has access to the information by hovering his mouse over the icon below the item of information (in this case the picture) that he or she has posted online. For instance, Figure 26 shows that the author's holiday picture is visible to one collection and two individual contacts, and that access has been denied to one individual contact.

The method of defining who has access to information described here does not only apply to items of content that a user places in a profile, but also to each item of *personal data* that he or she adds. Thus, when filling in profile fields such as one's location, 'About me', one's interests, skill or e-mail address, each of these items of personal information are accompanied by access rights settings. Thus, a user may choose to make his skills public to all members of Clique, while limiting the visibility of his e-mail address to specific contacts or collections, and keeping his phone number entirely private. Figure 27 shows the author's 'Biebster' profile page. In her profile the 'location' field is set to public. All members of Clique can see that she lives in Rotterdam. By contrast, her contact e-mail, mobile phone number and website are accessible only to specific collections and/or individuals. The field labelled 'About me' is accessible to all of her contacts, but her home phone number and interests are set to 'private', so that no other user will be able to see them.

[121] Such information may include, for instance, a phone number, home address or email address, which is required for creating a profile by the service provider, but can be kept private for everyone else.

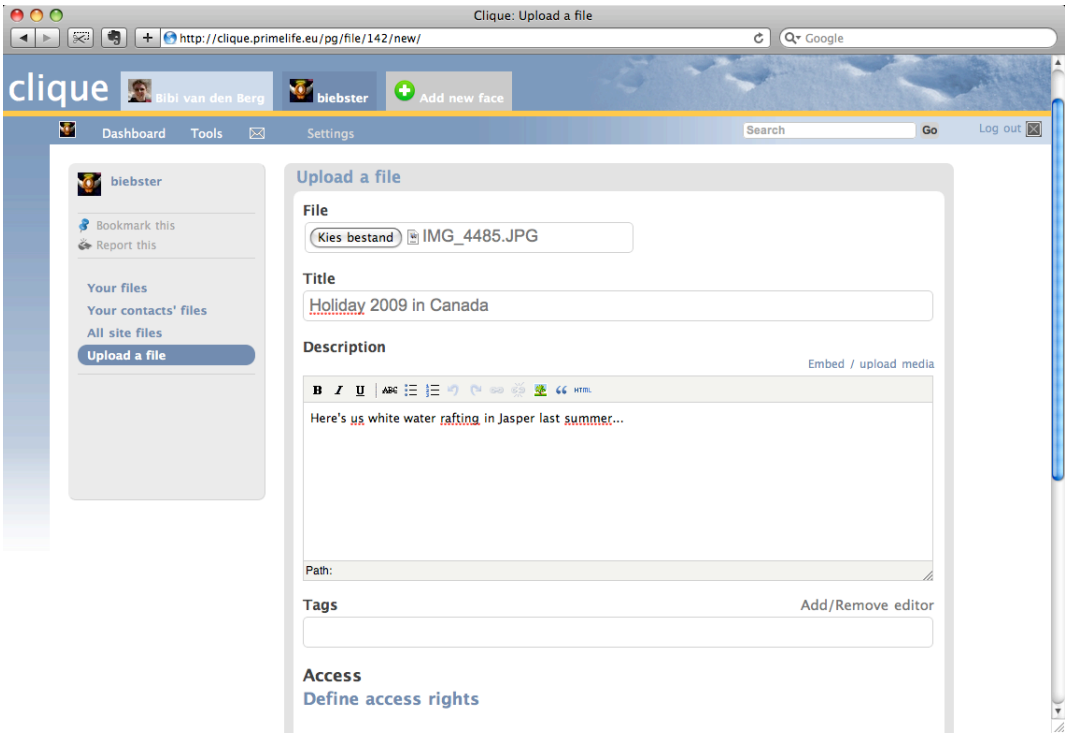


Figure 24: Uploading a file in Clique.

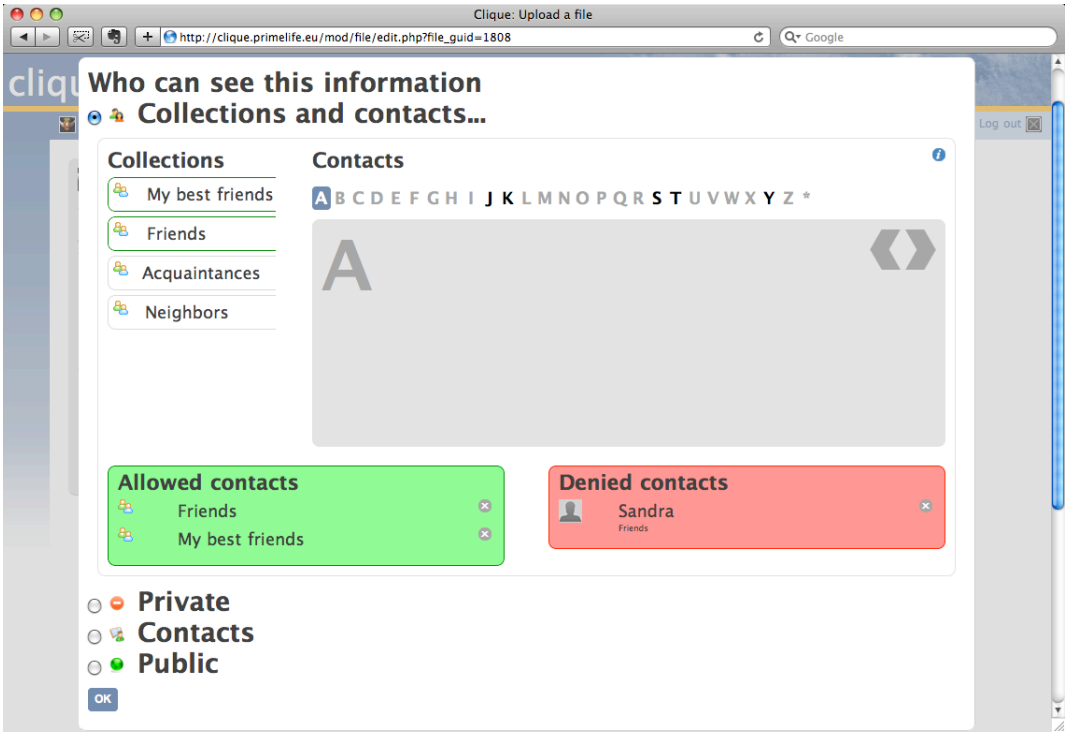


Figure 25: Defining who can see an item of information in Clique.

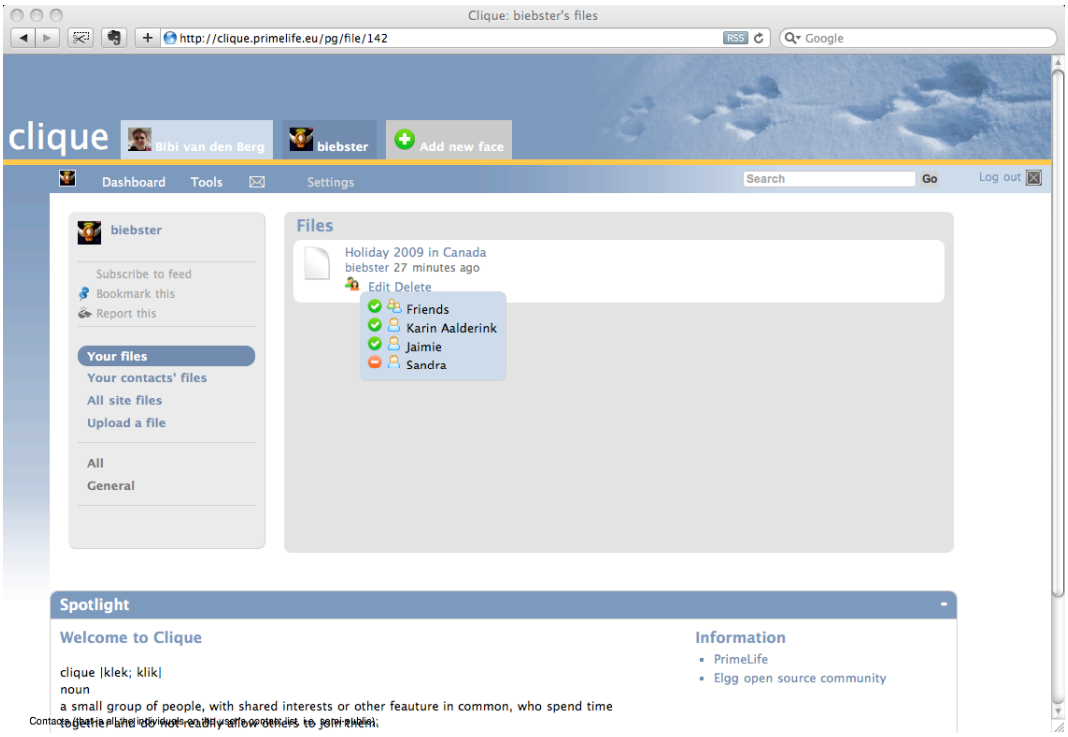


Figure 26: Feedback on who can see an item of information in Clique.

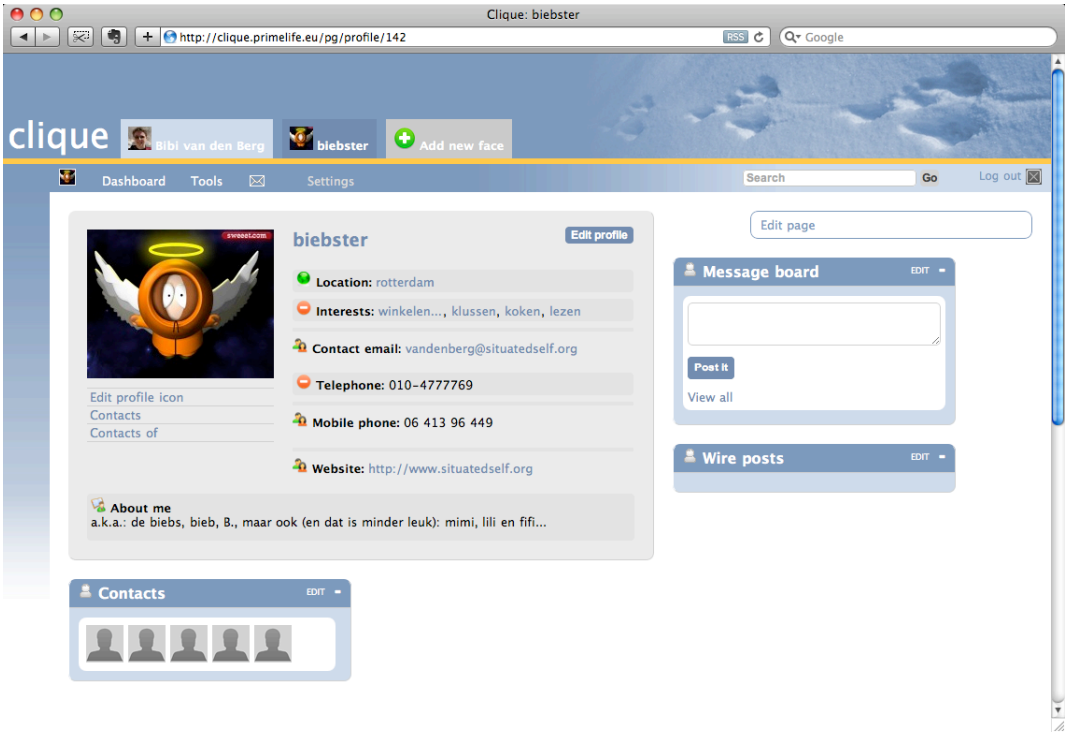


Figure 27: Access rights to personal data on a profile page in Clique.

The combination of these features – the creation and management of collections, contextualization through the availability of multiple faces, and the protection of contextual integrity through the

ability to set access rights to each item of information added to Clique – enable users to protect their privacy and present their identities in a way that is more true to the nature of social life as we know it in everyday life. By building these features we hope to have contributed to taking the first steps towards a second generation of social network sites that is more privacy-friendly and enhances user experiences for managing relationships and engaging in self-presentation.

7.3 Encrypting personal information in web 2.0: Scramble!

In this section we will introduce the third and final demonstrator we have developed in the PrimeLife project to solve some of the issues surrounding privacy and security in self-presentation in social network sites (and also in other web 2.0 environments), an encryption tool called Scramble!.

7.3.1 Introducing encryption tools for access control

We are not the first researchers to point towards the need for access control in social network sites, and some other tools have been built to this end in the past (for a more extensive discussion, cf. Beato *et al.*, 2009). For instance, the Lockr project[122] was initiated by a group of researchers from the University of Toronto, and offers the users of social network sites access control over the data they share by hiding and mapping the selected information into third-party storage. For example, images could be hidden in a storage server such as Picasa[123]. Our main concern with the Lockr extension is the need to rely on trusted third-party storage for the hidden information. The user does not keep full control over his own data, but rather has to place trust in a (commercial) third-party to guarantee a safer use of social network sites.

Another example of access control that was developed for social network sites is FlyByNight, which was developed by Matthew Lucas and Nikita Borisov of the University of Illinois (Lucas and Borisov, 2008). In their paper, Lucas and Borisov present a Facebook application to protect private data by storing these data in Facebook in encrypted form. Their application is social network site dependent, that is, it only works for Facebook, and relies on the servers of the social network itself for encryption key management. The decryption algorithm is implemented in JavaScript and retrieved from Facebook. Therefore, their scheme is browser-independent and portable, but its biggest disadvantage is that it is not secure against active attacks by the social network provider, Facebook. As we have seen in section 5.3 of Chapter 5 this is a serious shortcoming, since the providers of social network sites are, in fact, one of the three possible parties that may threaten the privacy of users (third parties and other users are the other two).

Our prototype application solves the shortcomings of both of these examples. It relies primarily on the user side and has no dependencies on any specific social network site. In contrast to FlyByNight it is entirely client-side dependent. Moreover, it doesn't use a third-party to store information, as is the case in the Lockr project. Also, what our access control mechanism enables, and what all other existing ones lack, is *selective* access control. In the next sections we will explain what our encryption tools consists of and how it works. In summary, our encryption tool, called Scramble!, has two key goals: a) users on social network sites are enabled to formulate who has access to the content and personal information they place in or attach to their profile, and b) all of the information (both content and personal data) that users place online are encrypted and will

[122] http://www.lockr.org/ [last accessed on 25 February 2010].
[123] http://picasa.google.com [last accessed on 25 February 2010].

only be visible to those contacts and/or collections that have the appropriate access rights. Individuals and collections that do not have access rights, cannot see the information, and nor can the social network site's provider.

7.3.2 The model behind our encryption tool

Social network sites can be understood to be a large graph, expressing the many connections between their users. Since we may assume that not all connections between users are mutual, these networks are actually *directed* graphs. Each profile in a social network site contains two kinds of information: the individual's personal information and his connections to others (i.e. his contacts). To manage the access control in a way that respects the principles addressed above in this deliverable, and in order to allow user to have control over his own private data, we propose a *tree-like structure* of the user profile node. We categorize the user profile in two types of classes:

- *Connections classes*, which classify the network of *connections* of a user (e.g. 'friends', 'family', 'colleagues' and so on and so forth). These classes represent collections and can be divided into sub-groups;
- *Content classes,* which classify the *content* that users place into their profile. These content data can also be divided into sub-classes, which we have called 'faces'. Think for instance of data related to hobbies, family, or work.

Formally, in order to define access control, we considered that each class represents a set. Thus, a set A is a sub-class of class B if $A \subset B$. In this way users' connections and content form a partially ordered set (lattice).

7.3.3 Access rights

Mapping the content and connection classes defines the access control rights. The class structure allows easy propagation of rights, without overloading the social network user. When a new item of information is introduced in a content class, all members that belong to a connection class and that have access rights to the content will have access to that information item. Similarly, when a new connection is added to a connection class, he or she will have access to all information items to which the other members of the same collection also have access. Due to the fact that the access control enforcement for information is in the hands of the user himself – that is, since we use the prototype application on the *client* side – the social network provider will not learn who has access rights to what information.

This model allows the user to control access to his information in a very fine-grained way. While technically skilled users might find this interesting, less computer-savvy people need to be provided with some default classes of connections and data, and preferably also a default mapping, in which a privacy level might be specified. In this way, we try to create a good balance between usability and confidentiality.

The user's profile is divided into 'connection classes' and 'content classes', which in turn are further divided into sub-groups of classes, forming a hierarchical structure. The graph representing the users' connection structure is stored on the provider's servers. In contrast, the user's list of connections, and the respective public keys, are controlled on the client side by the user himself. The classification of contacts into collections can thus differ from that stored on the social network site himself.

The access control mechanism works as follows: each time a user posts new content or adds/changes or deletes personal information to his profile on a social network site, he makes a selection within his connections classes to specify who will have access to the content and/or personal information. In this way, the user keeps his personal data private for a pre-defined audience. In practice this means, for instance, that all the members of the collection called 'friends' have access to all of the documents (blog posts, pictures, audio files, shared hyperlinks, etc.) from the user's face called 'private'. This is possible because all the members that belong to the collection called 'friends' share the secret to retrieve the content. Also note that users and data can reside in several connection/content classes simultaneously.

7.3.4 Access control enforcement

In our model we propose to use cryptographic techniques to enforce access control. In the prototype application we have built we use an OpenPGP[124] standard to keep social network users' data confidential. One nice feature of OpenPGP is that it supports encrypting to multiple recipients using hybrid encryption, by encrypting the content with a random secret and the secret with all the public keys of the set of users. We assume that each user holds a public and a secret OpenPGP key pair. Whenever a new connection between two social network users is established, these users exchange their public keys. The shared public keys are then stored locally and compose the user's circle of trust. The OpenPGP public key can also be retrieved from an online key server by name or e-mail mapping.

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

7.3.5 The encryption tool: Scramble!

Figure 28: About Scramble!

[124] OpenPGP is one of the world's most widely used encryption standards. Please see http://www.openpgp.org/ [last accessed on 25 February 2010].

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

Figure 29: The Scramble! address book, from which selective access rights can be managed.

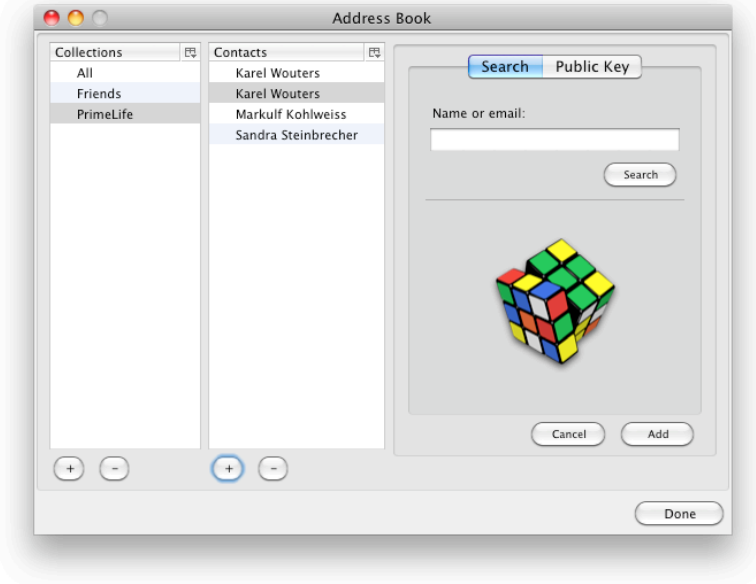


Figure 30: Adding a new contact to a collection in Scramble!

In Figure 29 users can assign contacts to collections, either predefined ones or self-defined ones. Figure 30 shows how a contact can be added to a collection: by typing in a name or email address the user can search for contact to add to this collection.

Since Scramble! is a Firefox extension it is not linked to a specific social network site, such as Facebook or MySpace, but works across platforms – we have done extensive testing with it in Facebook and MySpace, and also in our own social network site Clique, which we discussed in section 7.2. Figure 31 shows the plugin in (an earlier version of) Clique. In this picture the user has the plugin installed and switched on, and he or she has the proper access rights to read the information. This means that the content is decrypted and displayed as normal text.

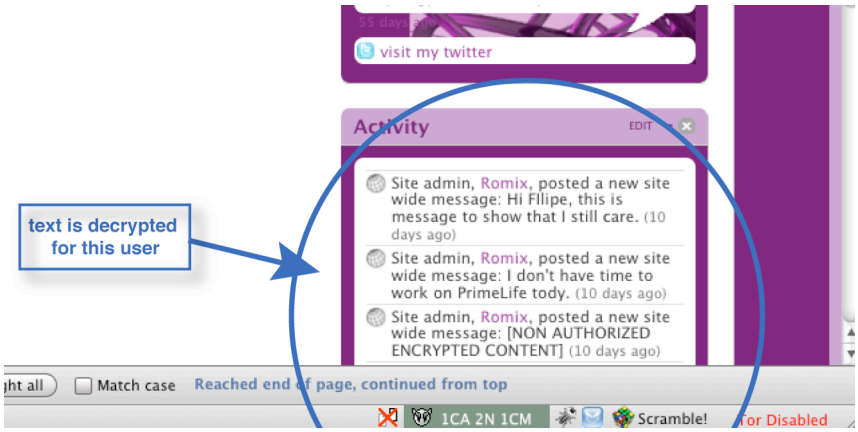


Figure 31: Using Scramble!: decrypted text.

In Figure 32 below the user has the plugin installed and switched on, but he or she does not have access rights to the information, so the information is not decrypted. Instead, he text is replaced by the phrase '[NON AUTHORIZED ENCRYPTED CONTENT]'.

Figure 32: Scramble! is switched on but the user does not have access rights.

Those who have not installed the plugin have no access to the information at all and instead see encrypted text. They see a different message from those who do have the plugin installed but have no access rights to this particular piece of information. Users who do not have the plugin installed see a so-called 'tiny URL', a hyperlink referring to an address where the encrypted text is stored on their screen instead of the decrypted information placed in the profile by the user (Figure 33).

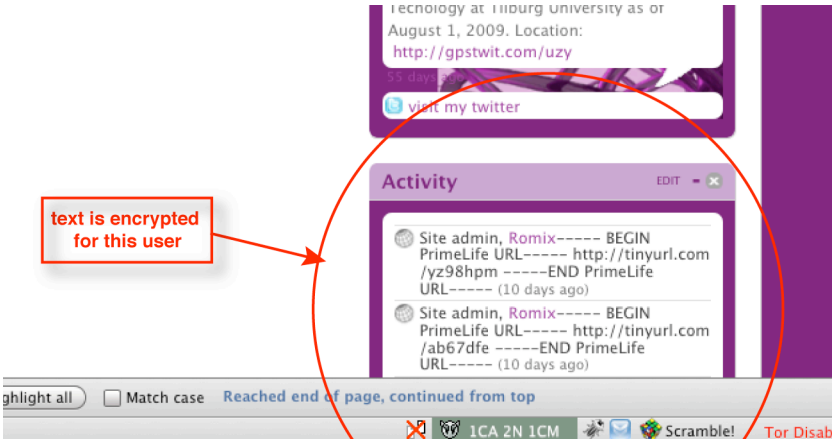


Figure 33: Scramble! is not installed: access is denied; the 'tiny URL' is displayed.

Now, since this encryption tool is built as a browser extension it isn't merely independent of the various social network sites, but could also be used in other kinds of web 2.0 environments, such as blogs, collaborative workspaces such as wikis, and forums. Using it is very simple. After installing the plugin a user can select any kind of text in fill-in fields on internet pages and simply choose 'Scramble!', after which the content will only be readable for those who have the right access key. Moreover, because the extension is integrated into the browser the encrypted content will be decrypted automatically for all authorized users, without their intervention. The exchange of keys runs in the background and requires no particular skills from the owner of the information, nor from those gaining access to it. Our extension is simple and aims at striking the difficult balance between usability and privacy for general users. Since we have used OpenPGP to build the encryption tool it will become available for the open source community after its current testing and fine-tuning phase.

In this chapter we have presented the three demonstrators that we have built in WP 1.2 of the PrimeLife project to contribute to solving issues of privacy and identity management in existing web 2.0 environments, and especially in collaborative workspaces and social network sites. All of the technical details of these three demonstrators, an installation package and the manuals of their respective operations are contained in a separate deliverable, D1.2.2, which accompanies this one. Describing these three demonstrators almost brings us to the end of this deliverable. However, there is one separate issue that we still want to present before we can turn to drawing conclusions on the work conducted in WP 1.2. so far. In the next chapter we present a legal analysis of the use of our encryption tool Scramble!. This research was conducted as a separate branch of work, but we feel it needs to be integrated into this deliverable, since it sheds light on the practices of use for Scramble! and has consequences for its future development and the design of a next version. This is why we will now turn to a legal analysis of Scramble!.

Chapter 8

Legal aspects of Scramble!

As we have argued throughout, this deliverable the rise of web 2.0 has led to new issues regarding privacy and data protection. Internet users provide personal content on a massive scale via web 2.0 platforms, and by doing so they are likely to be confronted with a wide variety of privacy risks. As we have seen in the previous chapter, one possible solution to diminishing privacy risks in web 2.0 is to enable users to *encrypt* the data they share online, for instance in social network sites, but also in other web 2.0 environments. To this end, we have developed an encryption tool called Scramble!. This tool, a Firefox extension, enables users to establish rules for audience segregation, i.e. to disclose information to specifically chosen individuals or collections within a user's list of contacts, such as family, best friends, colleagues, etc. Moreover, the tool enforces these access rules by means of encryption (Beato *et al.*, 2009). Thus, the tool allows users to, for instance, select a piece of text on their social network site profile and choose which contacts or collections are allowed to see that piece of text. Furthermore, it enables users to make data inaccessible to the social network site *provider.* The tool is generic and independent, which means that it can be used on any social network site, provided that a Firefox web browser is used. Notably, the use of the tool is currently limited to encrypting text, but it is likely that in the near future the tool will be capable of encrypting pictures and videos as well.

8.1 Introduction

In this chapter we aim to assess the use of the Firefox social network site encryption tool Scramble! from a legal perspective. The purpose is, *inter alia*, to assess such use in respect of current privacy- and crypto laws and -regulations in Europe and the United States, and to determine whether the use of such a tool in social network sites brings along any – general – legal objections. In doing so, we will presume that the encryption tool is able to encrypt all text, pictures and videos that can be placed on a social network site profile. The social network site that will be used as an example throughout the assessment is Facebook, the largest social network site in the world, with some 400 million members from all over the world.[125] Additionally, a specific

[125] http://www.facebook.com/press/info.php?statistics [last accessed on 25 February 2010]. Note that while Facebook is US-based, approximately 70% of all Facebook users resides outside the US.

analysis will be conducted in relation to the legality of the use of Scramble! from the perspective of Facebook's Terms of Use, which Facebook calls its 'Statement of Rights and Responsibilities'[126].

The research questions that we aim to answer in conducting this assessment are:

- Which legal obstacles or objections might arise when Scramble! would be made freely available for download without cost, on a EU-based website?
- If the tool would be downloaded from EU countries or from the US, which obstacles might occur when a citizen of one of the EU-Member States or of the US would use Scramble! for purposes of privacy protection or privacy control on his Facebook (a US based social network site) profile, all in light of EU and US privacy- and crypto laws and regulations in general and specifically in light of Facebook's Terms of Use?

As appears from the research question, we will focus only on what happens when the tool would be downloaded from within Europe to either a EU member state or to the United States, and the assessment of crypto regulation will thus be limited to this situation. This entails that we will look at European and US domestic regulation and European export regulation. Since privacy regulation in the European Union has been discussed extensively in Chapter 6 (sections 6.2 - 6.7) we will not repeat it here.

Throughout this chapter we will provide arguments pro and contra the use of scramble! in Facebook, as if the Facebook user and Facebook were in a discussion on this use. Since nothing is predefined in law, the arguments of both sides are important in examining the legal status of this encryption tool.

8.2 Crypto regulation

In today's information society, the art (or science) of keeping information secret, also referred to as 'cryptography', has become increasingly important. Nowadays, cryptography mostly revolves around processes of digital modification through which regular information is transformed into cipher text, that is, text is encoded by going through an encryption algorithm. In principle, encoded text can only be decoded by those who have the right key. With regard to the latter feature of encryption two distinctions can be made: *symmetric*-key cryptography and *a-symmetric* or *public-key* cryptography. In symmetric-key cryptography, the sender and receiver of the information share the same key, whereas in a-symmetric or public-key cryptography they use different keys; one *private* key and one *public* key. Here, the public key is used to encrypt the message, while the receiver can decrypt the information with his private (secret) key (cf. Koops, 1999: 35-39).

The public-key encryption method was introduced in 1976 by Whitfield Diffie and Martin Hellman[127] and since then cryptography became more widely used in the private sphere, mainly for reasons of privacy protection. Nowadays, cryptography is available or used on almost every personal computer in the world through a crypto mechanism called 'Transport Layer Security', provided by popular web browsers such as Firefox and Internet Explorer and almost every, if not all, e-mail servers.

Originally, cryptography was used only by governments to keep confidential information secret. With respect to national security, governments wish to preserve information security on the one

[126] See http://pl-pl.facebook.com/terms.php [last accessed on 17 February 2010].
[127] See http://en.wikipedia.org/wiki/Diffie–Hellman_key_exchange [last accessed on 25 February 2010].

hand, while on the other hand they wish to be able to intercept such information of others. This trade-off is clearly reflected in the legislation of most countries: legislators focused on regulating the export of crypto systems, because they want to "*avoid strong cryptography from falling into the hands of foreign powers*" (Koops, 1999: 97). At the same time, most states are reluctant to enact import regulation on crypto mechanisms since these mechanism allow governments to reveal the state of art in foreign encryption technology through cryptanalysis.

Note that this trade-off was limited to legislation for the public sphere – the use of cryptography in the private domain was, and in many countries still is, almost entirely disregarded in legislation. Nevertheless, with the excessive growth of the worldwide use of the internet an additional trade-off, between national security and the private enforcement of the (fundamental) right to privacy and data protection, has come to the fore. Therefore, one might expect that there is an increasing need for domestic regulation with respect to encryption, or to be more specific, legislation regulating the private use of encryption mechanisms. But as said, such civil use of encryption is already widely accessible via web browsers and e-mail servers and this ubiquity makes it impossible to enforce any national regulation, hence the lack of domestic crypto regulation seems reasonably understandable.

One issue that is often regulated domestically is the use of encryption for criminal purposes. The most recent debate on encryption policy concerns the relation between such policy and the enforcement of criminal law, more specifically the extent to which citizens should be confronted with a decryption order in case of criminal suspicion. Note that in certain countries not complying with a decryption order is considered a criminal offence. Another important issue in this debate is the relationship between a decryption order and the right against self-incrimination. While a decryption order is considered to be compatible with the right against self-incrimination in some countries – for instance, in the UK, the Netherlands (in case of terrorist activities), France and Belgium –, in others – for example in the US, at least in certain circumstances – this compatibility is debatable. This issue will be taken up in more detail below.

In the next sections, we will discuss the legal status of the private use of Scramble! in social network sites. We will presume the hypothetical situation that Scramble! is freely downloadable, without any further costs, from an EU-based website and discuss the legal context of this hypothesis from the position of EU and US law. More specifically, we will look at EU domestic regulation in section 8.3, thus assuming the crypto-tool will be used by citizens from the EU member states, and at US domestic regulation in section 8.4, presuming that the tool will be used by US citizens. When the latter would occur, the encryption software could – although this is not as evident as it seems – be exported from the EU to the US, hence the relevant EU export regulations will also be examined. It is debatable whether making a software program available for download to the rest (or part) of the world can be considered as 'export', since the person or company that provides the program does not actively introduce the program in another country. We will go into this discussion in the next section.

We will not assess relevant non-binding international regulations on encryption or the export thereof, such as the *Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies* or the *OECD Crypto Guidelines*, as these regulations (or guidelines) are not directly applicable. As it is up to each Member State to implement these into national legislation, their effects depend on national implementation and the actual effect can differ from country to country.

With regard to the Wassenaar Arrangement – the successor to the *Coordinating Committee for Multilateral Export Controls* (COCOM), signed in 1996 and now counting forty members[128] – it

[128] The participating member states are Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Latvia, Lithuania,

suffices to say that this is the most important piece of crypto-export regulation in the international field. It specifically controls the export of arms and so-called 'dual-use goods'. Dual-use goods are goods, technologies or software that can be used for both military and civil purposes[129] and cryptographic systems fall into this category. The Wassenaar Arrangement has been implemented in the European Union's Commission Regulation (EC) 1334/2000, on which we will elaborate in more detail in the section on EU export regulation.

With respect to the OECD Crypto Guidelines it suffices to say that the Guidelines do not provide any effective direction for (international) crypto regulation and hence its importance in the regulatory field is minor. As Koops rightly remarks, "*The OECD 'guidelines'* […] *do not guide. They leave it to every single state to strike a balance somewhere; virtually any balance, packed in proper rhetorics, will satisfy the OECD principles*" (Koops, 1999: 5).

8.3 EU crypto regulation

In this section we will look into the existing encryption legislation in the European Union from two legislative bodies: the European Union itself and the Council of Europe.

8.3.1 Domestic and export crypto regulation by the European Union

Within the European Union no domestic legislation can be found that is relevant to our case.[130] However, as mentioned, there is relevant EU legislation which regulates the *export* of encryption products of which the most important piece is the *Council Regulation (EC) No 1334/2000 on setting up a Community regime for the control of exports of dual-use items and technology* (hereafter: the 'Council Regulation' or 'Regulation').[131] The Regulation includes, among other things, the Wassenaar Arrangement, and is directly applicable to all EU Member States.

In Article 2(b), the Council Regulation defines 'export' as follows: "*(i) an export procedure within Article 161 of the Community Customs Code; (ii) a reexport within Article 182 of that Code, and (iii) transmission of software or technology by electronic media, fax or telephone to a destination outside the Community; this applies to oral transmission of technology by telephone only where the technology is contained in a document the relevant part of which is read out over the telephone, or is described over the telephone in such a way as to achieve substantially the same result*". The second paragraph of Article 2(c) of the Council Regulation proposes a definition of the term 'exporter': "*any natural or legal person who decides to transmit software or technology by electronic media, fax or telephone to a destination outside the Community*".

First, the definitions show that any interchange of Scramble! within the territory of the European Union cannot be considered as export under the Council Regulation, since both definitions use the phrase: "*to a destination outside the Community*". Hence, the only case in which export restrictions might occur under this Regulation is when the encryption tool would be downloaded from the European Union to another country, in our assessment to the United States particularly.

Luxembourg, Malta, Netherlands, New Zealand, Norway, Poland, Portugal, Republic of Korea, Romania, Russian Federation, Slovakia, Slovenia, South Africa, Spain, Sweden, Switzerland, Turkey, Ukraine, United Kingdom and the United States. See http://www.wassenaar.org [last accessed on 25 February 2010].

[129] See Article 2 Council Regulation 1334/2000.

[130] There is one Resolution on the lawful interception of telecommunications (96/C329/01), which, in relation to encryption, contains requirements for network operators and service providers.

[131] When referring to this EC regulation the author refers to the consolidated version of 2nd February 2009.

We must ask ourselves, then, whether an individual that makes the Scramble! software available on the internet for everyone to download is an 'exporter' and, if the tool would in fact be downloaded, whether the downloading of such program would constitute 'export' under the Council Regulation. In both the definition of 'export' – i.e. under (iii), which is the relevant definition in our case –, and in the definition of an 'exporter', the words *transmission* or *transmit* are used respectively. It appears that making a software crypto-tool such as Scramble! available is, in fact, a transmit – as in the definition of exporter – and that an actual download constitutes a transmission – as in the definition of export. One could argue that downloading a piece of software from a website constitutes a 'transmission', since data is, in face, passed on from the server to the equipment of the downloader and because the server (as an agent of its owner) can withhold the data from being downloaded. The server controls who can download the software or technology and hence controls the export. Therefore, for now we will presume that downloading does involve a transmission as defined here.

The next problem is whether making Scramble! available on an EU-based website involves a transmit "*to a destination outside the Community*", and whether the downloading of that program from another country (in this case: the US) should be seen as a transmission "*to a destination outside of the Community*". We assume that making such program available to the world includes the possible event that the software will be transmitted to other countries. Thus, by making the program available one facilitates export. In this chapter we will assume that this broad interpretation applies, and that, therefore, the Council Regulation applies and will be further assessed in the context of the private use of Scramble! in social network sites.

8.3.2 Export restrictions?

As we have seen in the previous section in principle Scramble! falls under the Council Regulation. Article 3 (paragraph 1) of the Regulation stipulates that "[a]*n authorization shall be required for the export of the dual-use items listed in Annex I*". Scramble! falls under this Annex, more specifically under part 5A002.a.1.a and 5A002.a.1.b (to be read in conjunction with 5D002.c.1), since it uses *hybrid* encryption as we have seen in the previous chapter. Hybrid encryption entails that a combination of symmetric and asymmetric algorithms is used.

However, there are some exceptions to the requirement of prior authorization for export, which are likely to apply to Scramble! and its export. First, the Council Regulation provides that its export controls do not apply to products "*accompanying their user for the user's personal use*".[132] What this phrase exactly means remains unclear from reading the Regulation, but an example that occurs in literature is an installed crypto program on a person's laptop, which he or she moves out of EU territory (cf. Taylor, 1999).[133] With this example in mind we may conclude that since Scramble! is intended for personal use, this crypto tool and its wider dissemination do fall under the 'personal use' exception.

Second, another exception in the Council Regulation can be found under paragraph 2 of the General Software Note under Annex I. It states that the export controls do not apply to software "[i]*n the public domain*". 'In the public domain' is defined in the Regulation as: "*'technology' or 'software' which has been made available without restrictions upon its further dissemination* [whereby] *copyright restrictions do not remove 'technology' or 'software' from being 'in the public domain'*". Since Scramble! is to become available for public use without any further costs

[132] See Annex I, Note 2 in the Dual-Use List Category 5, Part 2, 'Information Security'.
[133] Also see: Koops' 'Crypto Law Survey', http://rechten.uvt.nl/koops/cryptolaw/ [last accessed on 25 February 2010].

and is based on Open Source software, the tool seems very likely to fall under the 'public domain' exception. In consequence, its export would not be restricted by the conditions of the Regulation.

8.3.3 Domestic and export crypto regulation by the Council of Europe

The Council of Europe only has one piece of *domestic* regulation – no relevant export regulation could be found – that is relevant for the use of Scramble! to protect one's privacy, viz. the *Convention on Cybercrime*[134] of 2001. Just like the Wassenaar Arrangement that we've discussed above, the Cybercrime Convention is not directly applicable, but rather has to be implemented by its Member States. Thus, its application depends on the level of implementation in national law. Therefore, we will only discuss it briefly.

In the Convention, the Council tries to strike a balance between "*the interests of law enforcement and respect for fundamental human rights*", including "*rights concerning the respect for privacy*" and the "*the right to the protection of personal data*".[135] Paragraph 62 of the Convention's explanatory report shows how this balance is struck in relation to the use of encryption for the protection of privacy. In this paragraph a distinction is made between punishable acts committed "*without right*" and acts committed "*with right*". It then states the following: "*The modification of traffic data for the purpose of facilitating anonymous communications (e.g., the activities of anonymous remailer systems), or the modification of data for the purpose of secure communications (e.g. encryption), should* in principle *be considered a legitimate protection of privacy and, therefore, be considered as being undertaken with right*" (emphasis added). 'In principle' shows that Member States have some discretion in determining the legitimacy of the use of encryption for privacy purposes.

8.3.4 An obligation to decrypt?

Law enforcement agencies wishing to gather digital evidence face serious problems when coming across computer data that is inaccessible due to encryption. As Aljifri and Navarro state: "*It is evident that cryptography poses an important obstacle for their interests, as any kind of information encrypted using a powerful enough cryptosystem would turn out to be practically unbreakable without the decryption key, thus rendering the electronic wiretapping or computer search useless*" (Aljifri and Navarro, 2003: 197).

As a countermeasure to this problem, Article 18 of Section 2 of the Cybercrime Convention stipulates *inter alia* that "[e]*ach Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: a.) a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium*". In addition, Paragraph 176 of the Convention's Explanatory Reports mentions that "[p]*arties* could *establish obligations that the specified computer data or subscriber information must be produced in the manner specified in the order.*

---

[134] The Convention on Cybercrime was signed by the United States, Canada, South Africa, Japan, and 26 of the 43 Member States of the Council of Europe.

[135] Convention on Cybercrime, CETS No.: 185, 23 November 2001, Preamble. With regard to the right to privacy the Convention refers in its Preamble to "*the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights and other applicable international human rights treaties' and with regard to the right to data protection the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*".

This could include reference to a time period within which disclosure must be made, or to form, such as that the data or information be provided in 'plain text'" (emphasis added). These citations show that the Convention allows Member States to order decryption, but that this possibility should, at least in democratic societies, be subjected in principle to the right against self-incrimination as acknowledged in Article 6 of the European Convention on Human Rights (ECHR). Thus, Article 15 of the Cybercrime Convention reads: "*the establishment, implementation and application of the powers and procedures provided for in [Section 2] are subject to conditions and safeguard provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties*".

Nevertheless, we point out again that the Cybercrime Convention is not directly applicable in the Member States. With respect to the relationship between a decryption order and the right against self-incrimination it must be said that some Member States do, in fact, use this order without it being in violation of Article 6 of the ECHR. As said, in the UK, the Netherlands (in case of terrorist activity), France and Belgium a decryption order is compatible with the right against self-incrimination. Moreover, in other countries, police enforcement may have the authority to give a decryption order to anyone who has the ability to decrypt the cipher text – the suspect excluded.

This means that, in the context of social network sites, online friends who have access to the plain text can be ordered by an enforcement agency to decrypt the encrypted message. Even more disturbing is the fact that, in some countries – for instance in the UK[136] and France[137] – not adhering to such an order is penalized with two and three years of imprisonment respectively, or the suspect can get a higher sanction.

8.4 US crypto regulation

In the next section we will assess the relevant domestic US encryption regulation, assuming that a US citizen has downloaded Scramble! from a EU-based website. Note that the United States have no import restrictions regarding encryption, hence the actual transmit into the US shall not involve any legal obstacles.

There is however some, though no extensive, domestic regulation with respect to encryption. In the late 1990s a number of Bills were introduced on (domestic) crypto-regulation; these Bills mainly sought to penalize the use of encryption to conceal information related to criminal offences[138], yet at the same time aimed at loosening up the existing export controls for cryptosystems or software generally available in the international market.[139] Some proposals even specifically addressed the enhancement of, or even a right to the protection of privacy by means of encryption.[140] In the end, none of these Bills were passed and as a result the current amount of domestic encryption regulation, to be viewed next, is limited.

---

[136] See Regulation of Investigatory Powers Act 2000 (2000 Chapter 23), Part III, Article 53 (1) and (5).
[137] See Law 2001-1062 of 15 November 2001 on daily security, Article 31(II).
[138] For instance, the E-PRIVACY Act (1998); the Security And Freedom through Encryption Act (SAFE) (1996/1997/1999); and the Encryption for the National Interest Act (1999).
[139] For example, the E-PRIVACY Act (1998); the Security And Freedom through Encryption Act (SAFE) (1999); the Promote Reliable On-Line Transactions to Encourage Commerce and Trade (PROTECT) Act (1999); the Encrypted Communications Privacy Act (Leahy Bill) (1996/1997); and the Encryption for the National Interest Act (1999).
[140] For instance, the E-PRIVACY Act (1998); the Security And Freedom through Encryption Act (SAFE) (1996/1997/1999); the Encrypted Communications Privacy Act (Leahy Bill) (1996/1997); the Electronic Rights for the 21st Century Act (1999); and the Encryption for the National Interest Act (1999).

8.4.1 Encryption and the Digital Millennium Copyright Act

Until now, we have looked at Scramble! as a means to protect one's privacy in social network sites. However, the content that social network site users post on their profile page is covered, at least in most cases, by intellectual property rights, or IP rights for short. Think, for example, of blog posts or self-made pictures or videos. Bearing this in mind, encryption could function not only as a privacy enhancement mechanism, but also as an IP rights protection mechanism. Following this line of reasoning, the *Digital Millennium Copyright Act* (hereafter: DMCA) – enacted by US Congress in 1998 – would apply to encrypted content in social network sites, since it regulates, *inter alia*, copyright-protection systems such as encryption. More specifically, section 1201 of the DMCA entitled *Circumvention of copyright protection systems* applies. According to section 1201(a)(1)(A) of the DMCA, "*circumvent*[ing] *a technological measure that effectively controls access to a work*" protected by copyright is prohibited. The rationale behind this is to "*prevent unauthorized access to copyrighted works*" and to prevent "*the theft of copyrighted works*".[141]

Thus, it can be argued that when users would make use of Scramble! when adding content or exchanging messages on Facebook or other social network sites, the providers of these sites have no rights to decrypt the encrypted content, for instance through cryptanalysis, nor to block the use of Scramble! without prior permission of the copyright holder (i.e. in this case the user). To clarify, the DMCA defines the circumvention of a technological measure in Sec. 1201(a)(3)(A) as follows: "*to 'circumvent a technological measure' means to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner*". What's more, anyone who violates Section 1201 of the DMCA "*willfully and for purposes of commercial advantage or private financial gain*" can be penalized with a fine up to $500,000 for a first offence, or imprisoned for up to 5 years for repeated offences, according to Section 1204 of the DMCA.

However, Facebook and other social network sites could argue that prior permission for – possible – decryption was given by the copyright holder by agreeing to Facebook's general terms and conditions, with which the Facebook users grant Facebook an IP-license on their profile-content. Facebook writes: "*For content that is covered by intellectual property rights, like photos and videos ('IP content'), you specifically give us the following permission, subject to your privacy and application settings: you grant us a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook ('IP License')*".[142]

This raises an interesting question. To what content does the license agreement relate? Is it the source data as entered by the user in their web browser (human readable text), or is it the content as stored on Facebook's servers (scrambled text)? If the former applies, Facebook could require users to provide them unencrypted content. In the latter case, Facebook would have a license to use the scrambled content, which obviously is of no use to them because Facebook has no means (in a practical sense) to decrypt the data, and the DMCA would not permit breaking the encryption. We consider the latter interpretation to be valid, since Facebook's terms in general relate to content stored on their servers.

---

[141] See http://www.copyright.gov/reports/studies/dmca_report.html#N_5_ [last accessed on 1 March 2010].
[142] See http://pl-pl.facebook.com/terms.php [last accessed on 17 February 2010].

8.4.2 Encryption and US criminal law: A decryption order?

In this section we will look at two specific Chapters of the US Code, which determine the extent to which law enforcement agencies can intercept and disclose electronic communications, or order such disclosure from individuals, in our case, Facebook. First, we will look into Title 18, Chapter 119, which is entitled *Wire and Electronic Communications Interception and Interception of Oral Communications*. After this, we will address the Electronic Communications Privacy Act of 1986 as integrated in the US Code, Title 18, Chapter 121, which is entitled *Stored Wire and Electronic Communications and Transactional Records Access*. Our aim is to clarify the extent to which users and Facebook, as a so-called 'remote computing service'[143], can be confronted with an order to deliver encrypted communications or other data in decrypted form for purposes of criminal investigation.

Articles 2516 (2) and 2516 (3) of the U.S. Code (Title 18, Chapter 119) state that the interception of electronic communications is allowed "*by investigative or law enforcement officers*" in case of certain criminal offences, for instance in case of a felony. Next, article 2517 clarifies to whom these intercepted communications can be *disclosed*, which implies that the communication should be disclosed in the form as it is intercepted. This means that encrypted communication should be disclosed in encrypted form and no decryption order can follow from this paragraph. Moreover, article 2517(4) explicitly states that: "*No otherwise privileged wire, oral, or electronic communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character.*" From this article it appears that encrypted data will not lose their privilege when such data would be intercepted by a law enforcement agency.

The Electronic Communications Privacy Act states *inter alia* in article 2703 that under certain conditions "*a governmental entity may require the disclosure by a provider of electronic communication service*" or "*a provider of remote computing service*" of the "*contents of a wire or electronic communication*". Again, the article does not seem to imply an obligation on the part of Facebook to disclose the data it has stored in encrypted form, although the word 'contents' might possibly allow for another conclusion. When Facebook would be ordered to decrypt communication it would be confronted with serious practical problems since Scramble! provides for quite strong protection, making it almost impossible to crack the key, and the feasibility of such an order, therefore, is questionable in this regard.

8.4.3 Case law: A decryption order and the right against self-incrimination

An interesting case to mention with regard to decryption and the right against self-incrimination, as granted by the Fifth Amendment, is *United States v. Boucher – 2007 WL 4246473*, also referred to as Boucher I (D. Vermont, Nov. 29, 2009).

---

[143] See US Code, Title 18, Chapter 121, § 2711. (2): "*the term 'remote computing service' means the provision to the public of computer storage or processing services by means of an electronic communications system*".

In this case, the defendant, Boucher, was arrested for bringing child pornography into the United States. He had crossed the border from Canada to the United States carrying a laptop that contained child pornography. At the time of the border search, the drive containing the child pornography files was accessible without the use of a password. Boucher even helped the border patrol officers in finding and accessing the relevant drives but the agents never saw him entering a password. Later, when the laptop was handed over to the Vermont Department of Corrections for further investigation, the same drive search appeared to be inaccessible due to the use of PGP – a form of encryption – and a password was required to access the drive. Since it is nearly impossible to access the files without the password, Boucher was ordered by the grand jury to "*provide all documents, whether in electronic or paper form, reflecting any passwords used or associated with*" the seized laptop. Boucher labelled the subpoena as a violation of the right against self-incrimination as stated in the Fifth Amendment. Afterwards, the government agreed that providing the decrypted content – and thus not the password itself – was sufficient in adhering to the subpoena. The question that the Court then had to answer was "*whether compelling Boucher to enter the password into the laptop would violate his Fifth Amendment privilege against self-incrimination*."

The District Court of Vermont argued that "[c]*ompelling Boucher to produce the password compels him to display the contents of his mind to incriminate himself*" and the Court decided to quash the subpoena. The United States appealed and in *Boucher II – re Boucher, 2009 WL 424718* (D. Vermont, Feb. 19, 2009) – the Court reversed the ruling in Boucher I, directing Boucher to "*provide an unencrypted version of the Z drive viewed by the ICE* [Immigration and Customs Enforcement] *agent*". The Court quoted *United States v. Fox – 721 F.2d 32, 36* (2d Cir.1983) and stated that: "[t]*he act of producing documents in response to a subpoena may communicate incriminating facts 'in two situations: (1) 'if the existence and location of the subpoenaed papers are unknown to the government'; or (2) where production would 'implicitly authenticate' the documents'*."

The Magistrate in the lower court's proceedings found that the government did not know the location or contents of the hard drive, and that Boucher was therefore protected from compelled disclosure by the Fifth Amendment. However, the District Court noted that the government must only show "*with reasonable particularity that it knows of the existence and location of subpoenaed documents*." Because border patrol agents had viewed at least one image of child pornography on the hard drive in question, the court concluded that Boucher did not have Fifth Amendment protection. Thus, according to US case law, a decryption order does not violate the right against self-incrimination when a suspect initially cooperates in showing a part of the illegal content.

Note that this case does not reveal to what extent it is allowed to order a user's contact who can see the plain decrypted messages or other content sent via Facebook or other social network sites to decrypt them.

8.5 Scramble! A violation of Facebook's Terms of Use?

As we have seen in this deliverable, social network sites such as Facebook engage in a difficult balancing act between granting access rights to information stored in their network to third parties, and protecting the data individuals share in that network. On the one hand, the business model of social network sites builds on advertising revenues and targeted advertising, facilitated by the sale of users' information. On the other hand, social network sites have a responsibility to protect their

users, and are fully aware that significant privacy breaches by third parties can cause users to massively flee the system and find a new network elsewhere. Thus, social network sites know that without their content they have no value and safeguarding the content of their network is a crucial business goal.

Seen from this perspective, it seems likely that social network sites such as Facebook would strongly oppose the use of Scramble! within their domain, since it shields the content that users place on their profile pages from the provider's access. In this section we will investigate whether Facebook can block, forbid, or prevent the use of Scramble! based on its Terms of Use[144]. Before we begin, we point out that Facebook's Terms of Use are legally contractually binding. Users have to accept these Terms and cannot deviate from their rules and stipulations. In this section we will look at Facebook's Terms of Use in more detail.

In article 1 of the Terms of Use, Facebook states that the users' privacy is important to the company, but that the only possible way to control their privacy on Facebook is by the privacy settings that Facebook opts them to use. This means, in fact, that Facebook determines the scope of the users privacy. Facebook explicitly states as much in article 2 of the Terms of Use, and in the same article it also claims the following: "*You own all of the content and information you post on Facebook, and you can control how it is shared through your privacy and application settings.*" This claim is followed by the statement that the user permits Facebook an IP License over all content posted on the social network site, which we've discussed above (see section 8.4.1). Facebook continues: "*This IP License ends when you delete your IP content or your account unless your content has been shared with others, and they have not deleted it. When you delete IP content, it is deleted in a manner similar to emptying the recycle bin on a computer. However, you understand that removed content may persist in backup copies for a reasonable period of time (but will not be available to others). When you add an application and use* [the] *Platform, your content and information is shared with the application. We require applications to respect your privacy settings, but your agreement with that application will control how the application can use the content and information you share*".

Facebook could argue that any means of user privacy control outside the designed Facebook privacy settings are in violation of the Terms, since it is stated that this scope of privacy is controlled by the privacy and application settings.

Furthermore, the use of a social network site crypto tool such as Scramble! would seriously dilute the meaning and scope of the IP-license given by the Facebook user over its profile content. After all, when data is encrypted and therefore inaccessible to Facebook it would no longer have any ability to monitor such content for violations of their Terms (see article 3) or violations of law, at least regarding that particular content.

A Facebook user using Scramble! could be alleged of violating article 4 (5), which requires users to "*keep* […] *contact information accurate and up-to-date*", since encrypting such contact information would render the information inaccessible and invisible to Facebook, thus inaccurate or not as up-to-date as Facebook intends it to be. Additionally, article 4 (1) states that Facebook users must "*provide their real names and information*", and arguably encrypting such data could be seen as violation of this article.

An interesting issue with respect to using Scramble! in Facebook is related to article 5 (2) of the Facebook Terms of Use: "*We can remove any content or information you post on Facebook if we believe that it violates this Statement*". Facebook cannot see the actual content of the data encrypted by Scramble!. since what remains after the data has gone through the encryption algorithms is cipher text (see the description of Scramble! in section 7.3.5). Nevertheless, the scrambled data is stored on the Facebook servers and could easily be detected. If Facebook would

[144] See http://pl-pl.facebook.com/terms.php [last accessed on 17 February 2010].

feel, for any reason, that posting encrypted content is in violation of their Terms – e.g., because they have no ability to monitor such encrypted data – it could remove this content.

The argument that we posed earlier, saying that Scramble! does not only protect users' privacy but can also serve as an intellectual property rights protection mechanism, might be countered by the article 5 (3) of Facebook's Terms of Use: "*We will provide you with tools to help you protect your intellectual property rights*." This article implies, Facebook could argue, that the protection of intellectual property rights on Facebook is limited to the tools Facebook provides, and hence that no outside tools may be used for the same purposes. On the other hand, an interpretation that Facebook provides at least some tools for protecting the user's intellectual property rights, apart from what the user can do herself, is also possible.

Another possible violation could lie in the fact that with encryption, users can encrypt their name and profile picture.[145] Article 10 of the Terms of Use, entitled 'About Advertisements on Facebook', states the following: "*Our goal is to deliver ads that are not only valuable to advertisers, but also valuable to you. In order to do that, you agree to the following: You can use your privacy settings to limit how your name and profile picture may be associated with commercial or sponsored content served by us. You give us permission to use your name and profile picture in connection with that content, subject to the limits you place* […]". Subparagraph 1 expresses once more that the scope of the user's privacy is determined by the options Facebook provides through its privacy settings. The second sentence of this subparagraph states clearly that a user allows Facebook to use[146] their (real) name and profile picture, yet this use can be limited by the privacy settings. Additionally, it is interesting to note that the privacy settings do not allow users to determine the (non)visibility of their profile picture and name which means that this data is always visible to anyone; however, users can determine "*who can see* [their] *search result on Facebook*" (i.e. either 'everyone'; 'friends of friends' or 'friends', but never a customized set of friends), and whether or not users "*allow search engines to access* [their] *publicly available information*".[147] Publicly available information includes "*Name, Profile Picture, Gender, Current City, Networks, Friend List, and Pages*".

It seems obvious that Facebook does not want users to enhance their privacy through any other means than the ones that Facebook itself provides. If users would do so on a massive scale, the economic value of Facebook – i.e. their value in terms of possessing the data of millions of users, useful for purposes of targeted advertising and profiling – would seriously drop. Encrypting data would undermine the main goal of Facebook, which is (as stated in article 10) "*to deliver ads*". Additionally, disabling Facebook's use of users' profile names and pictures clearly constitutes a violation of article 10 (1) of the Facebook Terms.

Another interesting paragraph in the Facebook Terms is article 14: "*If you violate the letter or spirit of this Statement, or otherwise create possible legal exposure for us, we can stop providing all or part of Facebook to you*". Essentially Facebook can deny its service to its users for any reason it deems necessary, since the phrasing "*spirit of this Statement*" can be interpreted in any way. Hence, if Facebook were to consider the use Scramble! inappropriate for its own business model or service deployment, since it disables the company from seeing the content of messages or other posting, it would likely block those users using Scramble!.

---

[145] The current version of Scramble! cannot encrypt pictures or videos but it is highly likely that this will be possible in the near future.

[146] Facebook defines 'use' as "*use, copy, publicly perform or display, distribute, modify, translate, and create derivative works of*".

[147] See www.facebook.com. To see these features one needs to be logged in with a Facebook account.

8.6 Conclusions

Scramble! provides its users with means to control who can access their content on web 2.0 applications. In this sense it empowers users to live up to the data protection principles, and especially the principles of data minimization, minimal disclosure to third parties - and additionally data control and security of data processing. These principles thus provide support for the use of Scramble! and its likes in web 2.0 applications such as social network sites. SNS providers, at least according to the DPD, have no positive right to the data of the SNS users. Rather, it must be seen as a privilege to make use of this information, and when a SNS user would limit the SNS provider's ability of getting this information the provider would simply have tough luck.

Having said this, there may be other legal obstacles that hamper the implementation and use of Scramble!. In this chapter we have looked at some of the potential legal obstacles that may prevent users from installing and using Scramble! in social network sites, with the popular Facebook social network site as an example.

Since Scramble! implements crypto tools, crypto curbing legislation was addressed. We assume that Scramble! would be made available for download to the public from an EU based server. Download from the application to a non EU-member state (a third country) would constitute export of the application. Neither Council Regulation (EC) No 1334/2000 on setting up a Community regime for the control of exports of dual-use items and technology, nor the Convention on Cybercrime of 2001 seem to stand in the way of downloading or exporting Scramble! to third countries.

Another matter is whether Scramble! users can be required to hand over decrypted content by law enforcement agencies. The answer to this question, within the EU, depends on the transpositions of the Convention on Cybercrime into national law. In some countries, for instance in the UK, The Netherlands, Belgium and France, citizens can be forced to provide decrypted content.

With respect to US Scramble! use an interesting issue relates to section 1201(a)(1)(A) of the Digital Millennium Copyright Act (DMCA). When users encrypt their content, is Facebook then permitted to (try and) decrypt their content? The answer to this question is not straightforward but we are inclined to conclude that Facebook only gains an IP license towards the material stored on their servers. Section 1201(a)(1)(A) DMCA provides the user with means to legally prevent Facebook from decrypting their content without their consent.

Based on an assessment of the US Code (Title 18, Chapter 119) and case law, there seems to be no reason to assume that Facebook or user can be forced to provide decrypted content when required by a law enforcement agency, unless the suspect cooperated with law enforcement agencies early on in the process.

A final issue that was addressed is whether Facebook's Terms of Use stand in the way of adopting Scramble! as this tool would potentially undermine Facebook's business model. The spirit of the terms, as well as some concrete provisions lend hand to the conclusion that Facebook can indeed take action to prevent users form encrypting content, for instance because the maximum level of privacy is provided by Facebook itself, and users are required to keep certain information accurate – which is not the case when it is encrypted.

Chapter 9

Conclusions

In this deliverable we have investigated privacy issues and issues surrounding the management and expression of identities in web 2.0 environments, with a focus on collaborative workspaces (such as wikis, forums, weblogs, file sharing environments) and social network sites (such as Facebook, Friendster, MySpace and LinkedIn). In this last chapter we will summarize these findings (section 9.1) and draw conclusions on the basis of these findings (section 9.2).

9.1 Findings of this deliverable

In this section we will summarize the most important findings of this deliverable. With each finding we will refer back to the section in which it is discussed in more detail.

9.1.1 Web 2.0

The focus of this deliverable (and of much of the PrimeLife project in general) is on web 2.0 technologies, that is technologies related to or embedded in the second generation of the internet. We began this deliverable with a discussion of the key characteristics of web 2.0. These include the following:

- Internet users have become actively involved in the creation and management of content in the new internet environments that can collectively be called 'web 2.0'. So-called 'user-generated content' is created by the users of internet applications themselves, thereby turning these formerly passive consumers into 'prosumers', a contraction of producers and consumers (section 2.1.1);
- Web 2.0 is called the 'social web' since some of the key features of this next generation of the internet aim at starting, supporting or enhancing the management of social relationships (section 2.1.2);
- Co-operation between users is another key element of web 2.0. Users do not only create and manage content themselves to a larger degree than in the first generation of the internet, but

they also do so collectively. Thus, a significant portion of the content that is created and managed by users in web 2.0 is the result of their collective efforts (section 2.1.3);

- Whereas the first generation of software producers built internet technologies that consisted of downloadable, stand-alone, packaged software systems, such as browsers, in web 2.0 users access software that is embedded in the internet itself, and use these applications as services (section 2.1.4).

Web 2.0 consists of a wide variety of different environments that share the four characteristics we have just discussed and hence can be labelled 'social software'. Social software is software that focuses on one or more of the following aspects: (1) content management; (2) relationship management; and/or (3) management of the self (or self-presentation) (section 2.2). In this deliverable we have focused on two of the most widespread examples of: collaborative workspaces and social network sites. These two focal technologies can briefly be summarized thus:

- Collaborative workspaces are infrastructures and platforms that enable users to work together, for instance in gathering information or creating content in a collaborative manner but also in sharing data with each other. Examples include wiki systems, collaborative real-time editors, forums, weblogs and file sharing systems (section 2.3);
- Social network sites are internet environments in which users can (1) create a profile page to present themselves to others; (2) engage in social interaction with other through a list of contacts or 'friends' and (3) access other individuals' list of contacts to find new connections and expand their own network. Examples include Facebook, MySpace and Friendster (section 2.4).

9.1.2 Identity in web 2.0

The popularity of social network sites and (some kinds of) collaborative workspaces is an indicator of the fact that individuals feel these types of environments enable them to construct, manage, express, and share their identities with others. Some types of online environments, for instance online worlds such as Second Life, enable users to experiment with alternative or fictional identities, whereas weblogs and (some) social network sites invite them to present their 'real life' identities in a virtual world. Identity management is certainly one of the most important aspects of participating in social network sites – users create a profile page and fill it with information about themselves, thus actively engaging in self-presentation, which in turn may reflect back on them and influence their sense of self. In collaborative workspaces identity management is not the most important feature, since most collaborative workspaces revolve around the creation of content, rather than around the individuals who contribute to them. However, in some collaborative workspaces, such as weblogs, identity is an important factor indeed (section 2.5).

9.1.3 Privacy and web 2.0

'Privacy' is one of the most complex and contested concepts of our time, especially in light of the rise and massive spread of information and communication technologies. It has a wide variety of meanings (section 3.1), for instance:

- "*the right to be let alone*" (Warren and Brandeis, 1890);

- "*the ability to control and limit* physical*,* interactional*,* psychological *and* informational *access to the self or one's group*" (Burgoon et al., cited in Paine *et al.*, 2007: 526, emphasis in the original); or
- "*the freedom from unreasonable constraints on the construction of one's own identity*" (Agre and Rotenberg, 1997: 7).

These definitions reveal that discussions on privacy often revolve around the idea that privacy is the right to protect personal information, or to limit access to oneself, or to keep secrets, or alternatively, that it relates to differing degrees of intimacy that each individual engages in in his or her social life. In this deliverable we have chosen to align our interpretation of privacy with that of Helen Nissenbaum, who defines privacy as 'contextual integrity'. The key idea in this interpretation is that information is never 'personal' or 'sensitive' as such, but only contextually so. For instance, individuals do not mind sharing medical information with their doctor, but they do mind sharing it with their insurance company. Sharing this type of information with the latter is considered to be a violation of their contextual integrity (section 3.1.3).

Debates on privacy often contrast the value of respecting individuals' privacy with that of safeguarding collective security. We have argued that this is the wrong opposition because it assumes that protecting privacy is unnecessary if individuals have 'nothing to hide', i.e. if they have not committed or planned any crimes or offensive behaviours. The privacy-as-contextual-integrity perception shows how flawed this idea is: we all have something to hide, since we all want to keep some information private in some contexts (but not in all contexts) (section 3.2).

Privacy has especially become a topic of concern in a world of high technology, for the following reasons (section 3.3):

- Information and communication technologies enable us to effortlessly collect, copy, link and distribute information on a massive scale;
- Using these technologies enables us to store information indefinitely (at least in principle, if not always in practice), thus undermining the 'right to be forgotten';
- Since everyone can participate in online environments such as collaborative workspaces and social network sites individuals can easily damage the reputation of others, and it is difficult (if not outright impossible) to make such damage undone;
- When using the internet individuals often leave digital traces and personal information behind, without realizing it;
- Both technologies themselves and their human users are fallible, thus generating a mixture with possibly harmful consequences.

9.1.4 Privacy in collaborative workspaces

When analyzing privacy issues in collaborative workspaces we must begin by establishing which parties are the most important stakeholders in these environments. We distinguished between (1) third parties; (2) providers; and (3) users (section 4.1). We defined a number of privacy protection goals, which included the following (for the complete list Table 3 see in section 4.2):

- Confidentiality, that is, whether or not the owner of the data can keep his data private or disclose it only with active consent to individuals of his choice;
- Anonymity, i.e. whether an individual can participate anonymously in a collaborative workspace;

- Unlinkability, that is, whether individual items of content posted by a single individual cannot (collectively) be traced back to that individual; and
- Availability, which ensures that a user can always access his own personal data.

We have tested these goals in two existing popular examples collaborative workspaces: Wikipedia, the internet encyclopaedia (section 4.3), and phpBB.de, a German forum for software developers (section 4.4). We found that in both cases many of the privacy protection goals we formulated were not met, i.e. that the privacy of individuals was under threat in these sites, and that threats came from three different directions: (1) third parties, (2) the providers and (3) other users of the same platform. Our recommendations with respect to solving some of these issues, and the demonstrator we have built to exemplify a set of these solutions, will be discussed in the next section of this chapter (sections 9.2.1 and 9.2.2 respectively).

9.1.5 Privacy in social network sites

In recent years privacy issues in social network sites have received considerable media attention. A wide variety of privacy issues exist in these popular environments, and they come from different directions: (1) from individual users themselves or other users of the same social network sites; (2) from the providers of these sites; and/or (3) from third parties. We analyzed privacy issues from each of these angles. First, users may generate privacy problems for the following reasons (section 5.2):

- They lack an overview of the size and makeup of the audience that can access the content they post on their profile pages;
- They lack mechanisms to make different sides of themselves visible to different audiences (for instance only showing work-related information to colleagues and only showing holiday pictures to friends and family), which leads to what has been termed 'context-collision';
- Information persists in online environments and may thus come to haunt them years down the line outside the context for which it was originally intended;
- Social network sites invite peer surveillance, snooping and gossiping, thus enhancing the risk of privacy violations for others;
- Users only have limited control over the image that is presented of them in social network sites. Other users can post comments, place pictures of them online, or 'tag' content in which they appear, without the user's knowledge and largely outside his sphere of control.

Providers, in turn, can also harm the privacy of users in social network sites (section 5.3). They have access to all the information users post online and hence can build up quite extensive user profiles. It can sell these profiles to third parties for targeted advertising practices. Last, third parties themselves can affect the privacy of users in social network sites (section 5.4). For one, they can combine information from multiple separate social network sites into one user profile, thus diverging a much more detailed and complete picture of the user behind the various profiles in each site. Alternatively, they can use information from within individual social network sites as applications to enhance other websites outside the social network site domain. In both cases information about individual users may become accessible to audiences that did not originally have access to them.

Different *types* of data can be distinguished in social network sites (section 5.5), viz. (1) private data (data the users does not choose to share, for instance his date of birth); (2) data that is shared with a limited group of people, or semi-public data; and (3) public data, i.e. data that is shared with everyone. Privacy issues emerge especially when data that is shared with a limited audience is made public by other users, or when data that was intended to be private is made public to a limited audience or to everyone by other users. Based on these findings we formulated a number of privacy protection goals for social network sites (Table 8 in section 5.6), which include:

- Confidentiality, which means that data is protected against undesired access of others, both from inside the social network site and from outside;
- Integrity, which means that in social network sites data is protected against unsolicited changes made by other users, the provider or third parties;
- Availability, which means that data is protected against (temporary) disappearance from the social network site due to actions of other users, the provider or third parties.

From these privacy protection goals we have distilled a number of requirements for privacy-enhances social network sites, which we have put into practice in our social network site demonstrator Clique. Both the requirements and the demonstrator itself will be discussed in the second part of this chapter (sections 9.2.3 and 9.2.4 respectively).

9.1.6 Legal issues in social network sites and collaborative workspaces

There are a number of different pieces of European legislation that apply to social network sites and collaborative workspaces. These include, in summary:

- The Data Protection Directive (95/46/EC) (section 6.2): this directive defines a number of different roles with respect to data dissemination and data protection, for instance that of the 'data controller' and the 'data processor'. These roles are relevant in collaborative workspaces and social network sites as well. Moreover, the Data Protection Directive stipulates the principles of data processing, that is, which rights do data owners have when sharing their data, how should data be treated by providers etc.
- The e-Privacy Directive (2002/58/EC) (section 6.4): this directive formulates regulations with respect to, *inter alia*, location-based services (LBSs) and SPAM, which is also applicable to social network sites and collaborative workspaces;
- The Data Retention Directive (2006/24/EC) (section 6.5): this directive stipulates which data should be retained, how they should be stored, by whom, for how long, and who has access to them. Since large amounts of personal information are shared in social network sites and, to a lesser degree collaborative workspaces, this directive applies to these domains as well;
- The e-Commerce Directive (2000/31/EC) (section 6.6): this directive is relevant to social network sites and collaborative workspaces since it regulates the liability of Internet Service Providers (ISPs) and specifies their responsibilities and rights with respect to the monitoring of content created in their domains;
- The Copyright Directive (2001/31/EC) (section 6.7): this directive defines rules with respect to copyright, which are relevant to social network sites and collaborative workspaces as well, since the users of these domains may upload content over which they have no copyright.

Legal issues are more likely to arise in social network sites than in collaborative workspaces, since individuals generally share much more detailed personal information in the former than in the latter, and also because in social network sites often a number of services is combined, thus complicating issues of responsibility and liability, and generating more options for breaching users' privacy. Specific legal issues that arise in social network sites (section 6.8) include the following:

- Tagging: users can disclose others' personal details (name, e-mail address) by tagging information such as pictures or text disclosed in social network sites;
- It is not always clear to users whether the profile page of a social network site should be considered a public or a private space.

9.1.7 Legal issues with respect to encrypting information in web 2.0

One of the ways in which web 2.0 users could protect their privacy is by using encryption tools to shield off their information from the prying eyes of providers or third parties. When using such tools only the sender and receiver of the information would have the correct 'key' to decrypt the information; all others would see, for instance, a blurb of gobbledygook or an inaccessible hyperlink. In WP 1.2 we built a demonstrator with which such encryption practices could become reality, called Scramble!, which we will discuss in more detail in section 9.2.5 below. We have also conducted a legal analysis of the use of this tool in social network sites, with a focus on Facebook.

Since encryption has only very recently started being deployed on a large(r) scale by individual users of information and communication technologies there is not much legislation in this area yet. However, both in the European Union and the United States there are some pieces of regulation that would apply to the use of our demonstrator Scramble!. First, in the European Union (section 8.3) there is regulation with regard to the export of encryption tools from the EU to other countries. Moreover, there is regulation with respect to the obligation to decrypt: there are rules regarding the question of whether or not law enforcement officers can force individuals to decrypt an encrypted message, for instance when there is a suspicion of a crime or offence. Second, in the United States there are also different pieces of legislation that may apply to Scramble! and its use (section 8.4). In the United States, too, there is regulation with respect to orders to decrypt encrypted messages, and there is legislation that balances decryption orders with individuals' right against self-incrimination.

When looking at the Terms of Use of the largest social network site in the world, Facebook, it is clear that using Scramble! clashes with the goals of this social network site's provider (section 8.5). Facebook's providers build their business model on gathering as much personal information in their network as possible, so that they can sell this information to third parties for targeted advertisement and profiling purposes. However, when users use Scramble! it becomes impossible for the provider to see the content of their postings. This not only undermines Facebook's responsibility with respect to moderating the content of their domain, but also undercuts their business model. Therefore, it seems likely that Facebook will not encourage the use of Scramble! within their site, or will even actively combat it, despite the fact that it greatly strengthens the privacy of users.

9.2 Conclusions on the basis of the findings

In this second part of the last chapter we present a number of conclusions and recommendations. These are based on the findings that we have described in the first part of this chapter.

9.2.1 Solutions for privacy issues in collaborative workspaces

In Table 6 of section 4.6 we formulated a long list of general requirements that collaborative workspaces should (or could) meet to enhance the protection of privacy of their users. This list was based on the privacy protection goals that we had formulated earlier and which we have summarized above in section 9.1.4. Some of the key requirements include:

- Enhancing confidentiality in collaborative workspaces, for instance by raising the user's awareness of the potential audience that can read his or her posts, and by facilitating options so that the user can decide to whom he wishes to disclose the content he or she posts;
- Enhancing anonymity, not only by making it possible to contribute to collaborative in anonymous way but also by raising user awareness by providing feedback with regard to the level of anonymity (or non-anonymity) when posting content in a collaborative workspace;
- Enhancing unlinkability by improving users' protection against surveillance by third parties or providers;
- Enhancing availability by the creation of regular backups and through distributed storage.

The complete list of general requirements is listed in Table 6 on page 91.

From this list of general requirements we distilled one specific mechanism that would greatly increase the privacy protection of users in social network sites: the use of access control mechanisms. This would enable users to decide who can access the content they post in a collaborative workspace, thus raising awareness of the audience and facilitating a more precise demarcation of the intended audience from the perspective of the user. We set out to build such an access control mechanism and will describe it in the next section.

9.2.2 Demonstrator 1: the phpBB extension

The phpBB extension that we built in WP 1.2 is the first of three demonstrators. As the name reveals it was built for the popular internet forum phpBB. It has two central features:

- It enables users to specify an access control policy in the forum phpBB, thus determining who sees the information they post in the forum. To accomplish this the extension builds on existing PRIME modules (sections 7.1.2 - 7.1.5);
- It raises user awareness by providing feedback with regard to the visibility of the posted content, i.e. it provides feedback on who the audience is that can see the posted message.

9.2.3 Solutions for privacy issues in social network sites

Similar to the table of requirements for collaborative workspaces that we discussed above we also formulated a table of requirements for privacy-enhanced social network sites. This is Table 9 in section 5.7. The most important requirements in that list are:

- Enhancing confidentiality, most importantly through raised user-awareness with respect to the audience of information posted in their social network site profile, through the provision of mechanisms to cluster and diversify between different groups of contacts in line with those a user has in real life, and through the provision of mechanisms to mimic 'audience segregation' in social network sites (i.e. creating separate social contexts);
- Enhancing availability by making it easier for users to modify and remove profile data or even their entire account;
- Enhancing unlinkability by providing better protection against surveillance and profiling by providers and third parties.

The complete list of requirements for privacy-enhanced social network sites can be found in Table 9 on page 117.

9.2.4 Demonstrator 2: Clique

To put a number of the requirements we formulated in Table 9 into practice we built our own social network site called Clique (www.clique.primelife.eu). This social network site has the following key features (sections 7.2.3 - 7.2.5):

- It enables users to create 'collections', that is, it provides them with an opportunity to cluster contacts into separate groups, to which they can then choose to disclose information. Thus, users can set up fine-grained access control to the content they share via their profile page. For instance, they can share their holiday picture with family only (or even with specific members of the family and not others), and their work-related content with their colleagues or former colleagues;
- Users can contextualize their profiles further by creating different 'faces', each representing a different social sphere in which they also participate in real life. For example, they can create a 'professional' face in which they only disclose their professional identity, or a 'private' face in which they only disclose more personal information. Collections and contacts are attached to specific faces, thus further decreasing the chances of (accidental) information spill;
- Users can set the access rights to each item of information they post in their social network site profile. They can choose in which face they want to disclose it, to which collection(s) and/or to which individuals. They can also explicitly block individuals or collections from seeing the information.

9.2.5 Demonstrator 3: Scramble!

The third and final demonstrator we built in WP 1.2 is called Scramble! and can be used in collaborative workspaces, social network sites and other web 2.0 environments (sections 7.3.2 - 7.3.5). Scramble! is an encryption tool that enables users to encrypt any information typed into

interactive fields, so that only the user himself (sender) and his intended audience (receiver) can access it, because they have the right access key. All others see scrambled text – hence the name. Scramble! is a Firefox plugin and can thus be used in all web 2.0 environments that contain interactive fields, that is, if these are accessed using the Firefox browser.

This brings us to the end of this deliverable. In this deliverable we have documented two years of technical and social-scientific research into issues on privacy and identity management in social network sites and collaborative workspaces. We will continue this research in the next year and expand on the work completed so far. Next versions of all three of the demonstrators are under way, implementing more of the solutions proposed in this deliverable.

Bibi van den Berg and Ronald Leenes (TILT)

March 2010.

References

Acquisti, Alessandro, and Ralph Gross (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. In *Proceedings of the 6th Workshop on Privacy Enhancing Technologies*. Cambridge, UK.

Adams, Anne (1999). The implications of users' privacy perception on communication and information privacy policies. In *Proceedings of Telecommunications Policy Research Conference*. Washington, DC.

Agre, Philip, and Marc Rotenberg (1997). *Technology and privacy: The new landscape*. Cambridge, Mass.: MIT Press.

Aguiton, Christophe, and Dominique Cardon (2007). The strength of weak cooperation: An attempt to understand the meaning of web 2.0. *Communications & Strategies* Vol. 65: 51-65.

Aleo-Carreira, Cyndy (2009). Police turn to social networks - and fake profiles - in criminal investigations. *The Industry Standard*, 1 December 2009. Available from http://www.thestandard.com/news/2009/01/12/social-networking-becoming-bigger-factor-discovering-evidence-0 [last accessed on 09 February 2010].

Aljifri, Hassan, and Diego Sánchez Navarro (2003). International legal aspects of cryptography: Understanding cryptography. *Computers & Security* Vol. 22 (3): 196-203.

Austin, Lisa M. (2010). Control yourself, or at least your core self. *Bulletin of Science, Technology and Society* Vol. 30 (1): 26-30.

Baechle, Michael (2006). Social software. *Informatik Spektrum* Vol. 29 (2): 121-124.

Barnes, Susan B. (2006). A privacy paradox: social networking in the US. *First Monday* Vol. 11 (9).

Bauman, Zygmunt (2001). Identity in the globalizing world. In *The individualized society*. Cambridge (UK); Malden (MA): Polity Press: 140-153.

Bauman, Zygmunt, and Benedetto Vecchi (2004). *Identity: Conversations with Benedetto Vecchi, Themes for the 21st century*. Cambridge (UK); Malden (MA): Polity Press.

BBC_News (2009). Social network sites 'monitored'. *BBC News*, 25 March 2009. Available from http://news.bbc.co.uk/2/hi/7962631.stm [last accessed on 09 February 2010].

Beato, Filipe, Markulf Kohlweiss, and Karel Wouters (2009). Enforcing access control in social network sites. In *HotPets*.

Benkler, Yochai (2006). *The wealth of networks: How social production transforms markets and freedom*. New Haven [Conn.]: Yale University Press.

Bennett, Colin J., and Charles D. Raab (2006). *The governance of privacy: Policy instruments in global perspective*. [2nd and updated ed. Cambridge, Mass.: MIT Press.

Bernstein, A., and R. Ramchandani (2002). Don't Shoot the Messenger! A Discussion of ISP Liability. *Canadian Journal of Law and Technology* Vol. 1 (2): 77-85.

Blume, Peter (2002). *Protection of informational privacy*. 1st ed. Copenhagen: DJØF Pub.

boyd, danah (2008a). None of this is real: Identity and participation in Friendster. In *Structures of participation in digital culture*, edited by J. Karaganis. New York: Social Science Research Council: 132-157.

——— (2008b). *Taken out of context: American teen sociality in networked publics*. PhD Thesis, University of California, Berkeley, California, USA.

——— (2008c). Why youth (heart) social network sites: The role of networked publics in teenage social life. In *MacArthur Foundation Series on Digital Learning: Youth, identity and digital media*, edited by D. Buckingham. Cambridge (MA): MIT Press.

boyd, danah, and Nicole B. Ellison (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication* Vol. 13 (1): 210-230.

boyd, danah, and Jeffrey Heer (2006). Profiles as conversation: Networked identity performance on friendster. In *Proceedings of the Hawaii International Conference on System Sciences (HICSS-39)*: IEEE Computer Society.

Bryce, Jo, and Matthias Klang (2009). Young people, disclosure of personal information and online privacy: Control, choice and consequences. *Information Security Technical Report* Vol.: 1-7.

Castells, Manuel (2004). Informationalism, networks, and the network society: A theoretical blueprint. In *The network society: A cross-cultural perspective*, edited by M. Castells. Cheltenham (UK); Northampton (MA): Edward Elgar Publishers: 3-47.

Chambers, Deborah (2006). *New social ties: Contemporary connections in a fragmented society*. New York: Palgrave Macmillan.

Chandler, Daniel (1998). *Personal Home Pages and the Construction of Identities on the Web*. Available from http://www.aber.ac.uk/media/Documents/short/webident.html [last accessed on 2 June 2009].

Chew, Monica, Dirk Balfanz, and Ben Laurie (2008). (Under)mining privacy in social networks. In *W2SP 2008: Web 2.0 Security and Privacy 2008*. Oakland (CA), USA.

Crampton, Thomas (2007). *Eurovision, Wikipedia and Privacy*. Available from http://www.thomascrampton.com/uncategorized/eurovision-wikipedia-and-privacy [last accessed on 4 February 2010].

Cuijpers, Colette (2004). *Privacyrecht of privaatrecht: Een privaatrechtelijk alternatief voor de implementatie van de Europese privacyrichtlijn*: Wolf Legal Publishers.

Davies, Mark R., and Barbara A. Lee (2008). The legal implications of student use of social networking sites in the UK and US: current concerns and lessons for the future. *Education and the Law* Vol. 20 (3): 259-288.

Delanty, Gerard (2003). *Community*, *Key ideas*. New York (NY): Routledge.

DiNucci, Darcy (1999). Fragmented future. *Print Magazine* Vol. 4.

Donath, J., and dana boyd (2004). Public displays of connection. *BT Technology Journal* Vol. 22 (4): 71-83.

Döring, Nicola (2008). Reduced social cues / Cues filtered out approach. In *Schlüsselbegriffe der Medienpsychologie*, edited by N. Krämer, S. Schwan, D. Unz and M. Suckfüll. Stuttgart: Kohlhammer: 290-297.

Edwards, Lilian, and Ian Brown (2009). Data Control and Social Networking: Irreconcilable Ideas? In *Matwyshyn, A.*, edited by l. a. t. c. Harboring Data: Information security: Stanford University Press.

Ellis, C. A., S. J. Gibbs, and G. Rein (1991). Groupware: Some issues and experiences. *Communications of the ACM* Vol. 34 (1): 39-58.

ETSI (2007). Retained data: Handover interface for the request and delivery of retained data. Groningen (The Netherlands): European Telecommunications Standards Institute (ETSI).

Fenner, A. (2007). N.J. Miss in a fix over her pics. *The New York Post*, 5 July 2007. Available from http://www.nypost.com/seven/07062007/news/regionalnews/n_j__miss_in_a_fix_over_her_pics_regionalnews_austin_fenner__with_post_wire_services.htm [last accessed on 18 February 2010].

Finder, A. (2006). When a risqué online persona undermines a chance for a job. *The New York Times*, 11 June 2006. Available from http://query.nytimes.com/gst/fullpage.html?res=9C0DE3D61231F932A25755C0A9609C8B63 [last accessed on 18 February 2010].

Franz, Elke, Hagen Wahrig, Alexander Böttcher, and Katrin Borcea-Pfitzmann (2006). Access control in a privacy-aware e-learning environment. In *First International Conference on Availability, Reliability and Security*.

Gergen, Kenneth J. (1991). *The saturated self: Dilemmas of identity in contemporary life*. New York (NY): Basic Books.

Gijzemijter, Martin (2008). *Google API maakt sociale connecties draagbaar*. http://webwereld.nl, Available from http://webwereld.nl/nieuws/49740/google-api-maakt-sociale-connecties-draagbaar.html [last accessed on 12 February 2010].

Giles, G. (2005). Internet encyclopaedias go head to head. *Nature* Vol. 438: 900-901.

Goffman, Erving (1959). *The presentation of self in everyday life*. Garden City (NY): Doubleday.

——— (1963). *Behavior in public places: Notes on the social organization of gatherings*. New York (NY): Free Press of Glencoe.

——— (1968). Information control and personal identity. In *Stigma: Notes on the management of spoiled identity*. Harmondsworth: Penguin: 57-129.

——— (1986). *Frame analysis: An essay on the organization of experience*. Boston (MA): Northeastern University Press.

Grimmelmann, James (2008). *Facebook and the social dynamics of privacy [draft version]*. Available from http://works.bepress.com/james_grimmelmann/20/ [last accessed on 6 July 2009].

——— (2009). Saving Facebook. *Iowa Law Review* Vol. 94: 1137-1205.

Gross, Ralph, and Alessandro Acquisti (2005). Information revelation and privacy in online social networks. In *WPES'05*. Alexandria, Virginia (USA): ACM.

Grossman, Lev (2006). Time's person of the year: You. *Time Magazine* Vol.

Guernsey, Lisa (2008). Picture Your Name Here. *The New York Times*, 27 July 2008. Available from http://www.nytimes.com/2008/07/27/education/edlife/27facebook-innovation.html [last accessed on 18 February 2010].

Heng, Stefan, Thomas Meyer, and Antje Stobbe (2007). Be a driver, not a passenger: Implications of web 2.0 for financial institutions. *Deutsche Bank Research: E-conomics* Vol. 63: 1-11.

Hildebrandt, Mireille (2009). Technology and the end of law. In *Facing the limits of the law*, edited by E. Claes, W. Devroe and B. Keirsbilck. Berlin, Heidelberg: Springer.

Hogben, Giles (Ed.) (2007). *Security Issues and Recommendations for Online Social Networks*. Available from http://www.enisa.europa.eu/act/res/other-areas/social-networks/security-issues-and-recommendations-for-online-social-networks [last accessed on 15 February 2010].

Hough, Michelle G. (2009). Keeping it to ourselves: Technology, privacy, and the loss of reserve. *Technology in Society* Vol. 31 (4): 406-413.

Howe, Jeff (2008). *Crowdsourcing: Why the power of the crowd is driving the future of business*. 1st ed. New York: Crown Business.

International_Working_Group_on_Data_Protection_in_Telecommunications (2008). Report and Guidance on Privacy in Social Network Services. In *Rome Memorandum*. Rome.

Johnson, Bobbie (2007). Online investigations into job candidates could be illegal. *The Guardian*, 27 November 2007. Available from http://www.guardian.co.uk/technology/2007/nov/27/news.socialnetworking [last accessed on 9 February 2010].

Joinson, Adam N. (2008). *'Looking at', 'looking up' or 'keeping up' with people? Motives and uses of Facebook*. Paper presented at CHI 2008, 5-10 April, at Florence, Italy.

Kolbitsch, Josef (2006). *A unified structure for current collaborative systems*. Available from http://www.kolbitsch.org/research/papers/2006-Unified_Structure_for_Current_Collaborative_Systems.pdf [last accessed on 4 August 2008].

Koops, Bert-Jaap (1999). *The crypto controversy: A key conflict in the Information Society*, *Law and electronic commerce v. 6*. Boston: Kluwer Law International.

Kuner, Christopher (2007). *European Data Protection Law: corporate compliance and regulations*. 2 ed. Oxford: Oxford University Press.

Lampson, B. (1971). Protection. In *5th Princeton Symposium on Information Science and Systems*.

Lastowka, Greg (2008). User-generated content and virtual worlds. *Vanderbilt Journal of Entertainment and Technology Law* Vol. 10 (4): 893-917.

Leadbeater, Charles (2008). *We-think*. London: Profile.

Leenes, Ronald (2010). Context is everything: Sociality and privacy in online social network sites. In *Privacy and Identity Management for Life: Proceedings of Fifth International PrimeLife/IFIP Summer School*, edited by S. Fischer-Hübner and P. Duquenoy: Springer.

Leino, Juha, and Kari-Jouko Räihä (2007). *Case Amazon: Ratings and reviews as part of recommendations*. Paper presented at RecSys'07, 19–20 October, at Minneapolis, Minnesota, USA.

Lenhart, Amanda (2007). Social networking sites and teens: An overview. PEW Internet & American Life Project.

——— (2009). The democratization of online social networks. PEW Internet & American Life Project.

Lodder, A.R., and H.W.K. Kaspersen, eds. (2002). *eDirectives: Guide to European Union law on E-Commerce*: Kluwer Law International.

Lucas, Matthew M. , and Nikita Borisov (2008). FlyByNight: Mitigating the privacy risks of social networking. In *Proceedings of the 7th ACM workshop on Privacy in the Electronic Society (WPES)*. New York (NY): ACM.

Mabillot, David (2007). User generated content: Web 2.0 taking the video sector by storm. *Communications & Strategies* Vol. 65: 39-49.

Maines, David R. (2003). Interactionism's place. *Symbolic Interaction* Vol. 26 (1): 5-18.

Mayer-Schönberger, Viktor (2009). *Delete: The virtue of forgetting in the digital age*. Princeton, N.J.: Princeton University Press.

McDonagh, Patricia (2008). Taxman admits to Facebook 'trawl'. *Independent [Ireland]*, 25 February 2008. Available from http://www.independent.ie/national-news/taxman-admits-to-facebook-trawl-1297118.html [last accessed on 9 February 2010].

Mergel, Ines, Charlie Schweik, and Jane Fountain (2009). *The transformational effect of web 2.0 technologies on government*. Available from Available at SSRN: http://ssrn.com/abstract=1412796 [last accessed on 14 January 2010].

Meyrowitz, Joshua (1985). *No sense of place: The impact of electronic media on social behavior*. New York (NY): Oxford University Press.

——— (1990). Redefining the situation: Extending dramaturgy into a theory of social change and media effects. In *Beyond Goffman: Studies on communication, institution, and social interaction*, edited by S. H. Riggins. Berlin; New York (NY): Mouton De Gruyter: 65-99.

——— (2003). Global nomads in the digital veldt. In *Mobile democracy: Essays on society, self and politics*, edited by K. Nyíri. Vienna (Austria): Passagen Verlag: 91-102.

——— (2005). The rise of glocality: New senses of place and identity in the global village. In *The global and the local in mobile communication*, edited by K. Nyíri. Vienna (Austria): Passagen Verlag: 21-30.

Morley, David, and Kevin Robins (1995). *Spaces of identity: Global media, electronic landscapes, and cultural boundaries*. London; New York (NY): Routledge.

Nederlands_Dagblad (2008). Politie speurt of Hyves naar criminelen. *Nederlands Dagblad*, 20 May 2008. Available from http://www.nd.nl/artikelen/2008/mei/20/politie-speurt-op-hyves-naar-criminelen [last accessed on 9 February 2010].

Nissenbaum, Helen (1998). Protecting privacy in an information age: The problem of privacy in public. *Law and Philosophy* Vol. 17 (5-6): 559-596.

——— (2004). Privacy as contextual integrity. *Washington Law Review* Vol. 79 (119): 119-159.

——— (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford, Calif.: Stanford Law Books.

Norberg, Patricia A., Daniel R. Horne, and David A. Horne (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *The Journal of Consumer Affairs* Vol. 41 (1): 100-126.

O'Hara, Kieron, and Nigel Shadbolt (2008). *The spy in the coffee machine*. Oxford: Oneworld Publications.

O'Reilly, Tim (2007). What is web 2.0: Design patterns and business models for the next generation of software. *Communications & Strategies* Vol. 65 (1): 17-37.

Oomen, Isabelle, and Ronald Leenes (2008). Privacy risk perceptions and privacy protection strategies. In *Proceedings of IDMAN'07 – IFIP WG 11.6 working conference on Policies & Research in Identity Management*, edited by S. Fischer-Hübner. Dordrecht: Springer.

Osborne, D. (2008). User generated content (UGC): Trade mark and copyright infringement issues. *Journal of Intellectual Property Law & Practice* Vol. 3 (9): 555-562.

Paine, Carina, Ulf-Dietrich Reips, Stefan Stieger, Adam N. Joinson, and Tom Buchanan (2007). Internet users' perceptions of 'privacy concerns' and 'privacy actions'. *International Journal of Human-Computer Studies* Vol. 65 (6): 526-536.

Palen, Leysia, and Paul Dourish (2003). Unpacking 'privacy' for a networked world. In *Computer-Human Interaction (CHI) Conference 2003*. Ft. Lauderdale (FA).

Pankoke-Babatz, U., and A. Syri (1997). Collaborative workspace for time deferred electronic cooperation. In *Proceedings of the International ACM SIGGROUP Conference on Supporting Group Work: The integration Challenge*. Phoenix, Arizona, United States: ACM.

Perez, E. (2007). Officers increasingly using online social networks for intel. *The Milwaukee Journal Sentinel*, 3 October 2007. Available from http://www.policeone.com/investigations/articles/1360141/ [last accessed on 18 February 2010].

Pfitzmann, Andreas, and Marit Koehntopp (2001). Anonymity, unobservability, and pseudonymity: A proposal for terminology. In *Proceedings Workshop on Design Issues in Anonymity and Unobservability, LNCS 2009*, edited by H. Federrath: Springer Verlag.

Pimenidis, L., and E. Kosta (2008). The impact of the retention of traffic and location data on the internet user: A critical discussion. *Datenschutz und Datensicherheit* Vol. 2: 92-97.

Pötzsch, Stefanie (2009). Untersuchung des Einusses von wahrgenommener Privatsphäre und Anonymität auf die Kommunikation in einer Online-Community. In *Informatik 2009, Im Fokus das Leben: Volume 154 of Lecture Notes in Informatics*, edited by S. Fischer, E. Maehle and R. Reischuk. Bonn: Gesellschaft für Informatik: 2152–2165.

Pötzsch, Stefanie, and Katrin Borcea-Pfitzmann (2010). Privacy-respecting access control in collaborative workspaces. In *Privacy and Identity Management for Life: Proceedings of Fifth International PrimeLife/IFIP Summer School*, edited by S. Fischer-Hübner and P. Duquenoy: Springer.

Rachels, James (1975). Why privacy is important. *Philosophy and Public Affairs* Vol. 4 (4): 323-333.

Raynes-Goldie, Kate (2010). Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook. *First Monday* Vol. 15 (1).

Razavi, M.N., and L. Iversion (2007). Towards usable privacy for social software.

——— (2008). Supporting selective information sharing with people-tagging. In *Proceedings of the ACM CHI '08 Extended Abstracts on Human Factors in Computing Systems*.

Richter, Alexander, and Michael Koch (2007). Social software: Status quo und Zukunft. *Technischer Bericht* Vol. 2007-01: 1-49.

Sandhu, Ravi, E.J. Coyne, H.L. Feinstein, and C.E. Youman (1996). Role-based access control models. *IEEE Computer* Vol. 29 (2): 38-47.

Schlichter, J., M. Koch, and C. Xu (1998). Awareness: The common link between groupware and community support systems In *Community Computing and Support Systems: Social*

Interaction in networked Communities, edited by T. Ishda. Berlin, Heidelberg, New York: Springer-Verlag: 77-93.

Schmidt, Jan (2006). Social software: Onlinegestütztes Informations-, Identitäts- und Beziehungsmanagement. *Forschungsjournal Neue Soziale Bewegungen* Vol. (2): 37-47.

Shepherd, Jessica, and David Shariatmadari (2008). Would-be students checked on Facebook. *The Guardian*, 11 January 2008. Available from http://www.guardian.co.uk/uk/2008/jan/11/accesstouniversity.highereducation [last accessed on 18 February 2010].

Shirky, Clay (2008). *Here comes everybody: The power of organizing without organizations*. New York: Penguin Press.

Smart, E.J., J. Cascio, and J. Paffendorf (2007). *Metaverse Roadmap Overview*. Available from http://metaverseroadmap.org/MetaverseRoadmapOverview.pdf [last accessed on 22 January 2010].

Solove, Daniel J. (2004). *The digital person: Technology and privacy in the information age*. New York: New York University Press.

——— (2007a). "I've got nothing to hide" and other misunderstandings of privacy. *San Diego Law Review, Available at SSRN: http://ssrn.com/abstract=998565* Vol. 44: 745-772.

——— (2007b). *The future of reputation: Gossip, rumor, and privacy on the Internet*. New Haven: Yale University Press.

——— (2008). *Understanding privacy*. Cambridge, Mass.: Harvard University Press.

Sundén, Jenny (2003). *Material virtualities: Approaching online textual embodiment*, *Digital formations v. 13*. New York: P. Lang.

Surowiecki, James (2004). *The wisdom of crowds: why the many are smarter than the few and how collective wisdom shapes business, economies, societies and nations*. 1st ed. New York: Doubleday :.

Tapscott, Don (2009). *Grown up digital: How the Net generation is changing your world*. New York: McGraw-Hill.

Taylor, G. (1999). Wassenaar: The cryptic enigma. *Internet Law Bulletin (Online)* Vol. 2 (1).

Terwangne, C., and S. Louveaux (1997). Data protection and online networks. *CLSR* Vol. 13 (4).

Thomas, Roshan K. (1997). Team-based access control (TMAC): A primitive for applying role-based access controls in collaborative environments. In *RBAC '97: Proceedings of the second ACM workshop on Role-based access control*. New York (NY): ACM: 13-19.

Toffler, Alvin (1980). *The third wave*. 1st ed. New York: Morrow.

Tolone, William, Gail-Joon Ahn, Tanusree Pai, and Seng-Phil Hong (2005). Access control in collaborative systems. *ACM Comput. Surv.* Vol. 37 (1): 29-41.

Tufekci, Zeynep (2008). Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology and Society* Vol. 28 (1): 20-36.

Turkle, Sherry (1984). *The second self: Computers and the human spirit*. New York (NY): Simon and Schuster.

——— (1995). *Life on the screen: Identity in the age of the Internet*. New York (NY): Simon & Schuster.

——— (1996). Parallel lives: Working on identity in virtual space. In *Constructing the self in a mediated world: Inquiries in social construction*, edited by D. Grodin and T. R. Lindlof. Thousand Oaks (CA): Sage Publications: 156-176.

——— (2007). *Evocative objects: Things we think with*. Cambridge (MA): MIT Press.

Van Alsenoy, Brendan, Joris Ballet, Aleksandra Kuczerawy, and Jos Dumortier (2009). Social networks and web 2.0: are users also bound by data protection regulations? *Identity in the Information Society* Vol.

Van den Berg, Bibi (2008a). Self, script, and situation: Identity in a world of ICTs. In *The future of identity in the information society: Proceedings of the third IFIP WG 9.2, 9.6/11.6, 11.7/FIDIS International Summer School on the Future of Identity in the Information Society*, edited by S. Fischer-Hübner, P. Duquenoy, A. Zuccato and L. Martucci. New York (NY): Springer: 63-77.

——— (2008b). *The generalized everything: Constructing identities in a world of Ambient Intelligence*. Paper presented at Ethics, Technology and Identity Conference, 18-20 June, at Delft (The Netherlands).

——— (2009). *The situated self: Identity in a world of Ambient Intelligence*. Rotterdam (The Netherlands).

Vedder, Anton (2009). Privacy, een conceptuele articulatie. *Filosofie & Praktijk* Vol. 30 (5): 7-19.

Velleman, J. David *Artificial agency* 2007 [last accessed.

Walzer, Michael (1983). *Spheres of justice: A defense of pluralism and equality*. New York (NY): Basic Books.

Warren, Samuel, and Louis Brandeis (1890). The right to privacy. *Harvard Law Review* Vol. 4 (5).

Weinberger, David (2007). *Everything is miscellaneous: The power of the new digital disorder*. 1st ed. New York: Times Books.

Westin, Alan F. (1967). *Privacy and freedom*. [1st ed. New York: Atheneum.

Wilkinson, Dennis, and Bernardo Huberman (2007). *Cooperation and quality in Wikipedia*. Paper presented at WikiSym'07, 21–23 October, at Montréal, Québec, Canada.

Wolf, Gritta, and Andreas Pfitzmann (2000). Properties of protection goals and their integration into a user interface. *Computer Networks* Vol. 32: 685-699.

Wong, Rebecca, and Joseph Savirimuthu (2008). 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 (2).

Young, Alyson L., and Anabel Quan-Haase (2009). Information revelation and internet privacy concerns on social network sites: A case study of Facebook. In *C&T '09*. University Park, Pennsylvania (USA): ACM.