Université de Montréal

Towards a Privacy-enhanced Social Networking Site

par
Ai Thanh Ho

Département d'informatique et de recherche opérationnelle
Faculté des arts et des sciences

Thèse présentée à la Faculté des arts et des sciences
en vue de l'obtention du grade de Philosophiæ Doctor (Ph.D.)
en informatique

Avril, 2012

Université de Montréal
Faculté des arts et des sciences

Cette thèse intitulée:

Towards a Privacy-enhanced Social Networking Site

présentée par:

Ai Thanh Ho

a été évaluée par un jury composé des personnes suivantes:

Guy Lapalme,	président-rapporteur
Esma Aïmeur,	directrice de recherche
Sébastien Gambs,	codirecteur
Louis Salvail,	membre du jury
Julita Vassileva,	examinateur externe
André-A Lafrance,	représentant du doyen de la FAS

Thèse acceptée le: . . . .

RÉSUMÉ

L’avénement des réseaux sociaux, tel que Facebook, MySpace et LinkedIn, a fourni une plateforme permettant aux individus de rester facilement connectés avec leurs amis, leurs familles ou encore leurs collègues tout en les encourageant activement à partager leurs données personnelles à travers le réseau. Avec la richesse des activités disponibles sur un réseau social, la quantité et la variété des informations personnelles partagées sont considérables. De plus, de part leur nature numérique, ces informations peuvent être facilement copiées, modifiées ou divulguées sans le consentement explicite de leur propriétaire. Ainsi, l’information personnelle révélée par les réseaux sociaux peut affecter de manière concrète la vie de leurs utilisateurs avec des risques pour leur vie privée allant d’un simple embarras à la ruine complète de leur réputation, en passant par l’usurpation d’identité. Malheureusement, la plupart des utilisateurs ne sont pas conscients de ces risques et les outils mis en place par les réseaux sociaux actuels ne sont pas suffisants pour protéger efficacement la vie privée de leurs utilisateurs. En outre, même si un utilisateur peut contrôler l’accès à son propre profil, il ne peut pas contrôler ce que les autres révèlent à son sujet. En effet, les “amis” d’un utilisateur sur un réseau social peuvent parfois révéler plus d’information à son propos que celui-ci ne le souhaiterait.

Le respect de la vie privée est un droit fondamental pour chaque individu. Nous présentons dans cette thèse une approche qui vise à *accroître la prise de conscience des utilisateur*s des risques par rapport à leur vie privée et à *maintenir la souveraineté* sur leurs données lorsqu’ils utilisent un réseau social. La première contribution de cette thèse réside dans *la classification des risques multiples ainsi que les atteintes à la vie privée* des utilisateurs d’un réseau social. Nous introduisons ensuite un *cadre formel pour le respect de la vie privée* dans les réseaux sociaux ainsi que *le concept de politique de vie privée* (UPP). Celle-ci définie par l’utilisateur offre une manière simple et flexible de spécifier et communiquer leur attentes en terme de respect de la vie privée à d’autres utilisateurs, tiers parties ainsi qu’au fournisseur du réseau social. Par ailleurs, nous définissons une taxonomie (possiblement non-exhaustive) des *critères qu’un réseau social peut intégrer dans sa conception pour améliorer le respect de la vie privée*. En introduisant le concept de *réseau social respectueux de la vie privée* (PSNS), nous proposons *Privacy Watch*, un réseau social respectueux de la vie privée qui combine les concepts de *provenance* et *d'imputabilité* afin d'aider les utilisateurs à maintenir la souveraineté sur leurs données personnelles. Finalement, nous *décrivons* et *comparons* les différentes propositions de réseaux sociaux respectueux de la vie privée qui ont émergé récemment. Nous *classifions* aussi ces différentes approches au regard des critères de respect de la vie privée introduits dans cette thèse.

Mots clés: Vie privée, réseaux sociaux, imputabilité, filigrane, cryptage, contrôle d'accès.

ABSTRACT

The rise of Social Networking Sites (SNS), such as Facebook, Myspace, and LinkedIn has provided a platform for individuals to easily stay in touch with friends, family and colleagues and actively encourage their users to share personal information. With the wealth of activities available on SNS, the amount and variety of personal information shared is considerable and diverse. Additionally, due to its digital nature, this information can be easily copied, modified and disclosed without the explicit consent of their owner. Personal information disclosed from SNS could affect users' life, with privacy risks ranging from simple embarrassment to ruining their reputation, or even identity theft. Unfortunately, many users are not fully aware of the danger of divulging their personal information and the current privacy solutions are not flexible and thorough enough to protect user data. Furthermore, even though users of SNS can control access to their own profile, they cannot control what others may reveal about them. Friends can sometimes be untrustworthy and disclose more information about the user than they should.

Considering that privacy is a fundamental right for every individual, in this thesis, we present an approach that increases *privacy awareness* of the users and *maintains the sovereignty* of their data when using SNS. The first contribution of this thesis is the *classification of multiple types of risks* as well as *user expectations* regarding privacy in SNS. Afterwards, we introduce the *Privacy Framework for SNS* and the concept of *User Privacy Policy* (UPP) to offer users an easy and flexible way to specify and communicate their privacy concerns to other users, third parties and SNS provider. Additionally, we define a taxonomy (possibly non-exhaustive) of *privacy criteria* that can enhance the user privacy if they are integrated within the design of a SNS and introduce the concept of a *Privacy-enhanced SNS* (PSNS). Furthermore, we present also *Privacy Watch*, a theoretical proposal of a PSNS platform that combines the concept of provenance and accountability to help SNS users maintain sovereignty over their personal data. Finally, we *survey and compare* several privacy-enhanced SNS that were recently proposed that try to integrate some privacy features directly into the design of the system. We also *classify* these different approaches with respect to the privacy criteria developed.

Keywords: Privacy, social networking sites, accountability, watermarking, encryption, access control.

CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

CPM	Client Privacy Manager
PSNS	Privacy-enabled Social Networking Site
SNS	Social Networking Site
UPP	User Privacy Policy

(dedicace) To my parents and my husband.

ACKNOWLEDGMENTS

First of all I would like to express my heartfelt gratitude to my two advisors, Prof. Esma Aïmeur and Prof. Sébastien Gambs, whose expertise, understanding, and patience, added considerably to my graduate experience. I appreciate their vast knowledge and skill in many areas, and their assistance in writing papers and this thesis. They provided me with direction, technical support as well as moral support and became more of mentors and friends, than professors. I would like to thank the other members of my jury, Prof. Guy Lapalme, Prof. Louis Salvail, Prof. André A. Lafrance for the encouraging and constructive comments. Finally, I would like to thank Prof. Julita Vassileva from University of Saskatewan for taking time out from her busy schedule to serve as my external examiner.

One of the joys of completion is to look over the journey past and be thankful for all the friends and family who have helped and supported me along this long but fulfilling road.

I am in debt to Hicham Hage for proof reading my thesis as well as his generous help and moral support during my Ph.D. journey. I would like to thank the many graduate and undergraduate students I have worked with in Héron laboratory, especially David Schönfeld and Odilon Allognon for helping me implement Privacy Watch. I also thank my fellow PhD students: François Courtemanche, Maiga Abdou, Fod Touré for their invaluable insights and comments on my presentations and my thesis.

I would also like to thank my parents for the support they provided me through my entire life and in particular, I must acknowledge my father, without his love, encouragement and support, I would not have finished this thesis.

And last, but not least, to Minh, my husband, thank you for helping me achieve my dreams.

CHAPTER 1

INTRODUCTION

Recent advances in Information Technologies have brought important changes to the nature of communication and socialization. Indeed, throughout the last few years, blogs, forums, instant messaging, podcasts, online photo albums have bloomed all over the Internet. Nowadays, all these media are gathered together in Social Networking Sites (SNS). Starting at simple websites that allowed users to connect and interact with content posted by other users, SNS have developed rapidly by integrating new features as technology evolves. With many different activities available to the users, the amount and variety of data gathered by the SNS is especially great and diverse. On average, in one year, a user will *share* 415 pieces of content on Facebook, spend an average of about 23 minutes a day on Twitter, *tweeting* a total of around 15,795 tweets, *check in* 563 times on Foursquare and *upload* 196 hours of video on YouTube [77].

The rapid growth of SNS in recent years indicates that they are now a mainstream communication technology for many people. The people who use SNS see them as a fun and easy leisure activity. However, the reputation of these SNS has been tarnished by a number of incidents in news media, such as the massive worldwide spam campaign in Quechup [65]. For instance, the incident of the mobile application *Girls Around Me* highlight how much information an SNS knows about us. The application collected data from *Foursquare* [1], a location-based SNS for mobile devices, and used it to show local bars where women had checked in before matching this information with their Facebook profile. While the application only uses data that is publicly available on Foursquare and Facebook, a blogger reported that he was able to use Girls Around Me to find one person he found attractive, and was then able to discover her personal information such as full name, age, birthday, current location (based on a recent Foursquare check-in), marital status, school, political views, her favourite drink (based on Facebook photos), recent travels as well as her relatives' full names [79].

[1] `http://foursquare.com`

Although SNS provide some mechanisms (privacy settings, block users...) to protect users against these risks, it seems that there is still much to be desired. Consider for instance the following scenario. On Saturday evening, Alice went to a party at Carol's place and got dizzy through the abuse of grape juice. She had some pictures taken and then posted them on her Facebook account. Unfortunately, as her profile is opened to the public by default, everybody can have access to these pictures. Bob, another guest of Carol's party, took one of her party pictures, and modified it by attaching some "inappropriate" comments directly on the picture. After that, he reposted the "new" picture on his own Facebook account without bothering to tag or tell this to Alice (who he might only have met for the first time at this party). Afterwards, this picture is reshared and exchanged many times between friends. As a result, the existence of this photo may damage Alice's reputation and credibility.

This scenario illustrates the following privacy challenges:

1. How can Alice find out about the existence of the "new" picture as well as the inappropriate comments attached to it?
2. How can Alice discover who is the owner of the "new" picture in order to exert her right to be forgotten and to ask Bob to remove it?
3. How can she remove all the traces of this unflattering picture and the inappropriate comments before her boss gets to see them?
4. And finally, how can Alice safely share her personal pictures with friends without fear that they would use these pictures for other purposes?

Let us consider the case in which Bob is just an ignorant user who shared the picture as a joke. If contacted by Alice, Bob can easily remove the picture as well as his comments without needing much persuasion. However, if another malicious Facebook user has already copied this picture, removed all ownership metadata and claimed he is the "real" owner, then on most of the existing SNS, Alice has no way to force him to remove this picture if he does not want to.

Alice in the above scenario may not be representative of the whole population of SNS users but through her privacy challenges, we can detect multiple privacy problems within the current SNS. The top and foremost privacy problem is that *SNS users are not fully aware of the danger of divulging their personal information.* Although privacy and safety issues are the subject of much discussion in the media, these issues still did not emerge as 'top of mind' for most SNS users. They are seemingly unwilling to consider that there could be a more serious side to their activities on SNS. Even if they want to protect their privacy, with too much data and too many friends, it is very difficult for users to control who can see what in their profile pages. The second problem is that *privacy tools in SNS are not flexible enough to protect user data.* Most SNS only allow user to make public (available for everyone) or private (available only for Friends) the whole profile but not every part of it. The third problem is that when users of SNS can control access to their own profile, *they cannot control what others reveal about them.* There is also the possibility of information being passed on without one's consent. For instance, a user can upload an embarrassing photo of a friend; he could even tag the photo directly to his friend's profile.

Considering that privacy is a fundamental right for every individual, in this thesis, we present an approach that increases *privacy awareness* of the users and *maintains the sovereignty* of their data when using SNS. As a result, the users should be better equipped to defend against the underlaying risks of SNS, and that is the main objective of our project.

The first contribution of this thesis is the *classification of multiple types of risks* as well as *user expectations* regarding privacy in SNS. Specifically, we analyze and group privacy risks into three categories: *Security risks* (*e.g.*, identity theft, phishing, cyber predator...), *Reputation and Credibility risks* (*e.g.*, employees being fired due to social media slip-ups [70]) and *Profiling risks* (*e.g.*, spam, profiling...) (see Section 3.1). We also elicit *privacy requirements* of SNS users based on the finding of various surveys (Section 3.2) and our own preliminary study (Section 4.1).

Afterwards, we introduce the *Privacy Framework for SNS* and the concept of *User Privacy Policy* (UPP) to offer users an easy and flexible way to specify and communicate their privacy concerns to other users, third parties and SNS provider. In this Privacy Framework, the user data is divided into categories based on its privacy risk and its importance to the users. We also adapt the four privacy levels first proposed in our previous work to the context of SNS [2] . The *User Privacy Policy* is designed based on this framework and offers users an easy and flexible way to specify and then communicate their privacy concerns to other users, third parties and SNS service provider.

Additionally, we define a taxonomy (possibly non-exhaustive) of privacy criteria that can enhance the user privacy if they are integrated within the design of a SNS and introduce the concept of a Privacy-enhanced SNS (PSNS) (Section 4.4).

Furthermore, we present also Privacy Watch, a theoretical proposal of a PSNS platform that combines the concept of provenance and accountability to help SNS users maintain sovereignty over their personal data (Chapter 5). Privacy Watch is based on the hybrid architecture in which a centralized server (the SNS server) is responsible for storing the personal information of the user (but possibly encrypted). Users of Privacy Watch install *Client Privacy Manager* (CPM) on their computer (for instance as a Firefox or Chrome extension) that has the responsibility of helping them to enforce their sovereignty on their personal information. Privacy Watch also relies on an auxiliary channel such as an independent mail server to store and exchange privacy policies and encryption keys among users. Moreover, Privacy Watch creates privacy awareness among SNS users with the *Privacy Advisor* module (Section 5.2.1). The Privacy Advisor guides users when they determine their privacy levels based on three factors: main objective for using SNS, user background, and user privacy concerns. Based on the selected privacy levels, the Policy Builder lets users create their own UPP in a simple and easy-to-understand manner. While the UPP allows users to express their privacy concerns, this policy still needs to be enforced. In order to enforce the UPP, we present the *Privacy Controller* (server-side and client-side) and the *Accountability Manager*. While Privacy Controller detects and prevents unauthorized access to user data, the Accountability Manager inserts ownership information into user data (especially pictures and videos) to protect users against unauthorized uses of their information.

Finally, we survey and compare several privacy-enhanced SNS that were recently proposed that try to integrate some privacy features directly into the design of the system (Chapter 6). We also classify these different approaches with respect to the privacy criteria developed in Section 4.4.

This document is organized as follows: we present an overview of SNS in chapter 2. In chapter 3 we examine different types of risks as well as user expectations regarding privacy in SNS. Then we describe our preliminary study to examine the usage and privacy concerns of SNS users and introduce a Privacy Framework tailored for SNS in chapter 4. Privacy Watch, our proposed implementation for a Privacy-enhanced SNS, is introduced in chapter 5. Finally, we present a comparison survey of solutions that have been proposed to enhance the privacy of users of SNS in chapter 6 and conclude the document in chapter 7.

CHAPTER 2

SOCIAL NETWORKING SITES

In this chapter, we introduce the concept of Social Networking Site (SNS). More precisely, in the first subsection we give a definition as well as a brief history of SNS while in the second subsection we review some well-known and popular SNS and highlight the main functionalities of a SNS.

2.1 Definition and History

In the past few years SNS have become some of the most popular websites worldwide. In order to better understand SNS, we must consult its definition as well as its history.

2.1.1 Definition

The term “social networking sites” originates from “social network”, which represents relationships and flows between people, groups, organizations, animals, computers or other information/knowledge processing entities [11]. At the most basic level, SNS consists of a representation of each user (often a profile). The profile page acts as the homepage of the user and may include personal information such as photos, date of birth, gender, religion, favourite music, books quotes, hobbies ... In addition, users can often customize the appearance of their profile page with widgets and applications. Furthermore, users are able to create a network of contacts with whom they can connect that are sometimes called “Friends”. Users can view and traverse their list of Friends and those made by others within the SNS [19]. These Friends may be real friends or offline acquaintances, but also persons that are barely known from users and even persons that they have only met online. Therefore, the term “Friend” as it used by a SNS such as Facebook (see Figure 2.1) is often misleading and differs from its traditional meaning in the offline world. In this thesis, we use the term “Friend” in its broader sense as anyone who has been invited by another user and accepted the invitation to become his "Friend" [19]. Moreover, SNS usually provide a mechanism for users to "communicate and share" with their Friends, such as the possibility to add comments on the profiles of their Friends, instant messaging capacities or integrated mail accounts. Additionally, SNS also integrate other networking features such as the possibility to share picture and videos or the use of groups and forums. Another definition states that a SNS is simply a website that provides a virtual community for people interested in a particular subject or just to "hang out" together [47]. Finally, Boyd and Ellison [19] provide a more formal definition of SNS saying that they are "web-based services that allow individuals to:

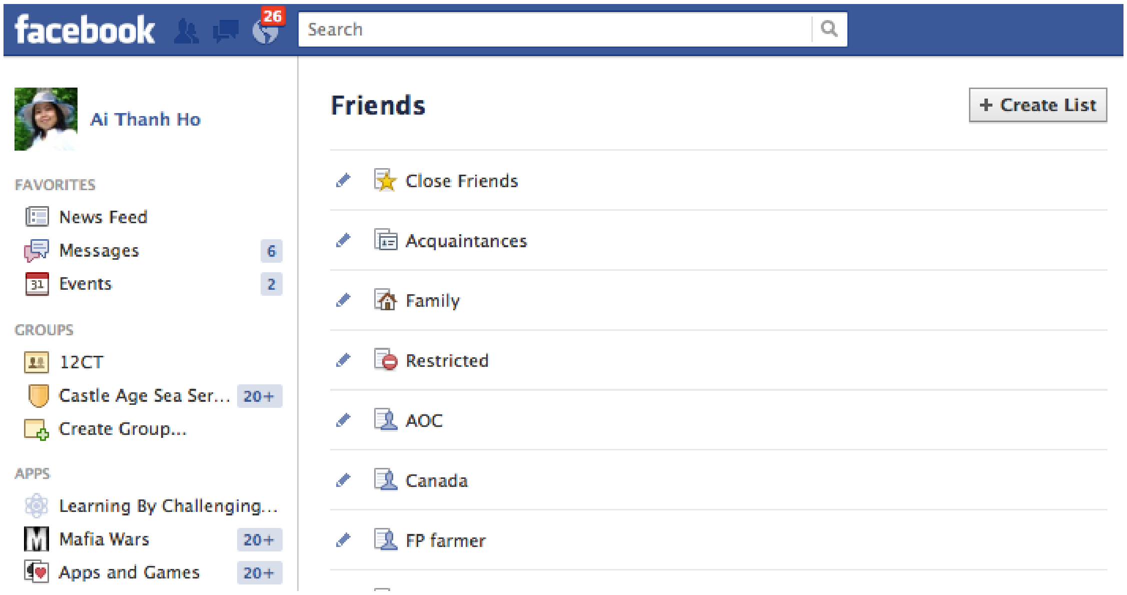


Figure 2.1: Friends in Facebook

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."

However, this definition falls short of describing newly emerging SNS such as Twitter[1] or resource-sharing websites with social networking components such as Youtube[2] and Picasa[3]. Moreover, it does not encompass the privacy and security concerns that appear in an online community. This motivates us to propose a broader definition of SNS.

Definition 2.1.1 (Social Networking Site)**.** A Social Netwoking Site (SNS) is a website that allow users to:

- *connect* with other users by befriending (Facebook), following (Twitter), subscribing (Youtube), ...
- *interact* with content posted by other users, for example by commenting, replying or rating,
- *restrict* their own content to authorized users only.

2.1.2 History

The connection and interaction features of a website are the main criteria that should be used to determine whether or not this website is a SNS. However, it is important to remember that these features predate the advent of SNS and already existed on the Internet for quite a long time. For instance, many dating and community websites included the use of profiles as early as the 1990s. Moreover, Instant Messaging services such as *AIM*[4] and *ICQ*[5] supported the concept of a list of Friends (one-way friends), although these lists were not made to be visible to others. According to Boyd and Ellison [19], *SixDegrees*[6] that was launched in 1997 was the first social networking site. It allowed users to create profiles, list their Friends and in 1998 it included the functionalities allowing users to traverse the Friends lists of their Friends. Six Degrees was followed by more popular social networking sites such as *BlackPlanet*[7] (1999), *Ryze*[8] (2000) and *Friendster*[9]

[1] http://twitter.com
[2] http://youtube.com
[3] http://picasa.com
[4] http://aim.com
[5] http://icq.com
[6] http://SixDegrees.com
[7] http://BlackPlanet.com
[8] http://Ryze.com
[9] http://Friendster.com

(2002). For instance, Friendster was originally launched in 2002 as an online dating site [29]. While most dating sites focused on introducing people to strangers with similar interests, Friendster was designed to help friends-of-friends meet, based on the assumption that friends-of-friends would make better romantic partners than strangers would [19]. From 2003 onwards, a plethora of SNS was launched, such as *MySpace* and *LinkedIn* in 2003, and *Facebook* in 2004. Nowadays, there are more than 300 SNS currently in existence [83].

2.1.3 Classification of Social Networking Sites

The existing SNS are very diverse in nature and promote different types of interactions and activities. For instance, Sharma [88] provides a comprehensive list of SNS and classify them into different categories such as Books, Business Networking and Professionals, Family, Friends, Hobbies and Interests, Media, Students and Social Bookmarking. Nations [73] summarizes SNS into three main categories: General Purpose, Niche Sites with a specific theme and International Sites. Huggins [56] also identifies three diffenrent types of SNS: Personal Contact Management, Business Networking Websites and Cultural Trends Networking Websites. Finally, Privacy Rights Clearinghouse [98] divides SNS into five main categories: Personal, Status update, Location, Content-sharing and Shared-interest networks. As our main concern deals with privacy issues inside SNS, we propose our own classification of SNS based on two criteria : (1) how they affect the privacy of their users and (2) the types of information exchanged among users.

2.1.3.1 Personal SNS

Personal SNS focus on giving the opportunity for users to connect with friends, acquaintances and the family. The users often put up a large amount of personal information on their profiles. Typical examples of personal SNS include *Facebook* [10], *QZone* [11]

[10] http://Facebook.com

[11] http://qzone.qq.com

and *Google+* [12].

- *Facebook*, founded by Mark Zuckerberg, was originally designed as a social networking site for Harvard students. After spreading from Harvard to other universities and down into high school, Facebook was opened to the public in 2006. On February 2012, Facebook had more than 845 million active users [13], of which 483 million are daily users [41] and has established as the leading SNS in 127 out of 136 countries as highlighted in a report of Vicos Blog [32].
- *QZone* is a Chinese SNS created by Tencent company in 2005. On November 2011, this SNS had more than 536 million users and was considered as the second largest SNS in the world [62]. The most popular applications on QZone are blogs, pictures sharing and connecting with new friends.
- *Google+* is a SNS operated by Google initially launched in June 2011 in a Beta format, and later publicly released in September 2011. Google+ directly integrates different Google social services, such as *Google Profiles* and *Google Buzz*, but also introduces novel features such as *Circles*, *Hangouts*, *Sparks* and *Huddles*.

2.1.3.2 Professional

The main purpose of *professional SNS* is to connect users with business contacts, both old and new, as well as to help them to find a job or look for employees. For example, *LinkedIn* [14], *Xing* [15] and *Doostang* [16] are websites that young professionals join mainly to accelerate their career. The information on these SNS often includes business contacts, expertise, recommendation and job offers. Most of the professional SNS are structured in such a way that they can be used to manage customer relationships [56].

- *LinkedIn* is a business-oriented SNS in which members invite other persons to be their “connections" (in contrast with the term “friends” used by Facebook). LinkedIn is at the same time a contact management system and a social network,

[12] `http://plus.google.com`

[13] “Active” users are defined as ones who access the site through the web or mobile, as well as those who do any Facebook action, such as Like a website or share tweets with Facebook

[14] `http://LinkedIn.com`

[15] `http://xing.com`

[16] `http://doostang.com`

and has a business related question-and-answer section where users can share and receive business advices.

- *Xing* is a SNS for business professionals that has more than 11.4 million members worldwide (as of September 2011)[17]. The members of XING can meet and exchange views with approximately 50,000 group specialists[18], while also meeting other members at networking events.

2.1.3.3 Hobbies and Interests

These SNS correspond mainly to places in which users share their hobbies and interests such as movies (*Flixster*[19]) and music (*Last.fm*[20]). As such, most information posted on these websites cannot be used to directly identify a user and are often considered to be less sensible with respect to his privacy.

- The motto of *Flixter* is to “stop watching bad movies". As such Flixter combines a SNS component with movie reviews and can be considered as the leading online destination for movie enthusiasts with more than 30 millions visitors per month and 2 billions movie ratings[21].
- *Last.fm* calls itself a social music site. In a nutshell, Last.fm allows registered users to create their own radio station that learns the musical tastes of a person and suggests new tunes personalized to the user interest. In addition, users can listen to the radio stations of friends and other Last.fm users.

2.1.3.4 Functional

Functional SNS provide different specific functionalities such as blogging, photos sharing, status sharing, social bookmarking and reviews of product. Often, these SNS does not necessarily capture demographic information but rather a large amount of per-

[17] http://corporate.xing.com/no_cache/english/company/xing-ag/
[18] Recognized experts with specialist knowledge of their particular field of work
[19] http://flixter.com
[20] http://last.fm
[21] http://www.flixster.com/about/

sonal information such as pictures. Examples of functional SNS include *LiveJournal*[22] (blog), *Picasa*[23] and *Flickr*[24] (picture sharing), *Digg*[25] and *StumbleUpon*[26] (social bookmarking), *Consmr*[27] (product reviews).

- *Livejournal*is a virtual community in which Internet users can manage a blog or a diary. In February 2012, more than 35 million accounts existed on LiveJournal with however only 1,9 millions listed as "active in some way"[28].
- *Flickr* is an image and video hosting website gathering an online community created by Ludicorp in 2004 and acquired by Yahoo one year later. Beside being a popular website for users to share and embed personal pictures, the service is widely used by bloggers to host images that they embed in blogs and social media. In June 2011, Yahoo reported that Flickr had a total of 51 million registered members and 80 million unique visitors[29].
- *Twitter* is at the same time a microblogging service and a SNS that enables its users to send and read text-based posts of up to 140 characters known as"tweets". Twitter was originally created in March 2006 by Jack Dorsey and launched the same year in July. The service quickly gained a worldwide popularity with over 300 million users as of March 2011, generating over 300 million tweets and handling over 1.6 billion search queries per day[30].

2.2 Features of SNS

The boundaries between the different types of SNS presented previously is not so clear and becomes fuzzier as many technologies exist to link different SNS together such as *RSS* and *OpenID*.

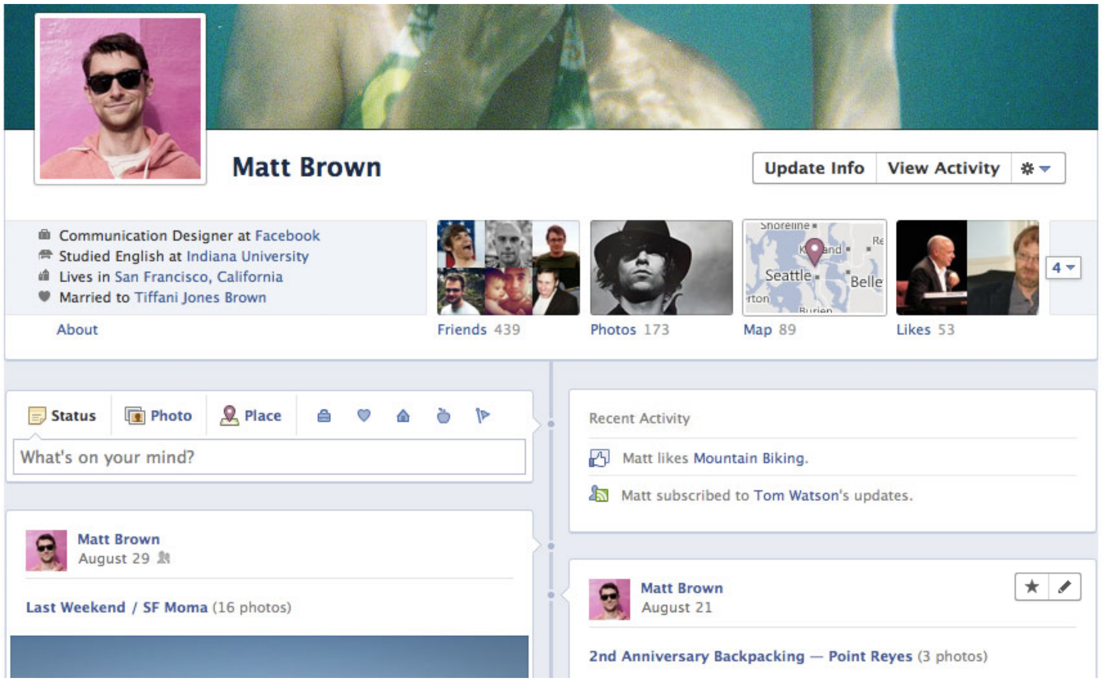
In this subsection, we will detail the different parts that we believe as being central to

[22] http://livejournal.com
[23] http://picasa.com
[24] http://flickr.com
[25] http://digg.com
[26] http://stumbleupon.com
[27] http://consmr.com
[28] http://www.livejournal.com/stats.bml
[29] http://advertising.yahoo.com/article/flickr.html
[30] http://yearinreview.twitter.com/en/whojoined.html

a SNS: *Profile*, *Friends*, *Networking features*, *Social applications and APIs*, and *Privacy and Security*.

2.2.1 Profile

Profiles can be considered as being the basic bricks of SNS. Profiles typically contain basic demographic information about the user such as name, gender, hometown and current location, . . . Alongside this basic personal information, most SNS also encourage users to write a short biography about themselves and to share their tastes and interests. While giving all this information may not be mandatory to register to a SNS, many users often fill their profiles in great details. In some SNS, users can customize their profile page by using skins, web widgets or their own HTML or CSS code. In consequence, the profile of a user ranges from very detailed like the Timeline feature in Facebook (see Figure 2.2) to very simple with only basic information such as Twitter (see Figure 2.3).



Matt Brown

Communication Designer at Facebook
Studied English at Indiana University
Lives in San Francisco, California
Married to Tiffani Jones Brown

What's on your mind?

Recent Activity

Matt likes Mountain Biking.

Matt subscribed to Tom Watson's updates.

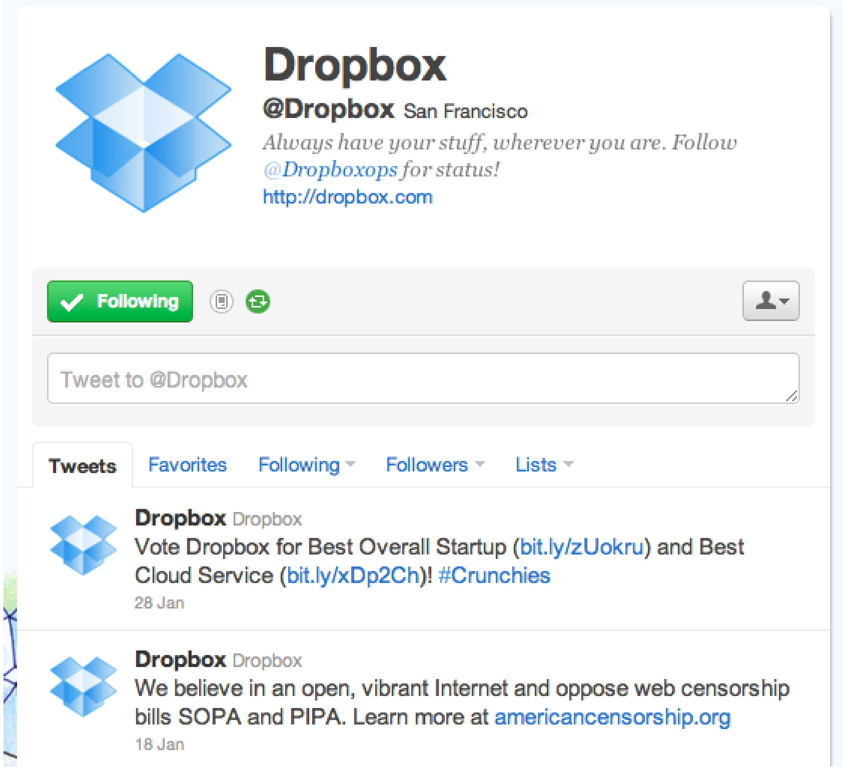
Matt Brown
August 29

Last Weekend / SF Moma (16 photos)

Matt Brown
August 21

2nd Anniversary Backpacking — Point Reyes (3 photos)

Figure 2.2: Facebook Profile with a Timeline view.



Dropbox

@Dropbox San Francisco

Always have your stuff, wherever you are. Follow @Dropboxops for status!

http://dropbox.com

Dropbox Dropbox
Vote Dropbox for Best Overall Startup (bit.ly/zUokru) and Best Cloud Service (bit.ly/xDp2Ch)! #Crunchies
28 Jan

Dropbox Dropbox
We believe in an open, vibrant Internet and oppose web censorship bills SOPA and PIPA. Learn more at americancensorship.org
18 Jan

Figure 2.3: Twitter profile.

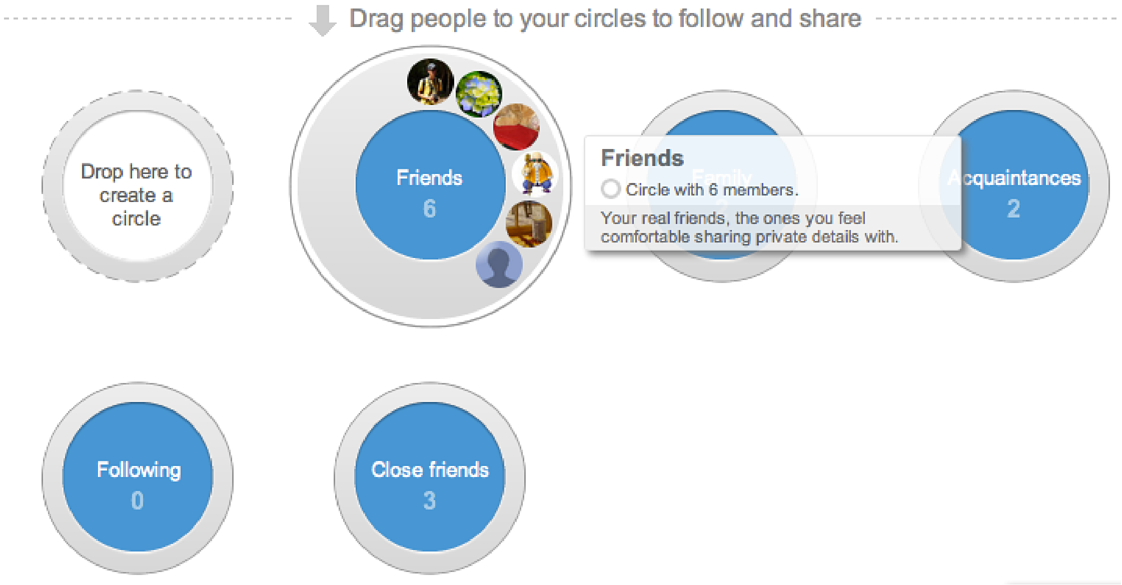
2.2.2 Friends

Most SNS are designed and built around the concept of *"Friends"*. On a SNS, a Friend can be a friend, a family member, an acquaintance, a friend of a friend, or even someone that the user has never met before except online. In 2009, the average number of Facebook friends that a person has is 120[31]. A SNS enables a user to keep track of the activities of his friends: for instance, when they post a new picture, update their profile, change their status or buy something new online.

A SNS generally has a search functionality that can help a user find new Friends. For instance, users can search for friends sharing the same hobbies, belonging to a certain age group, or living in some part of the world. The "friend" relationship can be either symmetric or asymmetric. If the relationship is asymmetric, when a user finds the profile

[31] Facebook Statistics (`http://www.facebook.com/note.php?note_id=55257228858&ref=mf`).

page of a potential Friend, he can directly "follow" that person without requiring his approval. In contrast in the case of a symmetric relationship, the SNS will first send a message to the other user requesting his approval of the Friendship. Afterwards upon approval of the friend request, the relationship becomes visible through the list of Friends of both users. For example in Google+, users can see which users have added them into their social *Circles* and can choose to add these persons into their circle as well (see Figure 6.1).



Your real friends, the ones you feel comfortable sharing private details with.

Figure 2.4: Friends and Circle in Google+.

2.2.3 Networking features

Besides the friendship relationship, some SNS also propose *networking features* to facilitate the interaction between users such as groups, chat rooms, instant messaging and bulletins. Each SNS also has its own particular features such as the ability to "poke" users on Facebook or "high five" a person on Hi5.

- *Groups*.

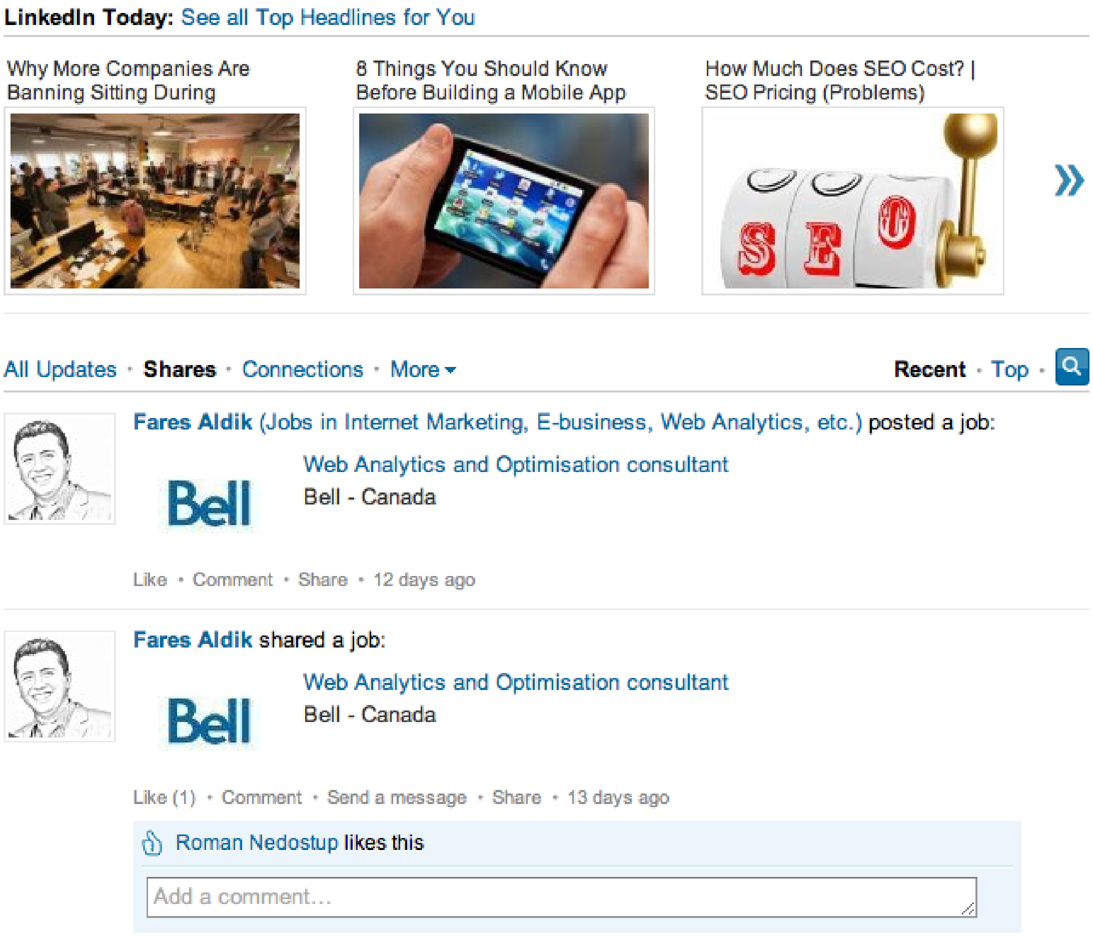
  Most SNS rely on the notion of *group* to help users find people with similar interests or engage in discussions on certain topics. A group can be anything from

"University of Montréal" to "People Who Like Books". Sometimes, groups are called by other names, such as "networks" on Facebook.

- *Events*.

  Events is a networking feature enabling Friends to learn about the coming of new events in their community as well as to organize social gatherings. For instance, on MySpace, it is possible to post a quiz or to decorate an Event page.
- *Tags*. A *tag* is a non-hierarchical keyword or term assigned to a piece of information[32]. For instance, a tag can be an internet bookmark, a digital picture or a computer file. This type of metadata describe an item and allows to find it through browsing or searching. Usually in most of the SNS, a user can associate any number of textual tags to a picture, and then browse through his albums by tags. In Facebook and Friendster, this step is taken even a step further by allowing users to associate a tag with a specific area of a picture. For example, a picture of a family in front of a landmark can have the individual faces of family members tagged with their first names and the landmark tagged with its name. If the tagged subject is not a member of Facebook, then the tag remains in plain text when the picture is published. However, as soon as the tagged subject registers in Facebook, his tag is transformed into a hyperlink to his Profile. When a user is tagged in a picture, he generally receives a brief notice.
- *News Feeds*. A *Feed* is a document (often XML-based) containing content items with web links to longer versions. RSS are useful tools to stay in contact with Friends. For instance, profile updates, blog posts and pictures and videos upload are often disseminated in the form of news feed (see Figure 2.5). The two main formats of web feeds are RSS and Atom. RSS has gained better popularity as it was implemented much sooner than Atom (1999 versus 2005). Atom, on the other hand, provides a mechanism to explicitly and unambiguously label the type of content being provided by the entry, and allows for a broad variety of payload types including plain text, escaped HTML, XHTML, XML, and references to external content such as documents, video and audio streams.[20]

[32] Computer Desktop Encyclopedia.



LinkedIn Today: See all Top Headlines for You

Why More Companies Are Banning Sitting During

8 Things You Should Know Before Building a Mobile App

How Much Does SEO Cost? | SEO Pricing (Problems)

All Updates · Shares · Connections · More
Recent · Top ·

Fares Aldik (Jobs in Internet Marketing, E-business, Web Analytics, etc.) posted a job:

Web Analytics and Optimisation consultant
Bell - Canada

Like · Comment · Share · 12 days ago

Fares Aldik shared a job:

Web Analytics and Optimisation consultant
Bell - Canada

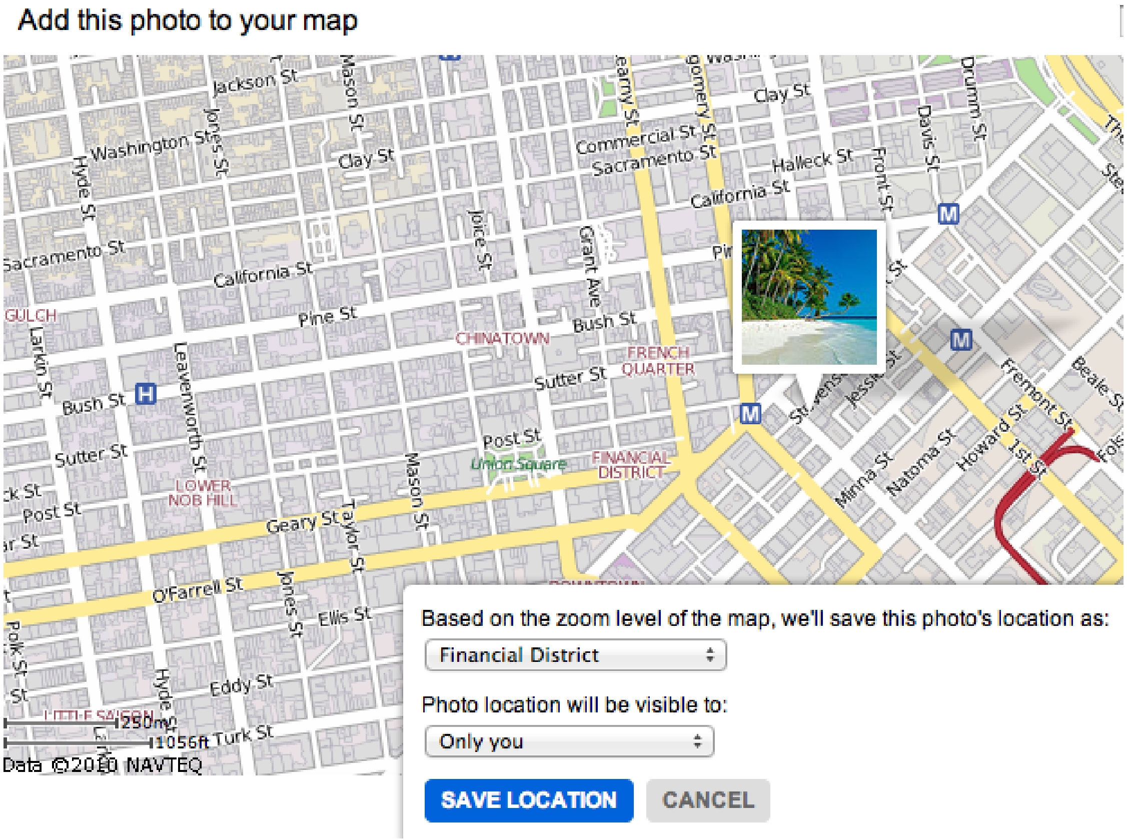
Roman Nedostup likes this

Figure 2.5: New Feeds in LinkedIn.

- *Location Sharing*. Most of the SNS let their users share their location whenever they update their status or post a new comment. For instance, when a user uploads a photo to Flickr, he can specify in which place this photo was taken (see Figure 2.6). The system can also automatically import location data from photos if the user so choose.

2.2.4 Social Applications and APIs

SNS, such as Facebook and Google+, include a vast number of *social applications* that users can add to their profiles. This was made possible because these SNS have



Add this photo to your map

Based on the zoom level of the map, we'll save this photo's location as:

Financial District

Photo location will be visible to:

Only you

Figure 2.6: Photo location in Flickr.

opened their interfaces to third-party developers who design and implement applications for the SNS platform. Each SNS offers its own brand of games and activities. For example, Bumper Stickers is a popular application in MySpace by which users can choose funny stickers to leave on their friends profile. This application was launched on April 2008, and by August 2008, 2.4 million users had installed it.

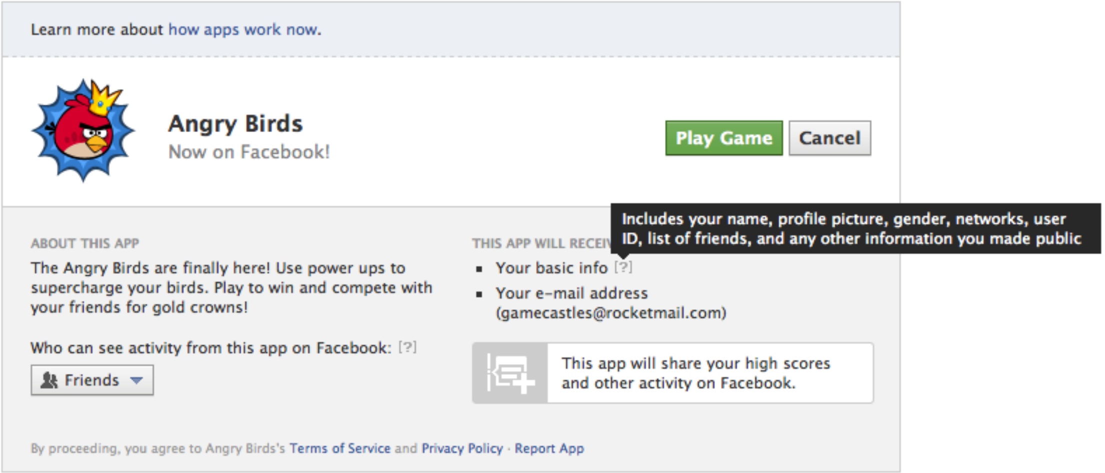
Facebook was the first to release a social networking API for third-party developers in May 2007. Applications built using this API pose serious privacy issues as the “installed” application can query the API for the user’s personal information as well as for information about the friends of the user (see Figure 2.7). Since the release of the Facebook Platform, 19 other sites, including Bebo [33], Friendster, Hi5 [34], Imeem [35], MyS-

[33] http://www.bebo.com

[34] http://www.hi5.com

[35] http://www.imeem.com

pace, Ning [36], Orkut [37], LinkedIn and XING [38], have joined together to support Google's *OpenSocial*, which defines a common API for social applications across multiple SNS. The development of OpenSocial is overseen and managed by the non-profit OpenSocial Foundation [39]. Applications implementing the OpenSocial APIs are made to be interoperable with any social network system supporting them. However, these new APIs, which are usually based on HTML, JavaScript and Google Gadgets [40], suffer from the same privacy concerns as Facebook (see Figure 2.8).



Learn more about how apps work now.

Angry Birds
Now on Facebook!

Includes your name, profile picture, gender, networks, user ID, list of friends, and any other information you made public

ABOUT THIS APP

The Angry Birds are finally here! Use power ups to supercharge your birds. Play to win and compete with your friends for gold crowns!

Who can see activity from this app on Facebook: [?]

Friends

THIS APP WILL RECEI

- Your basic info [?]
- Your e-mail address (gamecastles@rocketmail.com)

This app will share your high scores and other activity on Facebook.

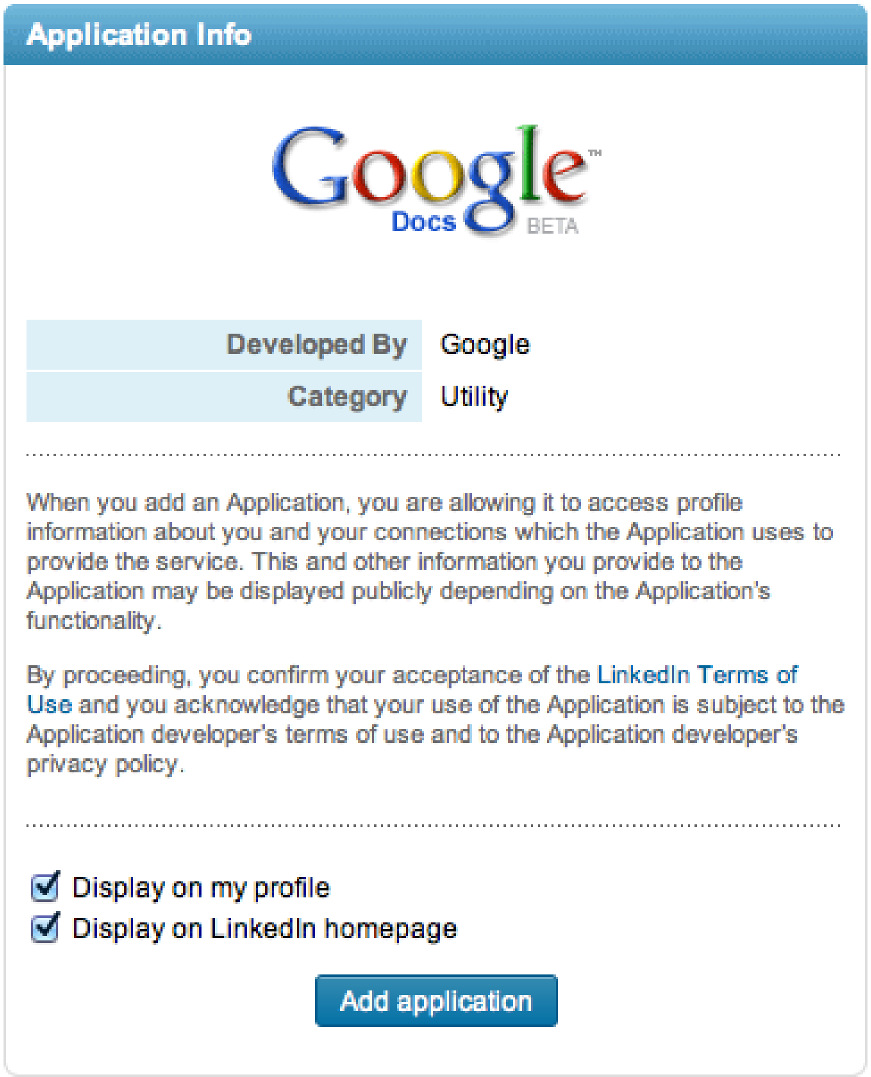
By proceeding, you agree to Angry Birds's Terms of Service and Privacy Policy · Report App

Figure 2.7: Angry Bird game based on Facebook Platform.

2.2.5 Privacy and Security

Most SNS provide privacy settings that can help the user to customize how his information is visible and who can access it. While MySpace only allows users to limit who can access their page, Facebook lets users control who can search for them, how they can be contacted as well as what stories get published to their profile and their Friends' News Feeds. LinkedIn allows users to change the visibility of their profiles and select

[36] http://www.ning.com
[37] http://www.orkut.com
[38] http://www.xing.com
[39] http://www.opensocial.org
[40] Google Gadgets are dynamic web content that can be embedded on a web page and are developped using the Google Gadgets API.



Developed By	Google
Category	Utility

When you add an Application, you are allowing it to access profile information about you and your connections which the Application uses to provide the service. This and other information you provide to the Application may be displayed publicly depending on the Application's functionality.

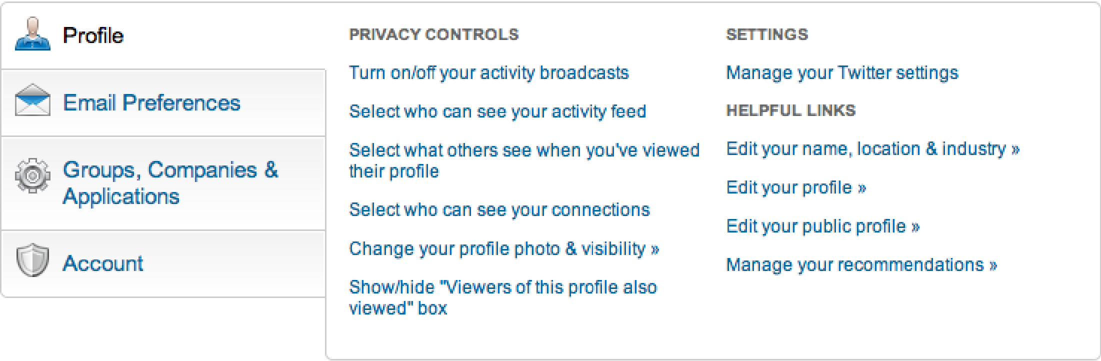
By proceeding, you confirm your acceptance of the LinkedIn Terms of Use and you acknowledge that your use of the Application is subject to the Application developer's terms of use and to the Application developer's privacy policy.

☑ Display on my profile
☑ Display on LinkedIn homepage

Figure 2.8: Google Docs app in LinkedIn.

who can see their activity feed (see Figure 2.9).

For the Net generation, SNS have become the preferred forum for social interactions, from posturing and role playing, sharing photos to simple discussion. However, because such SNS are relatively easy to join and to access, posted content can be viewed by anyone with an interest in the users' personal information. Privacy risks in SNS will be discussed in more details in the next chapter.



Profile

Email Preferences

Groups, Companies & Applications

Account

PRIVACY CONTROLS

Turn on/off your activity broadcasts

Select who can see your activity feed

Select what others see when you've viewed their profile

Select who can see your connections

Change your profile photo & visibility »

Show/hide "Viewers of this profile also viewed" box

SETTINGS

Manage your Twitter settings

HELPFUL LINKS

Edit your name, location & industry »

Edit your profile »

Edit your public profile »

Manage your recommendations »

Figure 2.9: Privacy Settings in LinkedIn.

CHAPTER 3

PRIVACY IN SOCIAL NETWORKING SITES

Activities like chatting, blogging, commenting, posting pictures and spending time on SNS such as Facebook and Myspace have become an important part of the online life of millions of Internet users. SNS record all the interactions occurring between users through the social network and retain them for potential uses such as profiling through data mining or the improvement or development of new services. Due to the high number of activities available on a SNS, large amount of personal information are collected on a daily basis and this information can be very diverse. In recent years, the reputation of SNS has been damaged by a number of privacy incidents relayed by news media and therefore SNS users have good reasons to be concerned about their privacy. Personal information disclosed from SNS could affect users' life, with privacy risks ranging from simple embarrassment to ruining their reputation, or even identity theft. Recently, a health department official in Washington used the message functionality of Facebook to get in touch with a teenager about her sexually transmitted disease (STD). The girl received a message saying that she needed to call the Spokane Regional Health District for important information about her health. The actual STD diagnosis was not included in the post, but the girl's mother says this is still a violation of her privacy [8].

In this chapter, we first examine different types of risks as well as user expectations regarding privacy in SNS. Secondly, we also briefly review the position of some privacy regulations and laws with respect to SNS [6].

3.1 Privacy Risks

There are many risks related to privacy that individuals incur on SNS, but we group them into three main categories: *Security*, *Reputation and Credibility*, and *Profiling*.

3.1.1 Security

Due to the large amount of personal information circulating in SNS, users may be exposed to *online attacks*, including identity theft [7], phishing, malware infection or cyber-harassment. For instance, according to the Identity Fraud Survey Report of Javelin on 2011 [60], people using SNS for five or more years are twice as likely as those newer to SNS to suffer from identity fraud (6.9% for five-plus-year users versus 3.2% for newer users). Moreover in a recent survey of 2011, Sophos points out that 67% of SNS users surveyed received spam messages against 57% at the end of 2009 [92]. Phishing and malware incidents also become more widespread, with 43% of SNS users spotting phishing attempts and 40% receiving malware. In addition, it is also likely that there are more unknowing victims. By collecting personal information available publicly in a user profile such as first and last name, address and date of birth, cyber-criminals may gather enough data to compromise the victims' financial records, thus facilitating organized criminal and terrorist activities.

Teenagers (especially young ones) are the most vulnerable age group for online attacks. They are also at high risk of being approached by online predators or becoming victims of cyber bullying. Online predators try to gradually seduce their targets through attention, affection, kindness, and even online gifts, and often devote considerable time, money, and energy to this effort [46]. Online predators are finding it easier and easier to locate and communicate with potential victims on SNS through publicly shared photos, profile pages and location-based services.

3.1.2 Reputation and Credibility

Reputation is the social evaluation of the public towards a person, a group of people, or an organization. It is an important factor in many fields, such as business, online communities or social status [36]. With the blooming of SNS, users' online reputation has extended beyond the World Wide Web and if the user's reputation is damaged, it can also affect his credibility in real life. As more and more people turn to SNS to chronicle their lives and socialize with friends, they are also learning that their words and pictures are reaching way beyond the circle of friends for whom they were intended [63]. For instance, stories of employees being fired due to social media slip-ups have been numerous in the news over the past few years [70]. On June 2010, five California nurses were suspended after it was discovered that they were discussing patient cases on Facebook. This situation was investigated for weeks by both the nurses' employer, Tri City Medical Center in San Diego, and the California Department of Health before the nurses were fired for allegedly violating privacy laws [95].

In addition, more and more companies use SNS to screen potential employees. In a recent survey of Reppler [96], more than 90% of recruiters and hiring managers have visited a potential candidates' profile on a social network as part of the screening process and 69% of these recruiters have rejected a candidate based on content found on his social networking profile. As a result, users of SNS may lose job opportunities due to the inappropriate information available on their profile. For instance, a teacher in Madison (Wisconsin) was recently suspended after pictures of her with weapons appeared on her Facebook profile [94]. Since the beginning of SNS, companies have turned to them to determine whether there is something about an applicant's lifestyle that would go against the core values of their corporation. But in some cases, they are going even further: Some have demanded applicants hand over their passwords so they can view individual's restricted profiles [99]. Moreover, users not only have to worry about their own profiles but also the profiles of their *Friends* [66]. For instance, even when a user profile is kept clean and professional, it may not really matter if their Friends swear, use drugs, get drunk and put all these things with vivid details with a link to the user profile.

Moreover, SNS affect not only the reputation of the employees but also can cause trouble to the employers. One of the first things many laid-off workers have been doing during this recession is to update their profiles on LinkedIn [23]. One of its features is “Get recommended” where the workers can click an online button and “Have colleagues, clients, teachers, and partners speak up for you". However, if someone has been dismissed because of poor performance, and a manager has given him a positive recommendation, the credibility of the company will be questioned.

3.1.3 Profiling

Profiling refers to “the recording and classification of behaviours” as defined by the Electronic Privacy Information Center [1] (EPIC). It has become an entire industry, sometimes called *Customer Relations Management* (CRM) or simply *Personalization*. Companies collect information from a number of resources, especially SNS, to build comprehensive profiles on individuals in order to sell products and to compile dossiers. This is often performed without the person’s explicit consent or even without leaving the chance for him to opt-out of the dossier building process.

In order to maintain services, SNS providers have to struggle to earn money by advertising. In a recent report of comScore [30], personal SNS such as *MySpace*, *Hi5*, *Bebo*, and *Classmates* accounted for more than 20% of all display ads viewed online in United States, with MySpace and Facebook combined together delivering more than 80% of ads. These statistics show that marketers are eager to use these fast-growing networks to advertise their products. Moreover, an Australian online-marketing company, uSocial, can help them to find potential customers. After trawling Facebook for users by searching for criteria such as age, location and interests, uSocial recommends potential customers to companies, which then approach them directly. For instance, a firm pays $727 for each 5,000 users who agree to be its friend (or 15 cents per friend). “Fans", who merely express support for a firm, are cheaper [38]. Facebook also offers a type of advertising that allows companies to target potential customers by letting users click on an advert to become that company’s fan. As a result, some SNS have become a network of advertising rather than friendship.

Although collecting publicly available data is not illegal, SNS users do not have any control on how this information will be exploited. For instance, it might be used by marketers for targeted advertising or sold to governments for law enforcement purposes. The collected data may affect a user’s welfare in the future as these profiles contain a great amount of personal information such as Social Insurance Number, shopping preferences, health information, household income or lifestyle habits, just to name a few. For

[1] http://epic.org/

example, if Bob boasts his fast driving attitude on an SNS, his car insurance company may classify him as a high risk customer in the future, resulting in a higher insurance rate even if he was never involved in any accident.

These privacy risks are much more noticeable in SNS than personal websites and blogs because SNS provide a sense of intimacy created by the community of online friends. With the motivation to communicate and maintain social relationships, the amount of information revealed willingly by the users is much greater than on other media. Moreover, SNS make it extremely easy to upload many different forms of personal information, such as age, contact information (including home address and phone numbers), pictures, sexual orientation and music preferences. SNS such as Facebook usually encourage users to use their real name, and *Google+* even goes a step further by requiring users to use real names and suspending accounts because the username does not seem to be genuine [104]. According to a 2007 survey [37], 91% of Facebook users and 62% of MySpace participants use their real name to identify themselves and 85% of the respondents either currently share or would share pictures of themselves on the aforementioned sites.

3.2 Users' Privacy Requirements

In order to elicit the privacy requirements of SNS users, we rely on a study in which focus group interviews and a survey of 210 subjects were used to gather the privacy concerns of SNS users [64]. More precisely, the study investigates the privacy concerns of individual users and how they impact the dynamics and self-disclosure of their information on SNS. According to the results of this study, we can define the following three main privacy concerns expressed by SNS users: *general accessibility*, *social threats coming from the user environment* and *organizational threats*.

3.2.1 General Accessibility

General accessibility to profile information was the most frequently mentioned concern. It refers to individuals being afraid of unauthorized access of the information provided on an SNS. Indeed, a report from Harris Poll [53] found that the majority of young adult respondents have a good grasp of the trade-offs involved when using SNS. For instance, an overwhelming majority (85%) of millennials (young adults from 18 to 34 years old) understood that participating to a SNS meant giving up some amount of privacy. Almost as many (81%) specify that their social network profile was only a snapshot of who they really are.

To deal with their distrust, young millennials are actively monitoring their digital footprints, an activity that is not new for them, according to Pew [71]. Between 2006 and 2009, more millennials said that they took steps to limit the amount of information available about them online than did respondents of older age groups. Older internet users appeared to relax their vigilance online while millennials maintained theirs. Moreover, millennials were more likely than older users to change their privacy settings in order to limit their online information, to delete people from their networks or other friends list and to limit who could see certain updates and erase comments that others made on their profile pages. However they did not stop there as 44% said they filtered updates posted by friends and 41% removed their names from pictures that friends had posted and tagged.

3.2.2 Social Threats from User Environment

Concerns about social threats are mainly related to the security risks stemming from the SNS user environment. These threats range from tagging a user in unwanted photos and leaving inappropriate comments about the user on their Wall or other public areas to user harassment such as cyber-bullying or denigration. For instance, peers may bully [43], belittle one another or post malicious comments. One possible consequence of younger groups' use of SNS derives from the rapid forming and dissolution of relationships. The dumpee has the opportunity to slander, abuse or reveal information, such as pictures, about the dumper [14]. A form of stalking behaviour is also possible, with the dumpee continuing to follow the person's activities. Even where relationships have not broken up, friends may post materials that are regarded as compromising without seeking the permission of the persons featured. One tragic example is the story of Phoebe

Prince, an Irish girl who committed suicide in early 2010 [16], who can be seen as a clear victim of this sort of abuse. Bullies from her school in Massachusetts had posted horrible statements about Phoebe as well as tormenting her outside of school. Her death thrust Facebook into the headlines again and clearly demonstrated how teenagers and young persons could use the SNS to victimize and bully classmates.

A 2010 study of Vision Critical [100] showed that 78% of SNS users who visit SNS daily have the impression that SNS are very dangerous places for children and teenagers. Another study of Ybarra, Michele and Mitchell [105] confirms this concern as 4% of participants from 10 to 15 years-old reported that they had received unwanted sexual solicitation on SNS. Moreover, they feel that these networks are "ruined" by "scams" and "sleazy ads." The situation appears to create an environment in which users are continually forced to assess the credibility of the persons and information they encounter.

3.2.3 Organizational threats

Organizational threats correspond to the privacy concerns that the members of the focus group raised with respect to the information collected by the SNS providers. Users tend to reduce self-representation on the platform when they fear that their information will be collected, stored, and used by the SNS and other third parties [51]. Indeed, when posting content that is covered by intellectual property rights, like pictures and videos ("IP content"), users are required to grant Facebook with a non-exclusive, transferable, sub-licensable, royalty-free and worldwide license to use any IP content that the users post or in connection with Facebook. As a result, in the Pew Internet and American Life Project's "Reputation Management and Social Media" report [71], 28% of 18-to-29-year-olds said they "never" felt they could trust a SNS, and half (51%) said only "sometimes."

3.3 Privacy Laws and Regulations

Individuals may assume that the same laws or societal rules that protect their privacy in the real world would apply as well to the digital world. However, the Internet remains largely unregulated and laws dealing with online privacy in general and SNS in particular are still under development [28]. In this section, we briefly review the position of some privacy regulations and laws with respect to SNS.

3.3.1 OECD Guidelines

The privacy guidelines issued by the Organization for Economic Cooperation and Development (OECD) [2] in 1980 became the basis of privacy laws and related policies in many countries, including the United States, Canada, Germany, Sweden, Australia, and New Zealand, as well as the European Union. These guidelines involve eight principles, which are often referred to as “*fair information practices*":

1. *Collection Limitation Principle:* The collection of personal data should be limited and obtained by lawful and fair means and, when appropriate, with the knowledge or consent of the data owner.
2. *Data Quality Principle:* Personal data should be as relevant, accurate, completed and up-to-date as possible for the purposes of data collection.
3. *Purpose Specification Principle:* The purposes of data collection should be specified at the time of collection and upon every change to these purposes. The use of personal data should closely follow these similar purposes.
4. *Use Limitation Principle:* Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Principle 3 without the consent of the data owner or the relevant law authority.
5. *Security Safeguards Principle:* Reasonable security measures should be employed to protect personal data against loss or unauthorized access, destruction, use, modification or data disclosure.

[2] http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html

6. *Openness Principle:* The public should be informed about privacy policies and practices, and individuals should be provided ready access to the use and collection of personal information.
7. *Individual Participation Principle:* An individual should have the right to know about data collection, to retrieve collected data, to change or delete collected data in a reasonable manner and to challenge the denial of these rights.
8. *Accountability Principle:* A data controller should be accountable for taking measures to implement these principles.

The privacy laws reviewed in the following subsections have been directly influenced by these fair information principles and the guidelines from OECD.

3.3.2 Europe

Early in 2009, the European Union (EU) Information Society Commissioner Vivianne Redding invested significant efforts in encouraging all major SNS to draft and adapt self-regulatory practices in order to improve the safety level for young users for SNS. Eighteen SNS providers (including Facebook, Bebo, DailyMotion and MySpace) have joined together in an agreement called the *Safer Social Networking Principles* for the EU [3], through which the participants accept to abide by basic self-regulatory principles, including:

1. Raise awareness about safety and acceptable behaviors.
2. Ensure that services are age-appropriate for the intended audience.
3. Empower users through tools and technology.
4. Provide easy-to-use mechanisms to report illicit conduct or improper content.
5. Promptly respond to notifications of illegal content or conduct.
6. Enable and encourage users to employ a safe approach to personal information and privacy.

[3] http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf

7. Assess the means for reviewing illegal or prohibited content/conduct.

On March 2011, Ms Redding, now Vice-President of the European Commission and EU Justice Commissioner, stated in a speech that SNS need to comply with the European laws if they have information about European citizens, and especially the *four pillars of privacy laws* in the EU [18]:

1. *Right to be forgotten:* Companies have to demonstrate the need for collecting personal data and the users have the right to withdraw or opt-out of any data collection efforts.
2. *Transparency:* Companies have to fully disclose to users all information regarding the data collection process.
3. *Privacy by default*: The default privacy settings should reflect a “true privacy” level for the users.
4. *Protection regardless of data location:* Privacy standards for European citizens should apply independently of the area of the world in which their data is being processed.

3.3.3 Canada

Canada is a federal country with shared jurisdiction between the federal government and the provinces or territories. Canada’s legal system protects privacy through the Canadian Charter of Rights and Freedoms, Canada’s Criminal Code and a number of provincial laws. For example, Canada’s federal private sector legislation, the Personal Information Protection and Electronic Documents Act (PIPEDA), last amended on April 2011 [4], imposes obligations on entities that collect, use or disclose personal information in the course of commercial activities. Ultimately, PIPEDA aims at striking a balance between a business’ need to use personal information to offer services and products, and an individual’s right to control how his personal information is used by that business. This model code incorporates the principles of: (1) *accountability*, (2) *identifying purposes*, (3) *consent*, (4) *limited collection*, (5) *limited use, disclosure and retention*,

[4] `http://laws-lois.justice.gc.ca/eng/acts/P-8.6/`

(6) *accuracy*, (7) *security measures,* (8) *openness*, (9) *individual access*, and (10) *challenging compliance*. As a principle-based statute, PIPEDA has proven to be remarkably technology-neutral and continues to be relevant in the face of newer technologies that were not even imagined at the time it was enacted.

Canadian courts are now familiar with Facebook and SNS and recognize that they contain private and personal information. Several cases have dealt with the relatively new issue of privacy and the production of the contents of a Facebook profile. The majority of cases are from Ontario, but it has relevance across the country. Generally, when the courts have determined that the personal information on a litigant's SNS is relevant to the matter before the court, they have ordered disclosure of that information. Courts have also affirmed in these cases that determining the relevance of information includes a consideration of privacy interests of the different actors. This may include any prejudice to the litigants or any third parties that may result from the disclosure of information from a SNS. However, courts have refrained from broadly concluding that privacy overrides established production obligations and the determination of relevance is made on a case-by-case basis. The test for relevance involves weighing the probative value of disclosing the information from a SNS versus its prejudicial effect. Moreover, parties must still prove the information's relevance, and privacy is still a factor the court considers when ordering disclosure.

3.3.4 Bill of Rights

The idea of having a *Bill of Rights for Users of SNS* has been around for some years, but no large audience of users has actually collated the key values and principles that should go into such a Bill of Rights and put them to a world-wide large scale vote. On May 2010, the Electronic Frontier Foundation has suggested three basic privacy-protective principles that SNS users should demand from their providers: *the right to have informed decision-making*, *the right to control* and *the right to leave* [78]. Based on these basic principles, attendees of the Computers, Freedom, and Privacy conference held in San Jose in June 2010[5] have proposed the following Social Network Users' Bill

[5] http://www.cfp2010.org/

of Rights:

"We the users expect social network sites to provide us the following rights in their Terms of Service, Privacy Policies, and implementations of their system:

1. *Honesty: Honor your privacy policy and terms of service.*
2. *Clarity: Make sure that policies, terms of service, and settings are easy to find and understand.*
3. *Freedom of speech: Do not delete or modify my data without a clear policy and justification.*
4. *Empowerment: Support assistive technologies and universal accessibility.*
5. *Self-protection: Support privacy-enhancing technologies.*
6. *Data minimization: Minimize the information I am required to provide and share with others.*
7. *Control: Let me control my data, and do not facilitate sharing it unless I agree first.*
8. *Predictability: Obtain my prior consent before significantly changing who can see my data.*
9. *Data portability: Make it easy for me to obtain a copy of my data.*
10. *Protection: Treat my data as securely as your own confidential data unless I choose to share it, and notify me if it is compromised.*
11. *Right to know: Show me how you are using my data and allow me to see who and what has access to it.*
12. *Right to self-define: Let me create more than one identity and use pseudonyms. Do not link them without my permission.*
13. *Right to appeal: Allow me to appeal punitive actions.*
14. *Right to withdraw: Allow me to delete my account, and remove my data."*

The voting of this Bill of Rights was opened until June 15, 2011 on Twitter[6] and Facebook[7]. To the best of our knowledge, the results of this vote have not been published

[6] `http://act.ly/23h`

[7] `https://www.facebook.com/CFPBillOfRights`

yet.

In this chapter, we have categorized different privacy risks that a user incurs when putting personal information on SNS and identified user privacy requirements for these SNS. While SNS and privacy may seem a priori to have two opposite goals, the next chapter will detail our proposed Privacy Framework which an SNS can integrate into its design to enhance the privacy of its users.

CHAPTER 4

PRIVACY FRAMEWORK FOR SOCIAL NETWORKING SITES

Since their introduction, SNS have fundamentally changed the way people communicate and interact with each other. However, alongside with the wealth of applications they offer, SNS also bring new risks due to the nature and the personal character of the information they collect and store. In particular, digital data (and thus personal data) can be easily copied, modified and disclosed without their owner's consent or without the explicit acknowledgment of other possible co-owners. In order to identifies the main privacy issues that SNS users have to face, we have conducted our own survey to *examine the usage and privacy concerns* raised by SNS [54].

To address the user privacy concerns detailed in Chapter 3, we introduce a *privacy framework tailored for SNS*. Specifically, since privacy revolves around user data, we have divided user data into groups having different privacy concerns and categorize the data based on its inherent privacy risk and its importance to the users. Afterwards, based on these categories, we describe a *User Privacy Policy* (UPP) that offer to users an easy and flexible way to express and communicate their privacy concerns to other users, third parties and SNS service provider. However, allowing users to express their privacy preferences is only the first step to enhance the protection of privacy in SNS and is not sufficient as such. Indeed, it is also fundamental to ensure that this privacy policy will be enforced in practice by the SNS provider and more generically to design a privacy-enhanced environment for the users. To this end, we introduce at the end of this chapter, the concept of a Privacy-enhanced Social Networking Site (PSNS).

4.1 Privacy Survey

Our preliminary study is based on an online survey that took place during ten days on September 2008 with 200 participants. Participants of the survey were mostly students and professionals in Canada, in which 71.5% (144 participants) have at least one

SNS account. These 144 participants are split mainly between students (51.39%) and employees (43.75%), with a majority within the age group of 18-30 years (74.31%). Moreover, the participants of our survey have a high level of education (59.72% have a Master or a higher degree), which we recognize may induce a bias on the output of the study.

The questionnaire contained 28 questions relating to *demographic attributes* (such as age, occupation, gender, etc.), *SNS usage* (main reason for joining the SNS, information put on the profile, relation to friends, etc.) and *privacy concerns* such as intellectual property and fear of unauthorized data access. Some of these questions were inspired from an earlier study on online privacy concern and protection on the Internet [21].

The survey was available online in English [1] and in French [2].

In the next section, we present our privacy framework derived from the results of this study as well as user privacy concerns and privacy principles.

4.2 Privacy Framework

The Privacy Framework is composed of the categorization of *User Data*, *Privacy Concerns*, *Groups of Trust* as well as *Privacy Levels* and *Tracking Levels*.

4.2.1 User Data

With the motivation to communicate and maintain relationships, the amount of information revealed willingly by user on SNS is much larger than what users usually shared on other media. In addition, SNS make it extremely easy to upload personal information such as age, contact information (including home address and phone number), pictures, sexual orientation and music preferences. Our study shows that 64.58% of the participants share photos of themselves on the SNS. Moreover, 93.06% of them are ready to provide partially or completely all the personal information on the SNS if they are required to do so. In our study, the users have listed the different types of information that

[1] `http://spreadsheets.google.com/viewform?key=p7AZRICDTMB4yGleAbYOwOA&hl=en`

[2] `http://spreadsheets.google.com/viewform?key=p7AZRICDTMB5J8EhxCVkFbg`

they put on their personal profile (see Figure 4.1).

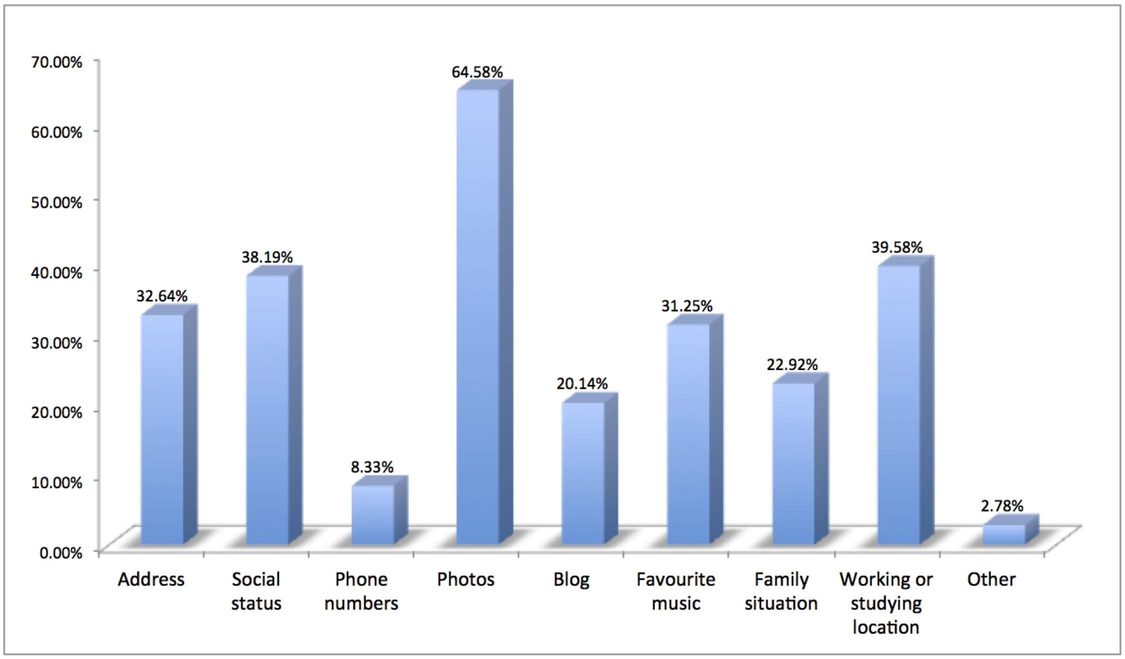


Figure 4.1: Information on SNS profiles.

Based on the answers to this study as well as the main features of a SNS (see Section 2.2), we categorize user data into 5 groups: *Identity*, *Demographic attributes*, *Activity*, *Social network*, and *Added content* (see Figure 4.2).

- The **Identity** refers to information that uniquely characterizes a user (or at least a small subset of individuals) and can be used to identified him such as his name, his address, his phone number or his social insurance number [72]
- The **Demographic attributes** refers to characteristics of the user that are far from being unique in the population such as age, gender, race or political view.
- The **Activity** lists all the activities performed by users through the SNS, such as adding new Friends, writing a comment in the profiles of other users or changing their status.
- The **Social network** refers to all the relationships of users in SNS, such as the identities of their Friends or the groups to which they have subscribed.
- The **Added content** corresponds to all the additional information (not included

in the previous items) that users put on their profile, including blogs, pictures, musical preferences or video clips.

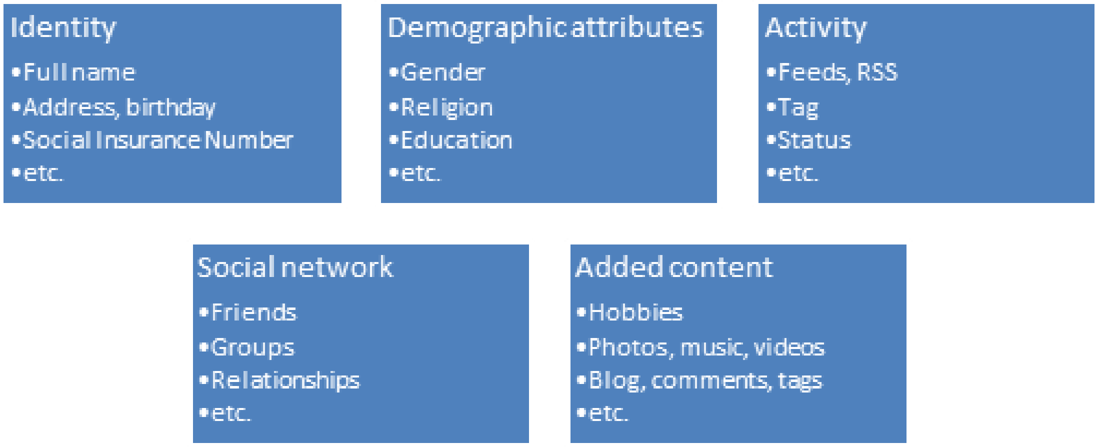


Figure 4.2: Different types of information put by users on their profiles.

4.2.2 Privacy Concerns

In order to estimate how much SNS users value their online privacy, we have performed a k-means cluster analysis on the answers given questions related to privacy concerns. For instance, this set of questions includes the following one: *“Are you concerned that the information you agree to share specifically with someone might be inappropriately forwarded to other users?”*. The answers vary from 1 (Not at all concerned) to 5 (very much concerned).

The k-means clustering algorithm when performed with $k = 2$ outputs two groups with respectively 92 and 52 members. Table 4.I details the average value of each variable for each group. For instance, members of Group 1 (63.88%) consider online privacy to be an important factor while members of Group 2 (36.11%) seem less concerned about privacy as their ratings are below the average.

Since it is clear that users may have different privacy expectations with respect to each piece of personal data, we propose four privacy settings that corresponds to the impact that a particular piece of user data may have on the privacy of a user: namely *Healthy*, *Harmless*, *Harmful* and *Poisonous*.

Table 4.I: Composition of the two clusters outputted.

Questions	**Cluster**	
	G1	G2
	Average	Average
Are you concerned that the information you agree to share specifically with someone might be inappropriately forwarded to other users?	4	3
Are you concerned that the photos shown in your profile may be downloaded and transmitted by others?	4	3
Are you concerned that the people you only know online are not who they say they are?	4	2
Are you concerned that other people might reveal your real identity and personal information online without your consent?	4	3
Are you concerned that your intellectual properties might be copied or abused by others? (For example: articles, photos and ideas)	4	2
Are you concerned about online identity theft, profiling or phishing?	4	2
Are you concerned that the SNS provider might divulge your information to other parties without your explicit consent?	4	3

- **Healthy data** refers to generic information about users such as nick name, hobbies, landscape pictures and music states. Specifically, even if an unauthorized person can get access to this data, it cannot be easily tracked back to the identity of the user. Therefore, we feel that a user can share this data with other entities without really worrying about the effect on his privacy.
- **Harmless data** contains demographic attributes, such as gender, religion, age group and political affiliation. The disclosure of harmless data as such does not generate *Security* risks or *Reputation and Credibility* risks. However, it can lead to *Profiling* as some marketing companies can collect this data and build a detailed profile of the user out of it.
- **Harmful data** corresponds to inappropriate pictures or blog entries that may damage the user's reputation (*e.g.*, a picture of Alex in his job uniform smoking pot). Therefore, the disclosure of this data can lead to *Reputation and Credibility* risks.
- Finally, **Poisonous data** is all the personal information that can potentially cause *Security* risks in case of disclosure such as the financial information or the name and address. In particular, one of the main risk is that cyber criminals may use this data to commit an identity theft.

The above classification of the user data is used by default but can be customized by the user depending on his privacy circumtances.

4.2.3 Groups of Trust

Basically, these four Privacy settings (*i.e.*, Healthy, Harmless, Harmful and Poisonous) are graduated by how much the disclosure of such information can lead a privacy risk for the user. Nonetheless, this categorization of user data is not sufficient on its own. Specifically, the level of risk does not depend only on the type of data being shared, but also on the person with whom this data has been shared. For example, allowing your sister to view your address and phone number (Poisonous data) might not be a risky thing to do because of the trust you have in your sister of not sharing or using this information against you. In our study, the average size of friends list varies significantly among the participants from less than 20 friends (32.64%), to 20 up to 50 friends (27.78%), 51 up to 80 friends (8.33%) and finally even more than 80 friends (30.56%). Most of the participants admitted that they have some persons in their "Friends list" that they know from real life but that are not really their friends (68.06%), or even strangers that have asked them to be their friends (25%) or people they would like to know better (5.56%) (see Figure 4.3). Moreover, around 26% of the participants of our survey admitted that they have already disclosed to other persons some pictures and comments of their friends without their explicit consent. Therefore, it seems likely that the privacy risks are exacerbated when the number of so-called friends is very large rather than when the user has a small core of close friends that can be more easily trusted.

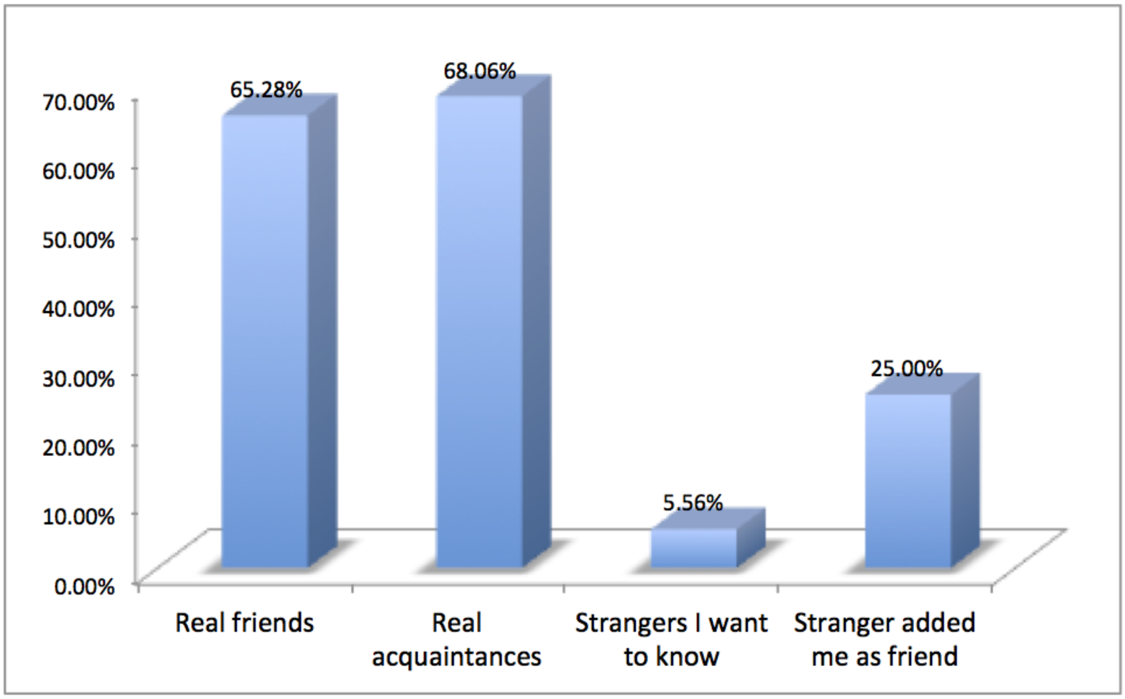


Figure 4.3: Which types of persons do you have in your friend lists?

Thus, according to the intimacy and trust that a particular SNS user has on his friends, we classify the person that can have access to the user profile into four basic groups: *Best Friends*, *Normal Friends*, *Casual Friends* and *Visitors*.

- The **Best Friends** are persons that the user trusts to the point that he can share nearly everything with them. Often, these persons are also the best friends of the user in real life.

- The **Normal Friends** can be family member, relatives or friends in real life.
- The **Casual Friends** usually correspond to persons whom the user knows only a little bit. For instance, the user may only be acquainted with them online.
- The **Visitors** could be users of the SNS or even outside not part of it. These persons are not directly part of the Friend list but they might be able to view some part of the profile of the user such as his name, his age, his location or his avatar.

4.2.4 Privacy Levels

Based on the classification of *privacy concerns* and *groups of trust*, we adapted the four levels of privacy developed in a previous work [2] to the context of SNS. More precisely, the four basic privacy levels that we have considered are the following.

- **No Privacy**: The user does not care about the privacy of his personal information. Basically, this results in everyone being able to see all the information that he has put on the SNS.
- **Soft privacy**: The user wants to show his Poisonous data only to his Best Friends, while the Casual and Normal Friends can access to the data of the user, except the Poisonous one. Finally, the Visitors are allowed to see only Harmless and Healthy data.
- **Hard privacy**: Like Soft privacy, the Normal Friends can still have access to Harmful data but the user put more limit on Visitors as they can only see the Healthy data while the Casual Friends only have access to Harmless and Healthy data.
- **Full privacy**: The user does not allow Visitors to access any information put on his profile. Moreover, the Poisonous and Harmful data are restricted to Best Friends and the Normal and Casual Friends can only access Harmless and Healthy data only.

Table 4.II summarizes the access rights of the four categories of groups of trust depending on the privacy level chosen by the user.

However, we think it is important to point out that a perfect level of “Full Privacy” does not really exist in SNS as the main objective of a SNS is about the sharing of

Table 4.II: Privacy levels.

	No Privacy	**Soft Privacy**	**Hard Privacy**	**Full Privacy**
Best Friends	All data	All data	All data	All data
Normal Friends		Harmful, Harmless and Healthy data	Harmful, Harmless and Healthy data	Harmless and Healthy data
Casual Friends			Harmless and Healthy data	Healthy data
Visitors		Harmless and Healthy data	Healthy data	No data

information. For instance, if someone really wants to keep some information private, he should simply not upload this information of the SNS.

4.2.5 Tracking Levels

Besides these privacy levels, the user may also worry about being tracked through profiles of other SNS users. Basically, there are three possible ways of tracking a user on a SNS: by clicking a profile link in a Friend list of a user, by following the name tag of a user or by reading information about a user through the profile of one of his Friends. To take this aspect into account, we have adapted the three Tracking levels defined in previous work [1, 52] to the context of SNS (see Table 4.III).

- **Strong tracking**: The user does not mind being tracked on SNS, whatever the means used to do that.
- **Weak tracking**: The user does not care if his name appears on the Friends list of another user but he does not want his Friends to be able to put a tag on their Profile that is directly linked to his profile.
- **No tracking**: The user does not want to be mentioned at all in his Friends' profile (*i.e.*, no name, no pictures, no tags) and he is unsearchable through the SNS.

We think of the privacy levels and the tracking levels that we propose as privacy settings that can enable a user to set the good equilibrium between his privacy and the

Table 4.III: Tracking Levels.

	Strong tracking	**Weak tracking**	**No tracking**
Best Friends	Tracking allowed	No tag	No information
Normal Friends			
Casual Friends			
Visitors			

utility he can get of the SNS. Indeed as the main objective of a user of a SNS is to connect persons and to share information, a SNS would become useless by definition if all the users of the SNS consider all their information as Harmful data and do not want other users to see it.

4.3 User Privacy Policy (UPP)

In order to enable users to communicate their privacy preferences before allowing access to their data, we propose to express them in the form of a User Privacy Policy (UPP). This UPP will act as an easy-to-understand policy for other users but also as a machine-readable policy for service providers and third parties [3].

Consider for instance the following illustrative scenario in which Alice has taken some pictures and considers them as being “private”. Alice only wants to share them with her friend Bob. In order to prevent Bob from distributing those photos without her consent, she specifies a UPP stating that only Bob can access her photos and thus restricting Bob from sharing them with other users. As such, the UPP is an effective mean to communicate Alice’s privacy preferences to her friends, and in this case to Bob in particular. Moreover, being a conservative person with respect to her privacy, Alice does not want anyone else besides her friends to learn anything about herself through interactions with the SNS, including her personal information and her contacts. However, when a friend of Bob visits his profile, he can easily discover Alice’s name on Bob’s Friends list. Moreover if that person mines the profile of Bob, he may also see all interactions between Bob and Alice. For instance, he may be able to discover statements such as “Yesterday, Bob comments on one of Alice’s photos”. In this case, a well-defined UPP (if enforced) would make Alice's name "disappear" completely from Bob's profile and therefore becoming invisible to the eyes of other users.

Furthermore, the UPP can also act as a kind of contract between Alice and Bob. Indeed, if Bob wants to become Friend with Alice, he has to accept and respect the privacy preferences of Alice such as not disclosing Alice's pictures and not mentioning her name in his profile and albums. One of the advantage of the UPP is that it can be easily adapted to work with any SNS. Overall, we think that the UPP should be able to address the following questions:

1. Who can access to the data?,
2. Which kind of data is being accessed?,
3. How will this data be used? and
4. What kind of tracking is allowed?.

4.3.1 Related Work

The UPP is inspired from P3P (The Platform for Privacy Preferences Project). The P3P standard is a protocol allowing websites to declare their intended use of information they collect [33]. Its main purpose is to give users more control over their personal information when surfing by enabling them to understand how websites use this information and also evaluating if a particular website respect his privacy desiderata (also expressed in the form of a P3P policy). P3P was developed by the World Wide Web Consortium (W3C) and officially recommended in 2002.

When a website uses P3P, it defines a set of policies stating their intended uses of personal information that it may be gathering from its visitors. On the user side of P3P, the user has also to specify his own set of policies and to state which personal information can be gathered by the websites that he visits. Then, when a user surfs on a particular website, P3P will compare the personal information the user is willing to disclose, and the information the server is asking for. If these two sets do not match, the P3P tool will inform the user about this fact and ask if he wants to proceed anyway to the website, thus risking to give more personal information than he is normally willing to do [3].

Despite their advantages, P3P tools are often too complex and confusing for most Internet users [39]. Moreover as many websites are reluctant to use P3P, when P3P users attempt to access the majority of commercial websites, they experience endless pop-up windows warning them that the website they are planning to visit is not compatible with their specified privacy preferences. Microsoft Internet Explorer, one of the most popular web browser, is able to display P3P privacy policies and compare the P3P policy with the user privacy settings [55]. However, the P3P functionality in Internet Explorer will not alert users if they entered a website that violates their privacy preferences. As a result, users who wish to take full advantages of P3P functionalities have to install additional software such as Privacy Bird [4] [24, 34]. Privacy Bird searches automatically for privacy policies at every web site the user visits and gives warnings about whether each site's policies match the privacy preferences of the user (see Figure 4.4).

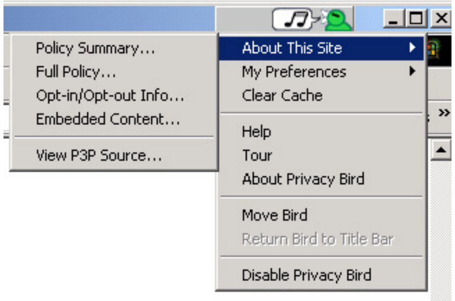


Figure 4.4: Privacy Bird.

The concept of UPP is also similar to the *User Data Policy* specified in the User-Centric Authentication and Privacy Control Mechanism for User Model Interoperability [101]. The User Data Policy is composed of two parts: *policy about application providers* and *policy about data usage*. First, the policy about application providers contains a list of trusted application providers and a list of blocked ones. Second, the policy about data usage is the classification of user data that are accessible to the data provider. The user can modify and update both parts of the User Data Policy at any time.

[3] The P3P Implementation Guide, retrieved 10.02.2012 from `http://www.p3ptoolbox.org/guide/section2.shtml`

[4] `http://www.privacybird.org/`

A popular way for users to share their work freely while maintaining control is to publish their work under a Creative Commons license [5]. Creative Commons licenses apply to work that are protected by copyright such as books, websites, blogs, pictures and other visual images, as well as to movies and sound recordings. These licenses give to the owners of such works, the ability to express permissions for others with respect to their work, such as the right to copy, to make derivative products or adaptations, to distribute or to make money out of their work. Creative Commons licenses are attached to the associated work and authorize everyone who comes in contact with the work to use it in a way that is consistent with the license. Unfortunately, personal data is not considered as a work in the same sense as movie or pictures so it cannot be protected by Creative Commons licenses. For instance, if Bob has a copy of Alice's Creative Commons licensed work, Bob can give a copy to Carol and Carol will be authorized to use the work consistently with the Creative Commons license. As a consequence, Alice is now considered as having a license agreement separately with both Bob and Carol, also she has maybe never been in contact directly with Carol.

Creative Commons licenses are expressed in three different formats: the Commons Deed (human-readable code), the Legal Code (lawyer-readable code), and the Metadata (machine-readable code) [26]. Creative Commons have also been extended to SNS through a third-party Facebook application [15] enabling users to choose a license for their photos, videos, and status updates and to place a Creative Commons license badge on their Facebook profile. Unfortunately, it is currently not possible to choose a Creative Commons license using a fine granularity such as a per picture or video basis. Following this step, Kang and Kagal have proposed a privacy-awareness framework for SNS called Respect My Privacy [61]. This framework enables users to declare the restrictions they wish to place on their data. Moreover, unlike Creative Commons that provides a standard set of licenses, communities of users can easily generate their own privacy/usage ontologies. However, Respect My Privacy encounters the same difficulty as Creative Commons licenses as the terms of use of Facebook itself still holds on this data regardless of the attached license.

[5] http://creativecommons.org/

4.3.2 Specification

The UPP follows the spirit of P3P but not exactly all its principles. For instance, likewise P3P, UPP is used to communicate privacy preferences among SNS users as well as between the user and the SNS provider or third party applications. As many companies are reluctant to adopt P3P, there are few websites on which the users can surf securely according to their preferences. While UPP is issued by the data owners themselves, and therefore everyone who wants to access the data of the user is obliged to abide by this policy (unless of course someone tries to access this data in a fraudulent manner).

When a user wants to limit the access to his data, he specifies a set of policies stating which type of personal information can be shared with which types of users. In order to become his Friend and access to his data, other users have to accept to abide by these policies. The same principle also applies to the SNS provider and to the third-party applications. For instance, the system will warn the user when the privacy policy of a third-party application conflicts with his UPP. In this situation, the user has basically two choices: (1) to accept to change his UPP according to that privacy policy or (2) reject the application.

We describe thereafter the main elements of UPP, which are expressed in XML format (see Figure 4.5).

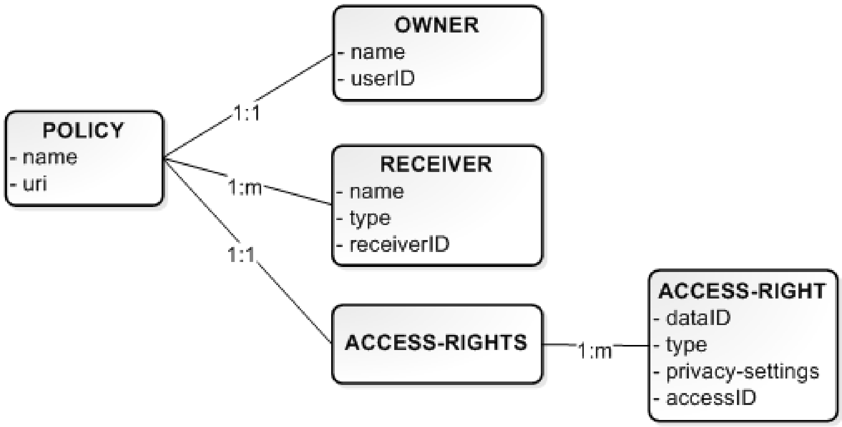


Figure 4.5: Elements of UPP.

- **The POLICY element.** A UPP may contain one or more POLICY element. The POLICY element corresponds to all the information of a policy and contains one owner, at least one receiver and one access rights. The main attributes of the Policy element are:
  - Name (mandatory): name of the policy.
  - URI (optional): URI of the natural language privacy statement.
- **The OWNER element** gives information about the issuer of this policy such as:

  ```
  <OWNER name= "Cindy" userID="Cindy1234"/>
  ```

  This element has two mandatory attributes: name and userID.
- **The RECEIVER element** contains a precise description of the object of this policy, such as a username, a group of users or an application. For example, this element could appear as:

  ```
  <RECEIVER name="CasualFriends" type="group" receiverID="CS1"/>
  ```

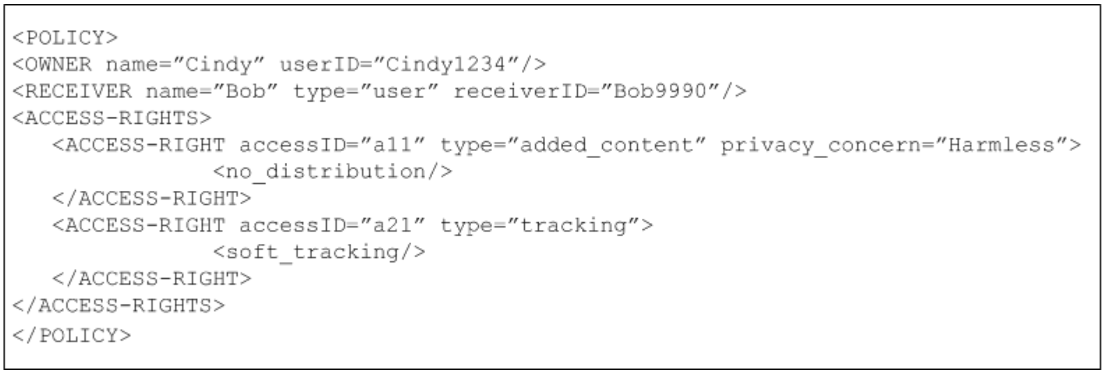
- **The ACCESS-RIGHTS element** indicates how the receiver of personal information should handle this information and may contain multiple ACCESS-RIGHT elements. Each ACCESS-RIGHT element contains the following attributes:
  - DataID (optional): id of the concern piece of information
  - AccessID (mandatory): id of the access right.
  - Data type (mandatory): Identity, Demographic Attribute, Activity, Social network, Added Content or Tracking.
  - Privacy concern (optional): represent the privacy concern of this piece of information: Healthy, Harmless, Harmful or Poisonous.

  The ACCESS-RIGHT element can have different values, including no_comment, no_distribution or no_tracking, weak_tracking, strong_tracking.

  ```
  <ACCESS-RIGHTS>
     <ACCESS-RIGHT accessid="a1" type="added_content"
  privacy_concern="Harmless">
                 <no_distribution/>
     </ACCESS-RIGHT>
  ```

```
    </ACCESS-RIGHTS>
```

Figure 4.6 describes an UPP of Cindy for Bob. All Cindy's Added Content set as "harmless" is viewable by Bob. However, Bob is not authorized to redistribute or share them with others. Furthermore, Cindy does not want her name to appear in Bob's profile and requires "weak_tracking", thus, Bob does not have the right to include her name in his Friend list or link to her profile (tag) in his blog.



```
<POLICY>
<OWNER name="Cindy" userID="Cindy1234"/>
<RECEIVER name="Bob" type="user" receiverID="Bob9990"/>
<ACCESS-RIGHTS>
   <ACCESS-RIGHT accessID="a11" type="added_content" privacy_concern="Harmless">
            <no_distribution/>
   </ACCESS-RIGHT>
   <ACCESS-RIGHT accessID="a21" type="tracking">
            <soft_tracking/>
   </ACCESS-RIGHT>
</ACCESS-RIGHTS>
</POLICY>
```

Figure 4.6: Example of UPP.

4.4 Privacy-enhanced Social Networking Site

Privacy is a fundamental right of each individual (*e.g.*, Article 12 of the Universal Declaration of Human Rights by the Assembly of United Nations, 1948) but is also a notion difficult to define and formalize, which can take different flavours depending on the context considered. *Privacy Enhancing Technologies* (PETs) are generally designed to respect two important principles:

- The *data minimization principle* states that only the information necessary to complete a particular application should be disclosed (and no more). This principle is a direct application of the legitimacy criteria defined by the European data protection directive (Article 7, [40]).
- The *data sovereignty principle* states that the data related to an individual belongs to him and that he should stay in control of how these data are used and for which purpose.

The fact that most of the current SNS does not respect the data minimization and the data sovereignty principles is not a fundamental impossibility result but rather a design choice made by the SNS providers. In the rest of this section, we will identify different privacy criteria that SNS can implement in order to increase the protection of the privacy of their users as well as propose our own definition of the Privacy-enhanced Social Networking Site (PSNS).

Thereafter, we propose a taxonomy (possibly non-exhaustive) of privacy criteria that can enhance the privacy of users if they are integrated within the design of a SNS. This taxonomy will help us to classify and compare the different privacy-enhanced SNS presented in Chapter 6.

The privacy criteria can be grouped into six generic categories: (1) *access control mechanisms*, (2) *friendly and flexible privacy settings*, (3) *transparency and awareness*, (4) *data sovereignty*, (5) *accountability* and (6) *reputation management*.

Access control mechanisms.

- *Customization of access control by groups of users and types of information.* A user generally possesses different circles of acquaintances ranging from close friends to family members and colleagues. If the SNS offers the user the possibility to group his friends by categories of users (for instance by level of trust), then this can be combined with a simple access control mechanism to restrict which type of information can be accessed by each group of users.
- *Customization of search.* If a user can specify to the SNS who can search his profile and which part of his personal information is relative to the search process and which is not, this will enhance the preservation of his privacy. For instance, a user might want to be totally invisible in the SNS for persons that do not belong to his list of friends, thus ensuring the property of "*unobservability*" (not being able to detect if a particular user is registered (or not) in the SNS).
- *Active blocking of information related to users.* Complementary to the customization of the search information related to his profile, a user should also have the possibility of removing tags of objects that point to his profile or hide his name on his friends' profile. For instance, the user may decide that some pictures are too

sensitive and erase the association between this picture and his profile. Otherwise, these pictures will appear when somebody searches for pictures associated to his identity.

Usability of privacy settings.

- Besides being flexible and expressive, the personalization of the privacy settings of the user should be done within an interface integrated in the SNS that is both user-friendly and easy to grasp for a typical user. In particular, filling the privacy settings should never become a barrier to the user because the interface is too complex.
- The privacy settings should be integrated into the main activity to facilitate the workflow (*i.e.*, putting the privacy settings next to each post). Treating access control management as a separate activity may distract the users from seeing the context of their main activities while managing the privacy settings [57].

Transparency and awareness.

- *Explicit privacy policy from the SNS and applications*. For the user to be aware of the privacy risks incurred by putting personal information on the SNS, a first step is for the SNS and its applications to state explicitly how they will use this information by expressing it as a privacy policy. This privacy policy should be easily comprehensible by the user, which means it should be expressed in terms that are easy to understand and not too complex.
- *Privacy lens*. The best way for a user to realize which information about him can leak is to see how his profile will appear in the eyes of other users, such as specific group of friends or even someone from outside the network. This feature is often called a privacy lens and some SNS are already providing it such as LinkedIn (“View My Public Profile as others see it") and Facebook (“View as” mode).

Data sovereignty.

- *Ownership and storage of the data.* It is important that the personal information shared by a user on a SNS remains his property. For instance, the SNS should not give this information to other entities or use it for advertising purpose without the user’s explicit consent (normally as stated in the privacy policy). In the extreme case where the user does not want to trust the SNS with his data, it is possible to imagine an architecture in which he could set up his own private server, which would be responsible for storing his data and managing the access control. In this situation, the SNS would only store the social graph related to the user (and not his personal data) and act as a gateway to connect individuals. Another possibility is to store encrypted data in the server of the SNS and to use an external channel to distribute to friends the keys necessary to decrypt personal data. However, these solutions seem to collide with the business model of most of current SNS and therefore there is a risk that their integration may be slowed down. Finally, instead of implementing the SNS in the form of a central authority, it is also possible to rely on a decentralized solution such as a peer-to-peer network. In this type of solution, the data is not stored only in one location but rather distributed among the nodes of a network, possibly using cryptographic techniques such as secret sharing schemes.

- *Right to oblivion*. A specific type of ownership is the right to oblivion, which states that there will be no data retention from the SNS if the user chooses to leave and that all his data will be erased. In particular, the SNS should not keep a back-up copy of the user account with the excuse that the user will potentially reactivate his account later.

Accountability.

- *Tracking how a user's information is disseminated*. In the digital world where it is possible to copy the information as often as desired, it is not easy to control how information is disseminated once it is out on the Internet. However, it is possible to imagine that by a combination of logs and techniques such as watermarking and traitor-tracing schemes, the dissemination of information can be (at least partially) controlled and that in case of a privacy breach, it is possible to identify those who have previously accessed this information.
- *Provenance*. Provenance refers to the origin, the history of the ownership or location of an object. For instance, it could be some metadata related to the provenance of the user photo that characterize its content and origin. This metadata could take

the form of an explicit privacy policy attached to the object or inserted in the form of a watermark (possibly invisible).

Reputation management:

- *Reputation system.* If the SNS relies on some kind of reputation mechanism, it becomes more difficult for a newcomer within the SNS to perform privacy breaches without his reputation being affected. Although actually almost no SNS integrates a reputation system, we believe that this feature could become an important asset to enhance privacy in future SNS.

Based on these privacy criteria, we define a *Privacy-enhanced Social Networking Site* (PSNS) as a SNS fulfilling the following properties:

- *Privacy awareness and customization.* A PSNS should make the user aware of some of the potential risks of sharing information with other SNS users. In addition, it also gives an easy and flexible way for to the user to express his privacy concerns in terms of a privacy policy and to compare it with the privacy policies of other actors such as the SNS provider, applications or other users.
- *Data minimization.* The user can check which part of his personal information is accessed by the SNS provider and third-party applications and how this information is used. In particular, the third-party applications should state clearly which personal information of the user they need and how they will process it. The user can then make an enlightened decision on whether or not to accept the third-party applications. The PSNS should also have an in-built mechanism to control the access to the information of the user and ensure that all SNS applications cannot access more data than authorized by the user.
- *Data sovereignty.* It should be stated explicitly in the privacy policy of the SNS that the personal data of the user belongs to him and not to the SNS that stores it. For instance, the SNS should not use the personal data of the user without its explicit consent and should not be able to sell it to other entities. Moreover, if the user decides to quit the SNS, the latter one should explicitly delete all the information stored regarding the user (and not even keep a copy for the uncertain case where the user might want to come back later). The user should also have

the possibility to track how his information is disseminated (for instance which friends have seen which pictures) but also to control information related to him that have been posted by other users (such as a tag on a picture pointing to his profile).

In this chapter, we describe the Privacy Framework for SNS and the concept of User Privacy Policy. Based on this Privacy Framework, we propose a taxonomy of privacy criteria that can enhance user privacy if they are integrated into the design of an SNS. We also introduce the concept of Privacy-enhanced SNS that takes into account these privacy criteria. In the next chapter, we will present Privacy Watch, our own theoretical proposal of a PSNS platform.

CHAPTER 5

PRIVACY WATCH

While SNS and privacy may seem *a priori* to have two opposite goals, we think that the fact that most of the current SNS do not respect the data minimization and the data sovereignty principles is a design choice made by the SNS providers. Therefore in this chapter, we describe Privacy Watch, our own proposed implementation for a Privacy-enhanced SNS [4]. With respect to the privacy criteria described in Section 4.4, Privacy Watch currently fulfils most of them except for a few as shown by the analysis at the end of this chapter.

Privacy Watch is based on the Privacy Framework for SNS detailed in Section 4.2. This framework provides users with an easy and flexible way to specify and communicate their privacy concerns to other users, third parties and SNS provider. In our system, the user can choose to which extent he trusts the SNS provider. More precisely based on his privacy level, the user will determine how much information he would like to share with the provider. For example, in the situation in which the user chooses *Full Privacy*, the SNS server is only trusted in storing an encrypted version of the personal information of the user. As a result, this piece of personal information can be consulted at any time by one of his friends but the SNS itself does not have access to this information (as the SNS server does not know the necessary decryption keys). As the purpose of Privacy Watch is precisely to protect the user privacy, the privacy level is set by default to *Full Privacy* (see Table 5.I).

Figure 5.1 presents an overview of the architecture of Privacy Watch. Privacy Watch is based on the hybrid architecture in which centralized server (the SNS server) is responsible for storing the personal information of the user (but possibly encrypted). Users of Privacy Watch install *Client Privacy Manager* (CPM) on their computer (for instance as a Firefox or Chrome extension) that has the responsibility of helping them to maintain the sovereignty on their personal information. Privacy Watch also relies on an auxiliary channel such as an independent mail server to store and exchange privacy policies and

Table 5.I: Default Privacy Settings in Privacy Watch.

	No Privacy	**Soft Privacy**	**Hard Privacy**	**Full Privacy (default)**
Default Privacy Setting	- Healthy	- Harmless	- Harmful	- Poisonous
Default Friend group	- Best Friends	- Normal Friends	- Acquaintance	- Visitor
Trust in SNS provider	- Best Friends - Do not encrypt data	- Normal Friends - Encrypt Poisonous data	- Acquaintance - Encrypt Harmful and Poisonous data	- Visitor - Encrypt all data
Access control	- Server side	- Server side	- Client side	- Client side

encryption keys among users. This is a form of protection of privacy by separating the information between two entities (the SNS server and the email provider). A fundamental security assumption is that these two entities are really independent and non-colluding [5].

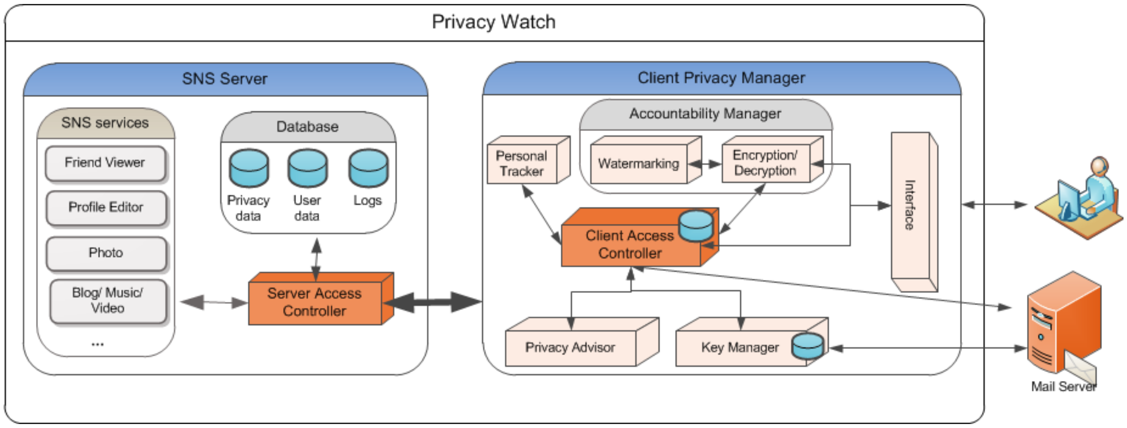


Figure 5.1: Architecture of Privacy Watch.

5.1 SNS Server

The SNS Server is composed of three modules: *Database*, *SNS Services* and *Server Access Controller*.

5.1.1 Database

This module stores the user data (encrypted or unencrypted) sent by the CPM, the privacy settings of the users (including UPP and other privacy preferences) as well as the logs of data access to the personal information.

5.1.2 SNS Services

This module takes care of all social services provided by the SNS such as Friends, Blog, Profile, RSS, Tagging, Photo or Music.

5.1.3 Server Access Controller

Going back to Figure 5.1, we can see that each access to user data has to pass through the Server Access Controller. The main purpose of the Server Access Controller is to verify the validity of an access before authorizing the retrieval of data.

Most of the current SNS offer users the option of specifying the privacy level of their profiles in one way or another. While MySpace only allow users to limit at a coarse level who can access their pages, Facebook lets users control who can search for them, how they can be contacted, as well as what information can be published on their profile and their friends' news feeds. An *access control scheme* is a mechanism that grants (or refuses) access to some object (such as data or resource) to an entity depending on the role and the credentials shown by this entity. While several types of access control mechanisms are possible, such as *identity-based*, *role-based*, and *rule-based* access control.

Most Web access today is performed using *identity-based* approaches [87] where access to all or some of the data is granted based on pre-existing agreements. For example, a user needs to provide correct login and password in order to enter a website.

Role-based access [44] is similar to identity-based access, except that instead of identifying a particular user, an access policy is created to allow users of a particular group to access various parts of the data. For instance, an administrator of a forum can classify the users in two groups: normal users and power users. The power users have access to the Movies and Music subforum while the normal users do not even see that these forums exist. The role-based and identity-based approaches are quite rigid and difficult to set up in a fine-grained way [102]. As a result, these approaches are not suitable for social networking activities with frequent content updates and volatile nature of friendship. *Rule-based* access control is more suitable for social networking activities as access policies are expressed as constraints on the type, depth and trust level of existing relationships [25]. This type of access scheme uses certificates to guarantee relationship authenticity and enforcement on the client-side follows a rule-based approach in which a subject requesting access to an object must demonstrate that he has the right to do so.

Our approach to the Access Controller is based on the modification of the rule-based approach. The system provides the user with four basic groups of Friends by default (see section 4.2.3). Based on these groups, the user can easily create or modify as many groups of Friends as they wanted by specifying their UPP. The Server Access Controller not only controls data access but also alerts a user whenever a violation of his UPP occurs. More precisely, each data request R composes of five parts: Request ID (ID), Requester ID (R_{ID}), Owner ID (O_{ID}), Request Data Type ($Type$) and Request Data ID ($Data_{ID}$): $R = (ID, R_{ID}, O_{ID}, Type, Data_{ID})$ The Access Controller searches for the UPP issued to the user or the application with the R_{ID} of the user who has O_{ID}. Afterwards the Access Controller checks if the requester has the right to access this data or not. If the answer is positive then the Access Controller retrieves the necessary data in the User Data database and sends it to the requester. If the requester does not have the corresponding access rights, the Privacy Controller informs the requester about the situation.

5.2 Client Privacy Manager

The Client Privacy Manager resides on the user side and is composed of the *Privacy Advisor*, the *Client Access Controller*, the *Key Manager*, the *Accountability Manager* and the *Personal Tracker* (see Figure 5.1).

5.2.1 Privacy Advisor

The proposed Privacy Framework in Chapter 4 is quite exhaustive and is able to cover most possible cases of privacy. However, normal users may have to spend a lot of time, especially at the beginning, to understand and to configure their privacy settings. The Privacy Advisor module recommends a privacy level that is adapted and tailored to users. The privacy level of a specific user is acquired through an elicitation process in the form of a question-response protocol between the Privacy Advisor and the user. The acquisition process should be both easy to understand (*i.e.*, expressed in natural language and non-legal terms) and flexible (*i.e.*, capture a whole range of privacy preferences). The Privacy Advisor also raises the awareness of users regarding the potential risks inherent to SNS and guides them during the creation of their UPP.

In order to determine the privacy level of a specific user, the Privacy Advisor takes into account three factors: *user purpose* for using SNS, *user background*, and *user privacy concerns*.

User purpose for using SNS

Ofcom[1] indicates that social networking users tend to fall into five distinct groups based on their behaviours and attitudes [76].

- *Alpha Socialisers* are people who used SNS to flirt, to meet new people, and to be entertained. They like to visit Friend lists and put a large quantity of comments on others' profile and photos. As a result, their network and number of Friends are quite large but most of them are only *Casual Friends*. Alpha Socialisers may also give out to Friends their contact details such as MSN address or telephone

[1] The Office of Communications (Ofcom) is a government-approved regulatory authority responsible for the broadcasting, telecommunications and postal industries of the United Kingdom (http://www.ofcom.org.uk/).

number so they can communicate easily outside the SNS. These actions can lead to disclosure of personal information and therefore *Security risks*.

- *Attention Seekers* are people who crave for attention and comments from other users. To get attention, they often post lots of pictures, primarily themselves and Friends in "suggestive poses, partying, drinking and portraying 'glamorous' lifestyles..." [76]. Their social network is quite extensible; nonetheless they tend to have active online connection with only a few Friends. Due to the large number of picture divulgation, the Attention Seekers are the most susceptible to *Reputation and Credibility* risks.
- *Followers* are persons who joined SNS to keep up with what their peers were doing. They often browse through Friends' albums, and only occasionally exchange comments and update their profile. Compared with Alpha Socialisers and Attention Seekers, users in this group are less likely to contact or meet people who they do not know. Consequently, most of their Friends are *Best Friends* and *Normal Friends*. In reality, these Followers on SNS have a moderate risk level of *Reputation and Credibility* risks as well as *Profiling* risks.
- *Faithfuls* are persons who typically used social networking sites to rekindle old friendships, often from school or university. They often leave their profile public so that old friends can find them easily on the SNS. For them SNS are useful tools to strengthen existing offline networks rather than to create new, virtual ones. Due to the profile being public, the Faithfuls are easy victims of *Profiling* and *Security* risks.
- *Functionals* are a minority of persons who tended to be single-minded in using SNS for a specific purpose, such as organizing parties, viewing photos or doing charity work. Ofcom [76] reported that most of them were pestered to join SNS by friends who are more involved . They are occasional users and generally log on for short visits. These users also suffer privacy risks because they do not spend time to learn about the possible privacy settings and leave their profile in the default state.

Users of each group have different notions of privacy and how they should behave on SNS. We created a questionnaire, denoted as $Q1$ in order to elicit the social group of a user (see Table 5.II).

Table 5.II: Questionaire Q1.

1. What is your main reason for joining the SNS?	2. When do you visit your page?
a. To entertain and have fun.	a. Every 5 minutes.
b. To introduce myself to the world.	b. When I have some new photos.
c. To connect with my real friends.	c. When my friends tell me.
d. To find my old friends.	d. Once in a while.
e. Other reason	

User background

User background is also an important factor in determining user privacy level. For instance, consider the age of a user: a user less than 12 years old is more likely to be targeted by online predators, whereas a 30-year-old should pay more attention to the shared information due to the risk of being victim of identity theft. Moreover, if the user is a student or an employee, he should pay attention to the policy of his school or company. If the user intends to apply for a job in a near future, he should remove all information that could damage his reputation and credibility in the eyes of recruiters, thus exercising his right to be forgotten.

We created another questionnaire, referred thereafter as *Q2*, to learn more about the user background than just the information available in his profile. Table 5.III displays some questions of Q2.

Table 5.III: Questionaire Q2.

1. How old are you?	2. What is your status?
a. Less than 15 years old.	a. Student in high school.
b. 16-30 years old.	b. Student in university.
c. 31-55 years old.	c. Employee.
d. Above 56 years old.	d. Retired.

User concern

Users can decide to protect themselves against *Security* risks, *Reputation and Credibility* risks, *Profiling* risks or all of them (see Section3.1). We created a questionnaire, denoted as *Q*3 in order to elicit user privacy concerns (see Table 5.IV).

Table 5.IV: Questionaire Q3.

1. Are you concerned that the SNS provider might divulge your information to other parties without your explicit consent? a. Not at all. b. Somewhat. c. Moderately. d. Quite a bit. e. Very much.	2. Are you concerned about online identity theft, cyberbullying or phishing? a. Not at all. b. Somewhat. c. Moderately. d. Quite a bit. e. Very much.

- *Security risks* include phishing, cyber bullying, online predator, and identity theft. In order to protect against Security risks, the user should not divulge their identity information or financial information on their profile or keep this information as Poisonous.
- *Reputation and Credibility risks*. User should set “inappropriate” pictures as Harmful or Poisonous and only allow a limited group of Friends to access this data.
- *Profiling risks*. User should limit the access to their profile to Friends and not let the Visitors access any information.

To summarize, the Privacy Advisor asks the user to answer three sets of questions in order to determine his privacy preferences (see Figure 5.2): User purpose (*Q1*), User background *(Q2*) and User concern (*Q3*). The process is decomposed in the following steps.

- **Step 1:** When the user has answered *Q1*, Privacy Advisor builds up a stereotype *P* of the user. There exists five main stereotypes: *Alpha Socialiser*, *Attention Seeker*, *Follower*, *Faithful* and *Functional*. Privacy Advisor then lists all the potential risks of the user’s activities and proposes the relevant Privacy level. Table 5.V summarizes these five stereotypes, their characteristics and the proposed Privacy level. It should be noted that we do not recommend users to apply Healthy as default Privacy Setting and No Privacy as default Privacy Level.

Table 5.V: Type of SNS users.

	Alpha Socialisers	**Attention Seekers**	**Followers**	**Faithfuls**	**Functionals**
Numbers of Friends	Many	Many	Medium	Medium	Several
Principal Profile Viewers	Casual Friends	Casual Friends	Normal Friends	Normal Friends	Casual Friends
Frequency of visits	Usually	Nearly always	Often	Less than often	Occasionally
Data	Lots of photos, comments, tags, activities	Lots of photos, comments, blog, tags, activities	Some photos, comments, activities	Some photos, comments, activities	Not applicable
Privacy Risks	Security Reputation and Credibility	Reputation and Credibility Securrity	Reputation and Credibility Profiling	Profiling	Profiling
Proposed Privacy Settings	Mostly Harmful	Mostly Harmful, Poisonous	Harmless	Harmless	Harmless
Proposed Privacy Level	Soft Privacy No Tracking	Soft Privacy No Tracking	Soft Privacy No Tracking	Soft Privacy No Tracking	Soft Privacy No Tracking

- **Step 2:** Once the user has answered *Q2*, Privacy Advisor adjusts the proposed privacy level to better protect him against unforseen privacy risks. For instance, if an *Attention Seeker* is under 18 years old, his privacy level should be changed to *Hard Privacy*. If the user skips Q2, Privacy Advisor still tries to get his demographic data from the User data database. During this step, Privacy Advisor also proposes four *Privacy settings* (Healthy, Harmless, Harmful, and Poisonous) to

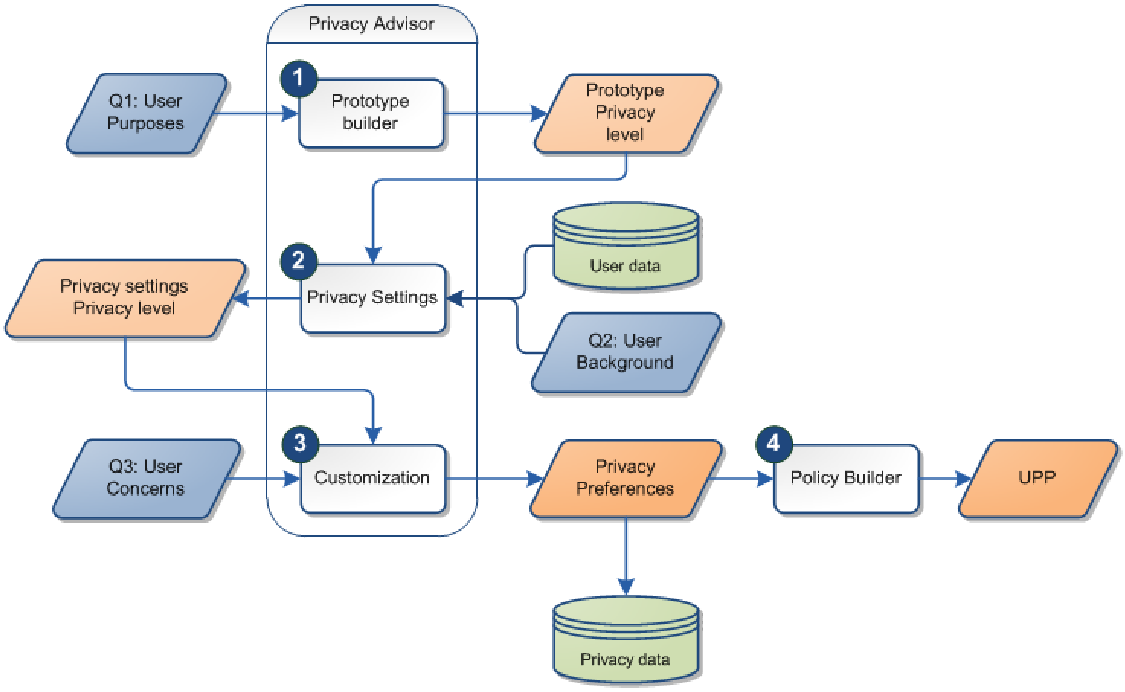
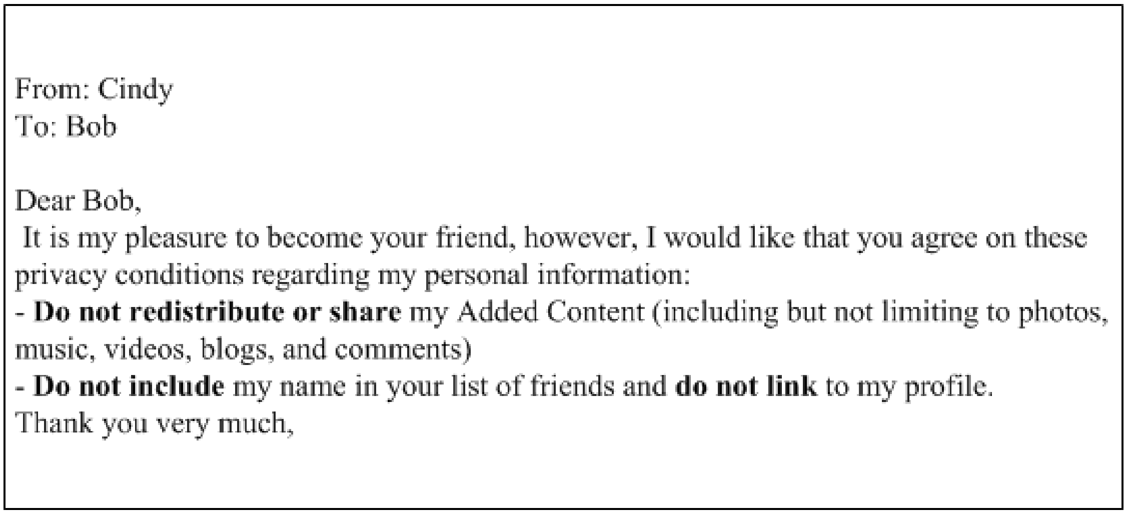


Figure 5.2: Privacy Advisor.

the user. For example, if the user works for a governmental organization, all blog entries criticizing his organization should be classified as Poisonous.

- **Step 3:** During this step, the Privacy Advisor lets the user adjust his privacy level (see Section 4.2.4) according to his privacy expectation. The Advisor also presents four basic *Groups of Trust* categories and gives the user the possibility to create more categories as well as provides him with guidelines on how to determine the access rights for each Group of Trust (see Section 4.2.3). The user's privacy preferences will be stored in the database.
- **Step 4:** The role of Policy Builder is to help SNS users build their own UPP (see Section 4.3) in a simple way. The Policy Builder relies on the information stored in the Privacy Preferences database to construct a XML-based privacy policy so that the user can restrict the access and uses of his personal information (see Figure 5.2). The users can read and/or modify the UPP in natural language or in XML format. Figure 5.3 described how the UPP in Figure 4.6 looks from the user's point of view. The Policy Builder also enables the user to create more Groups of

Trust, so that he can have more flexibility in defining his privacy settings.



From: Cindy
To: Bob

Dear Bob,
It is my pleasure to become your friend, however, I would like that you agree on these privacy conditions regarding my personal information:
- **Do not redistribute or share** my Added Content (including but not limiting to photos, music, videos, blogs, and comments)
- **Do not include** my name in your list of friends and **do not link** to my profile.
Thank you very much,

Figure 5.3: Alice's UPP for Bob

After using the Privacy Advisor, the user will be more aware of privacy risks behind his social networking activities and understands how to customize his privacy settings in SNS. Thus, Privacy Advisor helps raising the privacy awareness among SNS users.

5.2.2 Client Access Controller

This module monitors the access to and the dissemination of the user's personal information from the client side. When a user does not fully trust the SNS (which corresponds to *Full Privacy* and *Hard Privacy*), this module will assume the role of the Server Access Controller.

5.2.3 Key Manager

The Key Manager module is responsible for creating the keys used for *encryption and decryption*, managing user public/ privacy key, as well as the group signature used for access control on the SNS server.

In a nutshell, *group signature scheme* is a form of *anonymous credentials* that allows multiple-show unlinkability. More precisely, it allows an entity to prove (possibly several times) its right of access to some data without having to disclose its identity (instead it will only reveal the group to which it belongs). Group signature schemes were originally introduced by Chaum and van Heyst to provide anonymity to the signatory of a message [27]. In a group signature scheme, there is a single public verification key for the group, but each member of the group receives a different private signing key from the group manager (which in our case will be one of the users of the SNS). More precisely, group signature scheme (with optional anonymity removing) consists of the four following operations:

- *Registration of the user.* During the registration operation, the user assigns to one of his friends, a new private signature key, denoted by $\sigma_{G,U}$.
- *Signature of a message on behalf of the group.* This operation takes as input a message m and signing key $\sigma_{G,U}$ and produces a signature $\sigma_{G,U}(m)$ on this message.
- *Verification of a group signature.* This operation checks the validity of a group signature. It requires as input a verification key for the group, V_{KG}, which has been setup by the user and is publicly known, as well as a message m and a group signature on this message $\sigma_{G,U}(m)$. This operation produces as output either accept or reject depending on the validity of the signature.
- *Anonymity removal.* From the point of view of the SNS provider, it is impossible to distinguish if two group signatures come from the same individual or not due to the unlinkability property. However in exceptional situations, the user can (in association with the SNS provider) retrieve the identity of a particular signatory via the anonymity removing operation. This operation takes as input a message m and a group signature on this message $\sigma_{G,U}(m)$ and produces as output the identity of the signer U. In practice, this is done by first identifying the private signature key $\sigma_{G,U}$ from the signature and then retrieving the identity associated with this key.

In Privacy Watch, we use the Groups of Trust as the basic groups. The users can add and modify these Groups of Trust as necessary.

5.2.4 Accountability Manager

In order to enhance the privacy of the owner (and co-owners) of a piece of personal information (textual, visual, sound or structured data), we propose to attach to this information some *metadata* related to its *provenance* as well as an explicit *UPP* stating how this data can be used, processed and disseminated. The exact meaning of provenance depends on the context where it is applied and the goal it is expected to achieve. For instance, provenance represents the seven W's (Who, What, Where, Why, When, Which, (W)how) and could be used to assert ownership and attach an identity to an object [49]. Within the Accountability Manager, the metadata related to provenance contains the following information:

- *Content of the data:* The data type can be for instance text, picture, video, sound file or blog and other information can be attached such as textual description of the content or other related information.
- *Source:* The copyright holder (owner) of the data or the URL of the web page the data came from. If this piece of data is related to several individuals, there should be tags pointing to these individuals (if they are also users of the SNS).
- *Creation date:* The time when this data was created.
- *Location (if applicable):* The place where this data was created. This information may not be available or may not make sense for all types of data. For instance, while it is perfectly appropriate for a picture, it does not really apply to textual information such as profession or phone number.
- *Author:* The author of the data (*i.e.*, its creator) may be different from the copyright holder. For example, in the case of a medical record, the author of this data might be the doctor himself or even the hospital but the data should belong to the patient.
- *Privacy policy:* This metadata specifies which user and which privacy policy governs the rights attached to this piece of personal information.
- *Timestamp:* This metadata corresponds to the time when this provenance data was created. The timestamp may be different from the date of creation of the data (*e.g.*, a picture that has been shot 10 years before the provenance data is attached to this

picture).

- *Identities of receiver(s):* This metadata clearly states the identities of the individuals that have accessed and downloaded this piece of information.

In our architecture, this provenance data is either clearly attached to the personal information associated with it and/or inserted in the form of a watermark (explicit or hidden) if the data type lends itself to such action (for instance if the data is a picture or a video file).

5.2.4.1 Encryption/decryption module

This module is in charge of encrypting and decrypting the data of users when necessary. In Privacy Watch, we choose to use a *Symmetric Encryption scheme*, and in particular the *AES encryption algorithm*[2]. Symmetric Encryption is a type of encryption in which the same secret key is used to encrypt and decrypt information or there is a simple transform between the two keys. Symmetric-key algorithms can be further divided into *Stream algorithms* (Stream ciphers) and *Block algorithms* (Block ciphers). Stream algorithms encrypt the bits of information one at a time - operate on 1 bit (or sometimes 1 byte) of data at a time (in an online manner). Block cipher (method for encrypting data in blocks) is a symmetric cipher encrypting information by breaking it down into blocks before encrypting each block. A block cipher encrypts data in fixed sized blocks (commonly of 64 bits). AES is a symmetric key encryption technique that has replaced the commonly used Data Encryption Standard (DES). AES provides strong encryption and has been selected by the National Institute of Standards and Technology (NIST) as a Federal Information Processing Standard in November 2001 (FIPS-197) [75].

5.2.4.2 Watermarking module

This module manages the watermarking process such as the embedding of provenance data into personal information or the decryption of a particular watermark from

[2] Advanced Encryption Standard.

a modified data. If the UPP is combined with the Privacy Controller, they can prevent partially unauthorized access to user data. Indeed, a particular entity knows exactly what he can get from the user profile and how he can use it. However, when he has already downloaded the information, there is no way to ensure that he will comply with all the clauses stated in the UPP. Therefore we need a mechanism that can insert ownership information into the digital object. Whenever the ownership of a digital object is in question, this information can be extracted to identify the rightful owner.

On a digital picture, a watermark can be as simple as a faint logo or string of words superimposed over that picture. The main goal of placing watermark on pictures is to prevent others from copying or using the picture without permission. For instance, many websites put watermarks on pictures to indicate that a particular image is copyrighted, and that it may not be copied or used elsewhere without the permission of the website from which it originates.

Most programs for editing pictures and photo sharing websites provide watermark functions, from simple to more sophisticated ones, such as *Adobe Photoshop*, *Visual Watermark*, *Watermark Studio*, *uMark*, *PicMarkr*[3] and *WaterMark*[4] [103]. However, a *visual watermark* has the effect of significantly decreasing the quality of a picture and can be easily removed by using cropping or retouching tools. In contrast, *digital watermarking* embeds information directly into the digital material in such a way that it is imperceptible to a human observer but can easily be detected by a computer algorithm [84]. A *digital watermark* is a transparent and invisible pattern that is inserted into an appropriate component of some data by using a dedicated encoding algorithm [74]. One of the main advantages of this type of technique is that the medium itself is not compromised in anyway (*i.e.*, at first glance it appears the same as the original data). Moreover, watermarks do not get removed when the digital media is displayed or converted to other file formats. These watermarks also undergo the same transformations as the digital media in which they are embedded. Digital watermarking can be used in conjunction with

[3] `http://picmarkr.com`

[4] `http://watermark.ws`

services tracking the use of images across the web, such as *LicenseStream*[5], *PicScout*[6] and *ImageRights*[7] [103].

In a nutshell, a watermarking scheme generally comes with two operations: an *encoding* and a *decoding* operation. The encoding operation takes as input the original data (such as an image or video), generates a watermark that is embedded inside the medium and produces as output a modified version of this data integrating the watermarking. On the other hand, the decoding operation takes as input a candidate image possibly containing a watermark and returns either the watermark embedded inside the image or void if none was found. Watermarking systems can be classified according to several criteria. For instance with respect to *workspace domains*, it is possible to differentiate between three techniques: *spatial transform*, *discrete cosine transform* and *wavelets* [48]. In *spatial transform*, the watermark encoding takes place in the spatial domain, whereas the *discrete cosine transform* breaks up the image into different frequency bands, making it easier to encode watermarking information into the middle frequency bands of an image. Finally *wavelets* technique, the watermark encoding is done in the wavelet transform domain, which provides multi-resolution representation of the cover work.

According to the *type of detection*, watermarking systems can be divided into *blind* and *non-blind* schemes. *Non-blind techniques* use the original source in conjunction with modified data to extract the watermark by simple comparison and correlation procedures. Even though *blind techniques* are more insecure than non-blind methods, they have the main advantage of not requiring the original images to be able to detect the embedded watermark [84]. Moreover, blind techniques working with a spatial transform also have the shortest processing time in comparison to discrete cosine transform and wavelet techniques [90]. Within the context of Privacy Watch, we have mainly focused on using blind watermarking techniques.

[5] `http://licensestream.com`
[6] `http://picscout.com`
[7] `http://imagerights.com`

5.2.5 Personal Tracker

This module helps users to track how their own data is disseminated, both inside the SNS and even outside (*i.e.*, on the World Wide Web) by raising privacy awareness of users through different *data aggregators*.

Data aggregators are *people-search* tools that look into nearly every corner of the web to provide and gather information. These websites aggregate data from many online (SNS, blogs, newspapers, online photos...) and offline sources (phone directories, birth records, marriage records...) and are ready to sell these types of information to anyone willing to pay for it. For instance, *123people*[8] searches for people related information that is publicly available on the Internet. The search results are presented in a structured way for optimal usability and encompass results from traditional search engines, as well as pictures, videos, email addresses and phone numbers. In addition, they also contain social network profiles, blog entries, relevant documents, instant messenger IDs, news and Amazon results. *PeekYou*[9] is a database of public web links belonging to over 250 million people. Its primary goal is to create a single public profile for every person, summarizing his or her interests, work, schooling history, photos, physical address, e-mail address, websites, gender, age, and other biographical information. To date, over one billion links have been indexed. PeekYou provides a people search engine in which users can freely access this information, whether it relates to themselves or to other people. The site represents an opportunity for web users to control how their personal information appears across the web.

Visual search engines can also be considered as a form of data aggregators. However, pictures are much more difficult to search than textual data, and therefore visual search engines rely mostly on available tags and the text surrounding the picture [103]. However, using state of the art algorithms from Computer Vision, it is fairly easy for a computer to analyze the visual features of a picture in order to extract a fingerprint from it. On the other hand, it is very difficult to automatically attach a semantic to this picture. By using its fingerprint, it becomes possible to efficiently compare a particular picture to

[8] `http://123people.com`

[9] `http://peekyou.com`

the fingerprints of millions of other images in order to discover identical or very similar images. For instance, *TinEye* [10] can find exact matches of the image it was searching for. It can also find out the origin of an image, how it is being used, if modified variants of the picture exist, or if a higher resolution version is available. However, the efficiency of TinEye is limited and directly proportional to the number of pictures it has indexed (2.1 billion so far [11]). *Gazopa* [12] works in a similar manner to TinEye and has gathered a database of more than 80 million pictures. Using this system, users can search images based on the user's own photo, drawings, images found on the web and keywords. Moreover, Gazopa enables users to search for a similar image by using a comparison method relying on visual features such as a color or a shape. *Google Similar Images* also allows the users to search for images using as inputs pictures rather than words, by providing an option to click on the "Similar images" link under an image. However, the results do not seem as reliable as TinEye [81].

5.3 Mail Server

This module is a third party email server such as Hotmail and Gmail that is assumed to be independent from the SNS. It is used to store and exchange keys (for instance encryption/decryption keys) as well as UPP between users (in case where the user does not trust the SNS for doing so). We choose email as our key exchange channel because it is an open and federated platform that lets users choose their providers or hosting their own.

5.4 Scenario

When Bob registers to the SNS, he downloads and installs his *Client Privacy Manager* (CPM) as a browser plug-in. Based on the recommendation of the *Privacy Advisor*, Bob chooses his level of *privacy* among Full, Hard, Soft or No Privacy and specifies his *UPP*. For example, as Bob is "privacy-addicted", he chooses *Full Privacy*.

[10] http://tineye.com

[11] http://www.tineye.com/updates

[12] http://gazopa.com

The *Key Manager* in the CPM creates an account for Bob on the *Mail Server* that will be used for *key sharing*. The Key Manager then creates different keys (K_{PS}) for encrypting many attributes of his profile as well as the public key of group signature key (SK_G) for each *Group of Trust*.

When Bob uploads the photo *pict* on his online album in the SNS, the Privacy Advisor proposes to Bob a suitable UPP for this data according to his privacy preferences. The photo *pict* and the associated UPP are sent to the *Client Access Controller*. The Client Access Controller then asks the *Watermarking* module to verify whether there is any evidence that the photo *pict* might belong to another user. If the answer is negative, the module embeds into the picture as an invisible watermark the public signature key of Bob PK_{Bob}, the description of the UPP P as well as the signature of Bob on this metadata $\sigma_{Bob}(P)$. Therefore, the photo *pict* becomes $W(pict, PK_{Bob}, P, \sigma_{Bob}(P))$. The *Encryption* module then encrypts *pict* with the secret key K_{PS}. The encrypted photo $E_{K_{PS}}(W(pict, PK_{Bob}, P, \sigma_{Bob}(P)))$ are stored inside the *User data* database (see Figure 5.4).

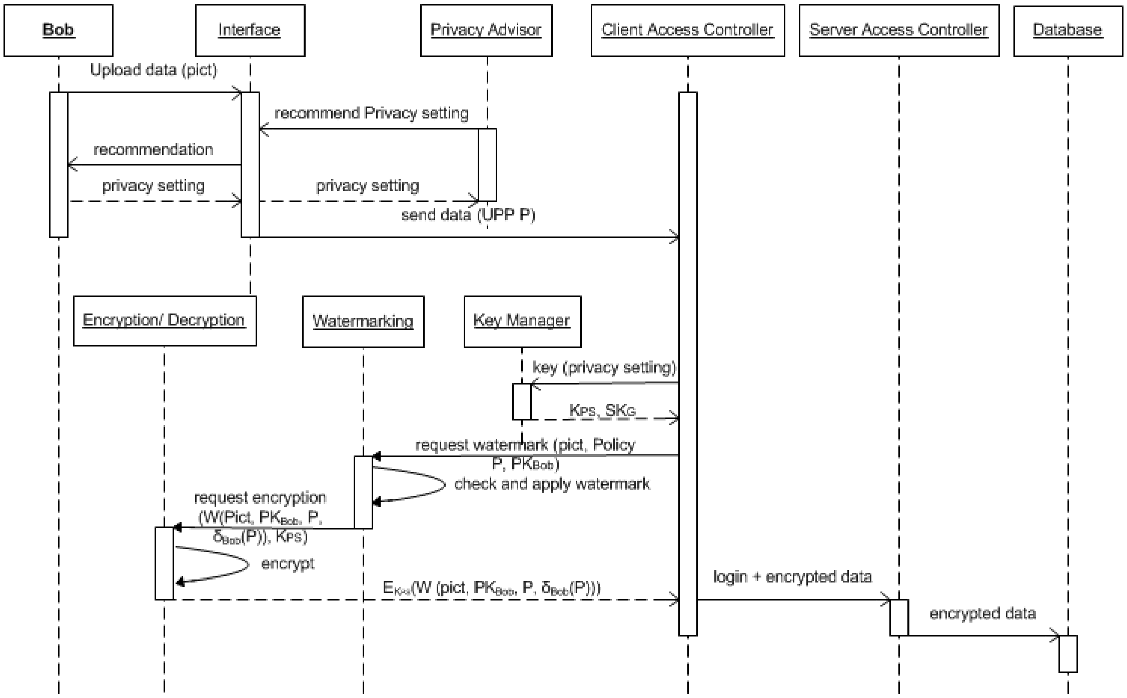
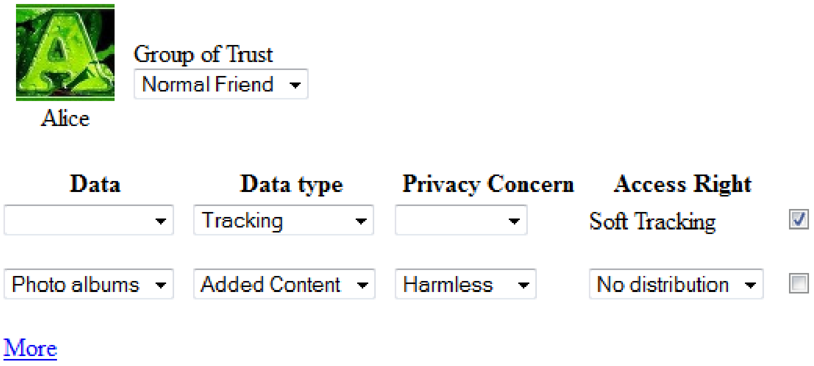


Figure 5.4: Watermarking and Encryption process.

Bob can now use the SNS to connect with friends and choose to befriend Alice. The Privacy Advisor proposes to Bob four possible *Groups of Trust* (Best friend, Normal friend, Casual friend, Visitor). For example, Bob chooses to classify Alice as Normal friend (see Figure 5.5). The Client Access Controller in Privacy Watch knows the UPP that Bob has specified for this particular friend group and emails this UPP to Alice. In order to befriend Bob, Alice has to accept this UPP and then her Access Controller now stores Bob's UPP. Bob's Key Manager connects to the independent Mail Server in order to send an email to Alice with her private signature key $SK_{NormalFriends}$ as well as all K_{PS} of the attributes that she is allowed to see as a normal friend of Bob.



Alice

Group of Trust: Normal Friend

Data	Data type	Privacy Concern	Access Right	
	Tracking		Soft Tracking	☑
Photo albums	Added Content	Harmless	No distribution	□

More

Figure 5.5: Privacy Advisor

When Alice wants to see the photo *pict*, her Client Access Controller retrieves the group key $SK_{NormalFriends}$ from the Key Manager, then sends a request to see the picture to the Server Access Controller. The Server Access Controller then sends a random challenge to Alice, which she has to sign with her private signature key $SK_{NormalFriends}$ to prove her right to access this data. The Server Access Controller then sends the UPP of the picture *pict* to Alice and requires her to accept it. Alice's Client Access Controller then returns the UPP signed by Alice to the Server Access Controller. After that, the Server Access Controller saves the UPP together with Alice's signature and the current timestamp and returns the encrypted photo $E_{K_{PS}}(W(pict, PK_{Bob}, P, \sigma_{Bob}(P)))$ to Alice. Using the symmetric key K_{PS}, the Decryption module can now decrypt the photo and returns $W(pict, PK_{Bob}, P, \sigma_{Bob}(P))$ to Alice who can now visualize the picture (see

Figure 5.6).

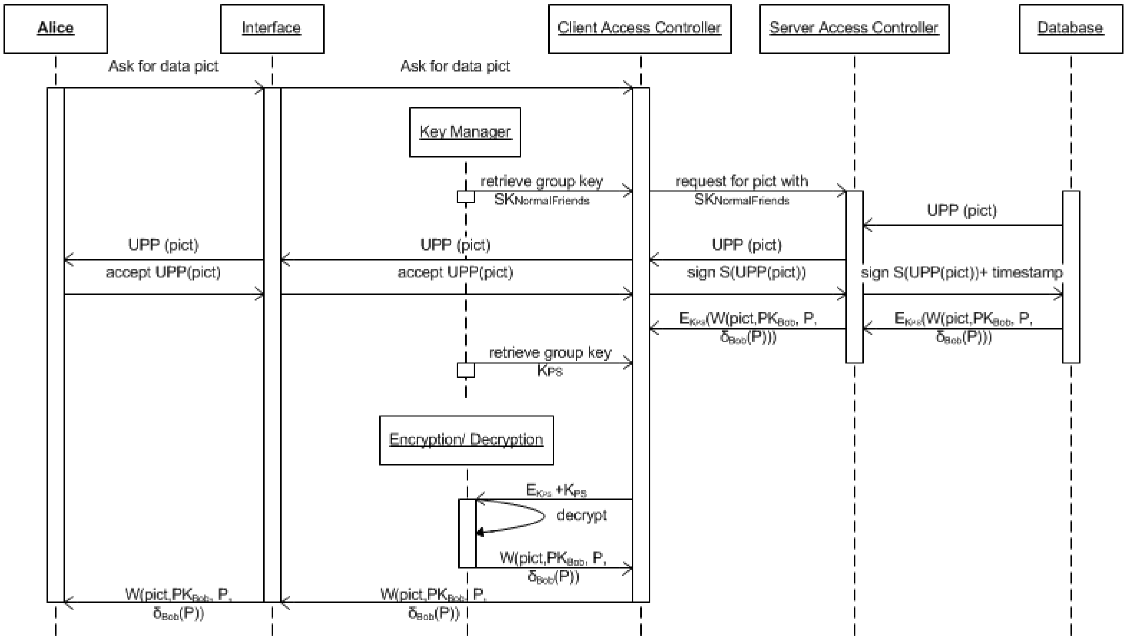

Alice
Interface
Client Access Controller
Server Access Controller
Database
Ask for data pict
Ask for data pict
Key Manager
retrieve group key $SK_{NormalFriends}$
request for pict with $SK_{NormalFriends}$
UPP (pict)
UPP (pict)
UPP (pict)
UPP (pict)
accept UPP(pict)
accept UPP(pict)
sign S(UPP(pict))
sign S(UPP(pict))+ timestamp
$E_{K_{PS}}$(W(pict,PK_{Bob}, P, δ_{Bob}(P)))
$E_{K_{PS}}$(W(pict,PK_{Bob}, P, δ_{Bob}(P)))
retrieve group key K_{PS}
Encryption/ Decryption
$E_{K_{PS}}$ +K_{PS}
decrypt
W(pict,PK_{Bob}, P, δ_{Bob}(P))
W(pict,PK_{Bob}, P, δ_{Bob}(P))
W(pict,PK_{Bob}, P, δ_{Bob}(P))

Figure 5.6: Information flow of Decryption process.

5.5 Implementation

In order to provide users with an access control tool we have developed a prototype implementation that partially integrates the tools and functionalities described previously in this chapter. The prototype was implemented with the help of two other Master students, Odilon Allognon and David Schönfeld.

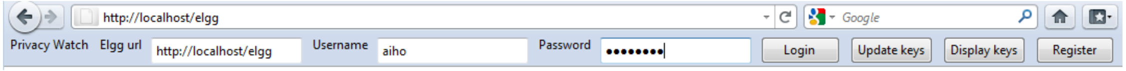
5.5.1 Implementation Details

An SNS was created using the Elgg [13] open-source social networking platform. In a nutshell, Elgg provides the necessary functionality for an SNS including advanced user management and administration, cross-site tagging, powerful access control lists and internationalization support. The prototype was developed as a Firefox [14] extension

[13] http://www.elgg.org/

[14] http://www.mozilla.org/en-US/firefox/

(see Figure 5.7) allowing client-side access control enforcement across independent platforms. We choose Firefox because it is one of the most popular web browser and works across multiple platforms.



http://localhost/elgg

Privacy Watch Elgg url http://localhost/elgg Username aiho Password ••••••••

Figure 5.7: Firefox Extension of Privacy Watch.

The Firefox extension development is done by using the following languages:

- *XUL* [15] for the user interface
- *JavaScript* for event management
- *XPCom* [16] for the object libraries
- *Python* for connection to email server, key management and encryption

The encryption was done using pyCrypto [17], a Python library. The algorithm chosen is AES encryption in OFB [18] mode. An overview of the prototype is detailed in Figure 5.8.

5.5.2 Functionalities

Within the prototype of Privacy Watch, users can exercise the control over their data and protect their data from the SNS. In particular, only members of users' groups of trust can be allowed to have access to a target content. In order to use the prototype, the user first registers with the SNS then manually creates an email address on Gmail server (see Figure 5.9). The Connection module then automatically retrieve all keys stored in the email server and transfers it to the Key Manager.

The Key Manager module store all user encryption keys as well as the keys of his friends inside an encrypted XML database. The prototype is still under development and many functionalities are not implemented yet, such as the Watermarking and Personal Tracker module. Currently four principal functionalities that have been developed are:

[15] XML User Interface Language.
[16] Cross Platform Component Object Model.
[17] `http://pypi.python.org/pypi/pycrypto`
[18] Output feedback.

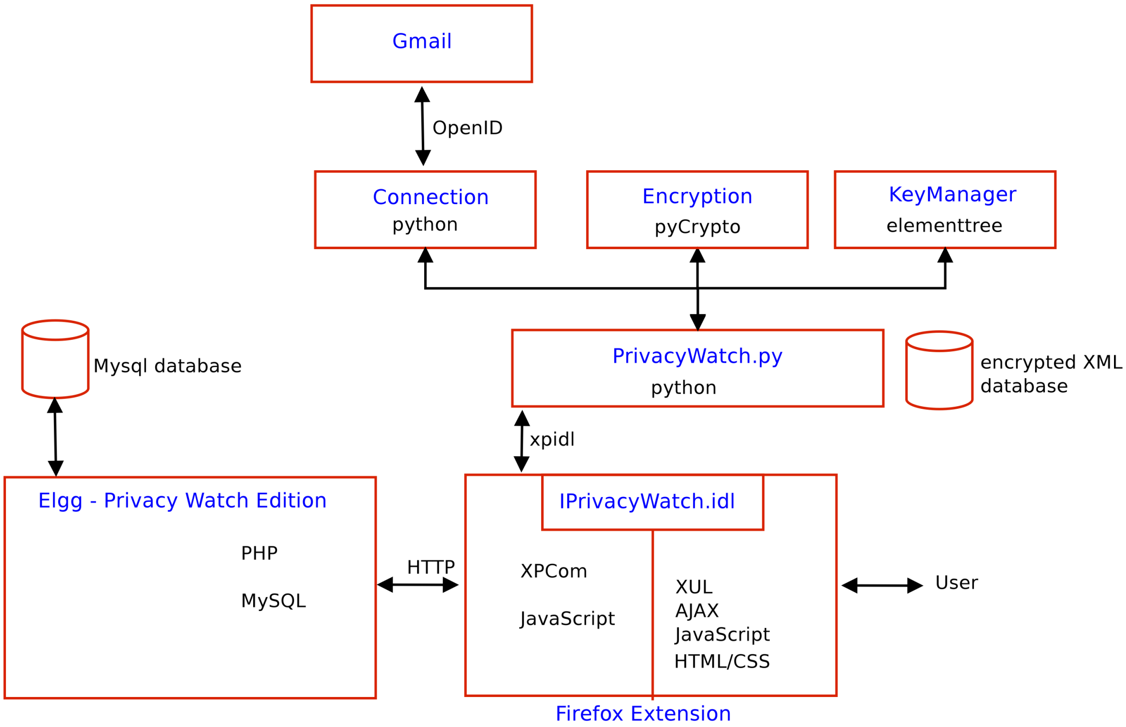
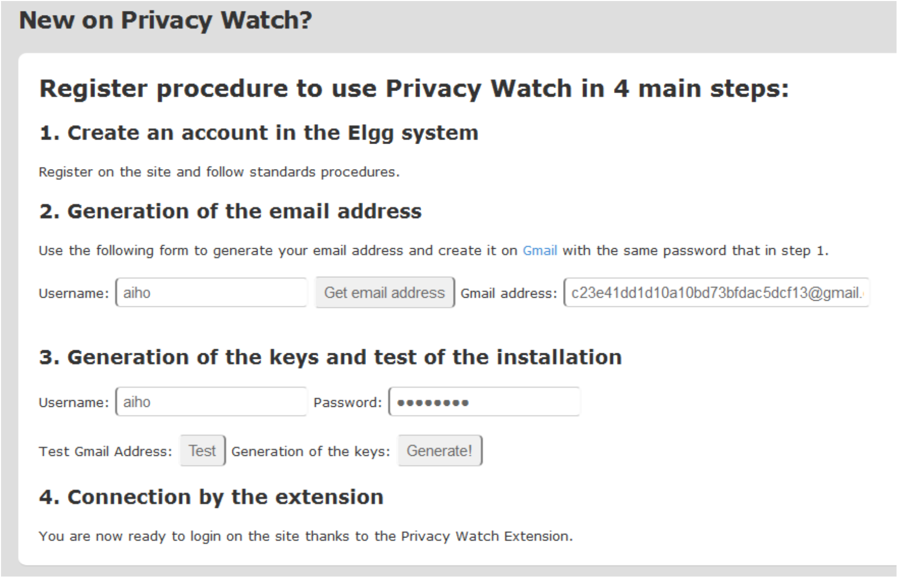


Figure 5.8: Implementation of Privacy Watch.



New on Privacy Watch?

Register procedure to use Privacy Watch in 4 main steps:

1. Create an account in the Elgg system

Register on the site and follow standards procedures.

2. Generation of the email address

Use the following form to generate your email address and create it on Gmail with the same password that in step 1.

Username: aiho Gmail address: c23e41dd1d10a10bd73bfdac5dcf13@gmail.

3. Generation of the keys and test of the installation

Username: aiho Password: ••••••••

Test Gmail Address: Generation of the keys:

4. Connection by the extension

You are now ready to login on the site thanks to the Privacy Watch Extension.

Figure 5.9: New User Registration.

1. Connection to SNS server and email server.

2. Key management and encrypted XML key database via email server.
3. Seamless decryption on friends' profile if the user has appropriate keys.
4. Encryption of data based on privacy levels.

5.6 Analysis of Privacy Watch

The main objective of Privacy Watch is to provide an individual the possibilities to review and partially control how his personal information flows both inside and outside the SNS (through the use of data aggregators and visual search engines). With respect to the privacy criteria that we define in Chapter 4, Privacy Watch currently fulfils most of them. Specifically, the *access control mechanism* of Privacy Watch allows users to specify their privacy settings in the form of User Privacy Policy for each friend, each Group of Trust, each piece of data or even each type of data (*e.g.* different UPPs for Harmful data and Harmless data). Furthermore, using the UPP with a specific Tracking level, the user can make himself "invisible" to the search process of SNS as well as disables tags pointing to his profile.

It is not easy to set up multiple UPP and to decide the appropriate privacy settings. Fortunately, the Privacy Advisor comes to the rescue with personalized recommendation of privacy settings. This module also helps the user better understand the potential risks inherent to the SNS. Thus, it ensures that all choices of privacy settings are *user-friendly* and easy to grasp for a typical user.

To increase the usability of the system, we choose mail server as the key distribution channel as it is a mature, scalable, open and federated infrastructure supporting over 1 billion users [45]. The key database is also stored as email messages so that users can access to it from anywhere that has an Internet connection. At first sight, this solution may seem vulnerable to attacks. However, as the email created by the Key Manager is used only for key distribution, it is not much exposed to spamming and outward attacks such as viruses, malware, and other forms of malicious threats. Furthermore, because this email address is a random pseudonym (*e.g.* c23e78ss1dd0078adcdu836@gmail.com instead of aithanhho@gmail.com), it is not easy to guess and less likely to become victim of spamming and phishing attacks.

Regarding the criteria of *Transparency and awareness*, as Privacy Watch is only an SNS platform, the requirement of *explicit privacy policy from the SNS and applications* is not applicable. Nevertheless, because the users have the choice to trust the SNS with their unencrypted personal data, Privacy Watch may encourage the SNS provider to provide users with greater access to easy-to-understand and transparent policy information. Additionally, the Privacy Advisor also allow realize which information about him can leak is to see how his profile will appear in the eyes of other users.

With respect to *data sovereignty*, Privacy Watch allows users to store encrypted data on SNS server and decryption keys on a independent mail server. As a result, personal information shared by a user on a SNS always remains his property. Moreover, the Accountability Manager (see Section 5.2.4) can help users detect and trace the origin of a privacy breach once it has occurred. Thus, the users of Privacy Watch are able to claim back their privacy by asking the responsible person to erase this data or by providing evidences to a third party such as the SNS provider or a judge.

Last but not least, as Privacy Watch is built as a generic PSNS platform, existing SNS can be modified to follow the architecture of Privacy Watch, albeit with significant code modification. As the SNS Server component of Privacy Watch is designed based on Elgg, an open source SNS platform, it is not too different from the architecture of existing SNS. While the Server Access Controller and the Privacy database have to be completely redesigned, the SNS services and User database stay the same. However, this choice is entirely depended on SNS providers as they have to allow users to store encrypted data and/or fictional personal information, which may violate their own Terms of use.

In this chapter we introduced the architecture of Privacy Watch, our own PSNS platform. Moreover, we illustrated our system with a functional scenario. However, there is still work to be done such as the reputation manager and the report spam/abuse mechanism. The comparison between Privacy Watch and other privacy-enhanced solutions will be presented in the next chapter.

CHAPTER 6

COMPARATIVE STUDY OF PRIVACY-ENHANCED SOCIAL NETWORKING SITES

In this chapter, we give an overview of solutions that have been proposed to enhance the privacy of users of SNS [6]. These solutions can be divided mainly in three categories: *centralized SNS*, *privacy add-ons* and *distributed SNS*. We also compare these solutions according to the privacy criteria identified in Section 4.4.

6.1 Centralized SNS

Most of the current SNS, such as Facebook, LinkedIn or Google+, are centralized SNS in which the data of the users is under the control of a central entity that stores it on its servers.

6.1.1 Facebook

Facebook[1] is a SNS that was originally launched in February 2004. Since its beginning, Facebook has undergone a remarkable transformation. When it started, it was a private space for communication with a chosen group. Soon, it transformed into a platform in which almost all the user information is public by default. Today, it has become a platform where users have no choice but to make certain information public such as name, profile pictures, network and comments on a Page's wall, and this public information may be shared by Facebook with its partner websites and used to target ads. Luckily, Facebook provides some powerful options to protect users online but it is up to the users to proactively use them. For instance, Facebook includes the following privacy features:

- *Sharing.* The user can use the inline audience selector to control who can see the content he post on a day-to-day basis (such as status updates, photos and videos).

[1] http://www.facebook.com/

It also includes the possibility to tailor the personal information that a user shares about himself (*e.g.*, birthday and contact information) and even content that others share about him (*e.g.*, comments on his posts and photos). Facebook provides a standard vocabulary of policies (*i.e.*, no-one, only-me, friends, friends-of-friends, everyone) from which resource owners may choose from.

- *Tag review.* The user will get a notification every time he is tagged before the tags appear, therefore we can approve or ignore the tag request by going to see the content itself.
- *Apps and website.* The user can control which information about him is shared with websites and apps, including search engines. The user can view his apps, remove any he does not want to use, or turn off the platform completely.

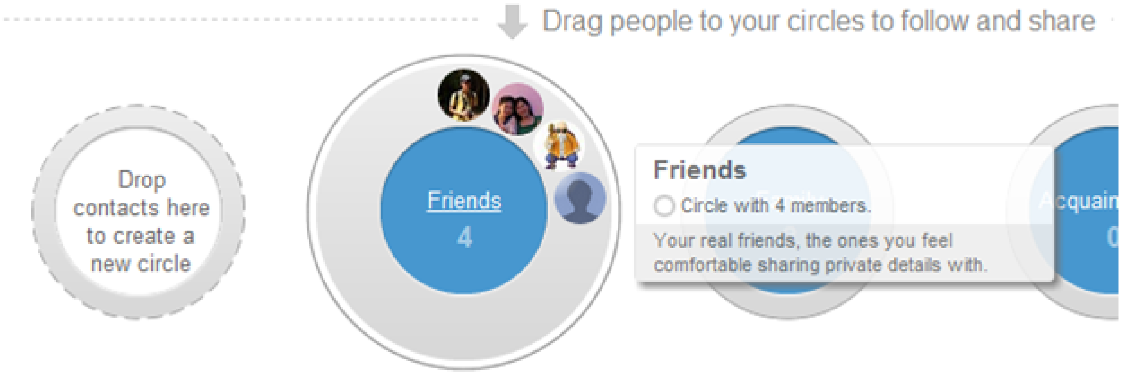
6.1.2 Google+

Google+ [2] is a SNS operated by Google that opened to the public in September 2011. Google+ is built as a layer that not only integrates different Google social services, such as Google Profiles and Google Buzz, but also introduces many new features including *Circles*, *Hangouts*, *Sparks* and *Huddles*. For instance, Google+ includes the following features:

- *Circles* enables users to organize contacts into different groups (Figure 6.1) for sharing across various Google products and services such as Google Documents and Google Calendar. Although other users can view a list of contacts, they cannot view the circle to which they belong unless the user has explicitly chosen to make it visible. The privacy settings also allows users to hide the users in their circles as well as who has them in their circle. Organization is done through a drag-and-drop interface that is quite intuitive. This system replaces the typical friends list function used by SNS such as Facebook.
- *Huddle* is a feature available on Android, iPhone, and SMS devices that allows communication within circles through instant messaging.

[2] `http://plus.google.com`

- *Hangouts* are places used to facilitate group video chat (with a maximum of 10 people participating in a single Hangout at a particular moment in time). However, anyone on the web could potentially join the Hangout provided they possess the unique URL of the Hangout.
- *Instant Upload* is a functionality specific to Android mobile devices, which stores pictures or videos in a private album such that they can be shared later with other users.
- *Sparks* is a front-end to Google Search, enabling user to identify topics they might be interested in sharing with others. In this manner, "featured interests" sparks are also available based on the topics that others globally find interesting.
- *Streams* allow users to see updates from those in their circles, which are similar in spirit to Facebook's news feed. The input box of a stream allows users to enter a status update or use icons to upload and share photo and videos.



Drag people to your circles to follow and share

Drop contacts here to create a new circle

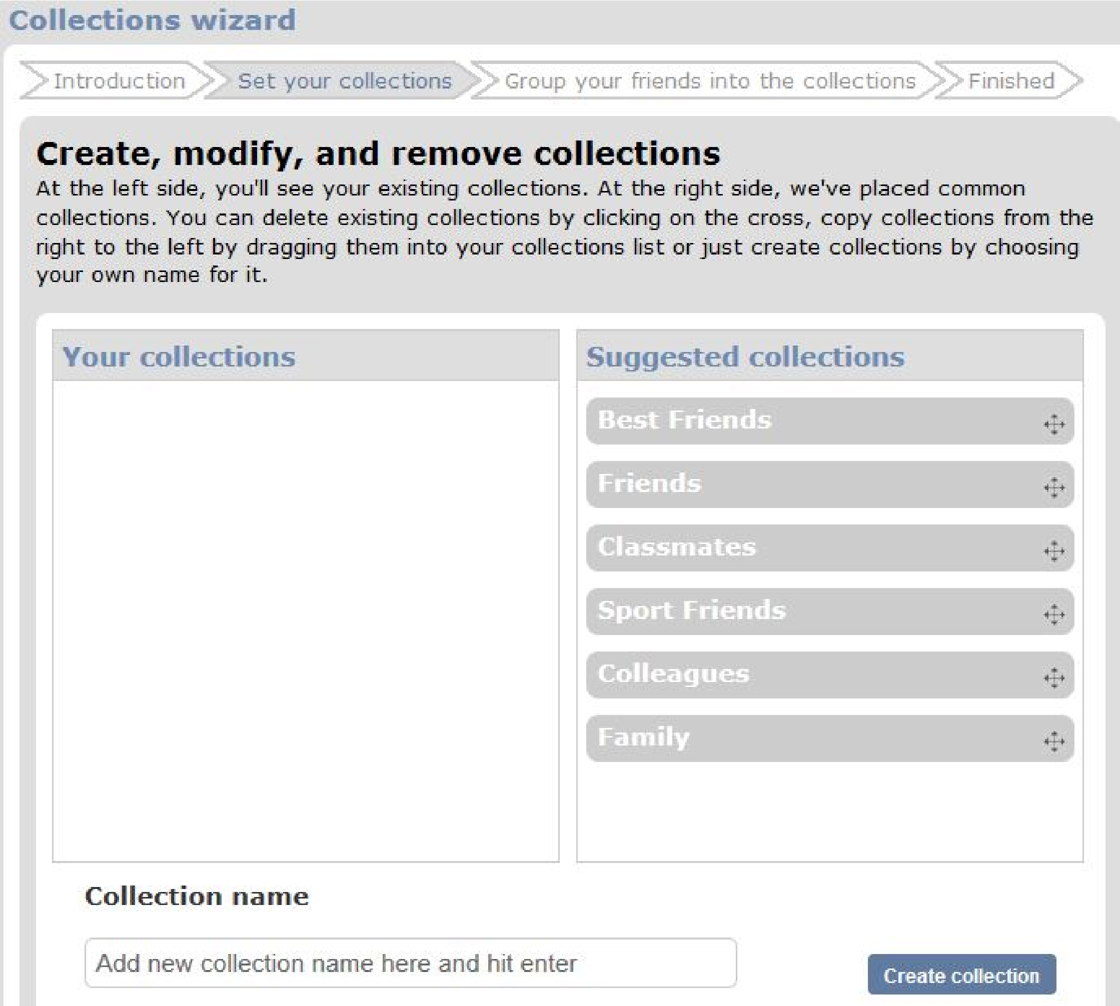
Your real friends, the ones you feel comfortable sharing private details with.

Figure 6.1: Google Circles.

At first glance, the privacy settings for Google+ appear to be fairly straightforward. Unfortunately, some users discovered that the "resharing" feature could become a privacy issue as information shared within a private Google+ circle could be (re)shared to the public, thus defeating the whole idea of circles [82]. However, it seems that a partial fix is now available, as a drop-down menu has been enabled for users to disable resharing after a post has already been made.

6.1.3 Clique

Clique[3] is based and an extension of the Elgg[4] social networking platform.



Create, modify, and remove collections

At the left side, you'll see your existing collections. At the right side, we've placed common collections. You can delete existing collections by clicking on the cross, copy collections from the right to the left by dragging them into your collections list or just create collections by choosing your own name for it.

Figure 6.2: Collection Wizard from Clique.

We describe thereafter some of the privacy features of Clique:

- *Collections.* Contacts are organized in collections, which roughly correspond to social circles. Users can form different groups by defining close friends, family,

[3] `http://clique.primelife.eu`

[4] `http://www.elgg.org`

colleagues and former school-friends (Figure 6.2).

- *Flexible access control to content.* All content contains attribute certificate policies based on moving collections and contacts that can be defined using a simple and easy-to-use graphical user interface.
- *Visual audience indicators.* Content are labeled with icons showing who has access to this information.
- *Fading relations.* Depending on the activity of one's contacts, these users slowly disappear. At first, this happens through visual indicators in the form of a colored border around user icon, and later by closing access to one's data from the automatically defriended contact.

Clique provides users with a social network platform that enables them to keep control over their privacy. More precisely, fine-grained access control mechanisms are available and configuration of multiple identities (*e.g.* family, personal, professional) can be used for interactions with other users. When posting a data item, such as for instance the name, birthday or profile photo on the site, the user can define for every single other users whether they should be able to see it or not.

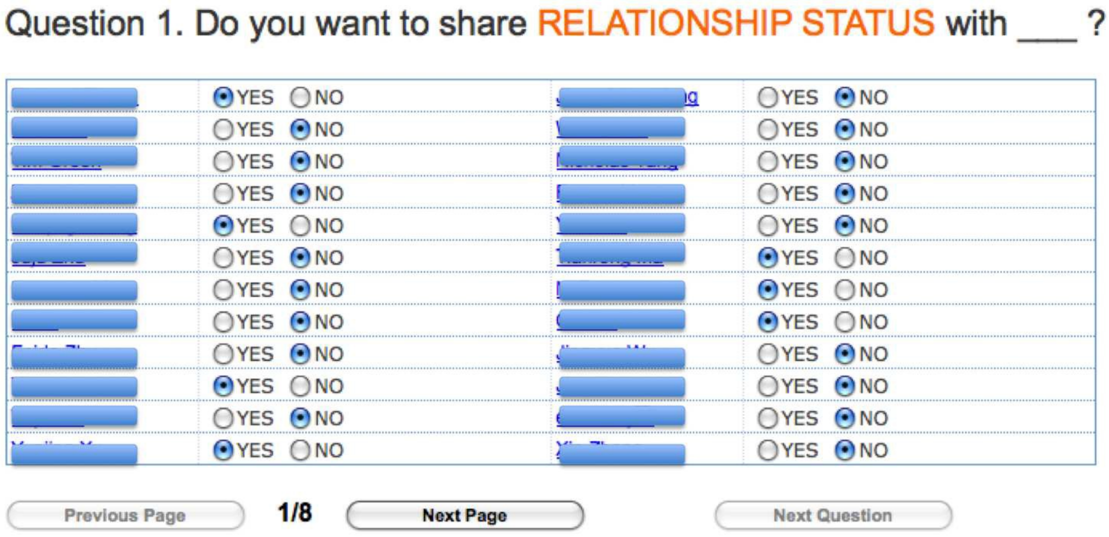
6.2 Privacy add-ons

All the most widely used SNS are based on a centralized architecture in which the data of users is stored on a server in the hands of the SNS provider. Currently, many of these SNS are facing criticisms and even lawsuits [59] regarding the way they manage the privacy of their users. Historically, a first approach for helping users to protect their privacy in these SNS was in the form of privacy add-ons that were integrated within the existing systems, rather than constructing an entirely new privacy-enhanced SNS from scratch that would face the cold start issue. We categorize the privacy add-ons into three groups: *Privacy Recommendatio*n, *Encryption and Hiding*, and *Access Control*.

6.2.1 Privacy Recommendation

Even though Facebook has recently changed and simplified its privacy settings in response to criticisms from privacy advocates and the public, their privacy settings remain complicated and confusing for a large proportion of users [17]. To address this issue "Recommendation add-ons" such as *Privacy Wizard* [42], *Facebook Privacy Scanner*[5] and *Privacy Defender*[6] are useful tools that help users to properly configure the privacy settings of their SNS account and raise awareness by making them understand which parts of their profile are sensible and publicly available.

- The *Privacy Wizard* (still in conception stage) is an application that infers a privacy-preference model by collecting gathering privacy preferences from users (*e.g.*, what kind of information they want to show to their colleagues). This system relies on the observation that users often define their privacy preferences by an implicit set of rules (refer to as a model). Once learned, this model is then used to automatically derive the user's detailed privacy settings (Figure 6.3).



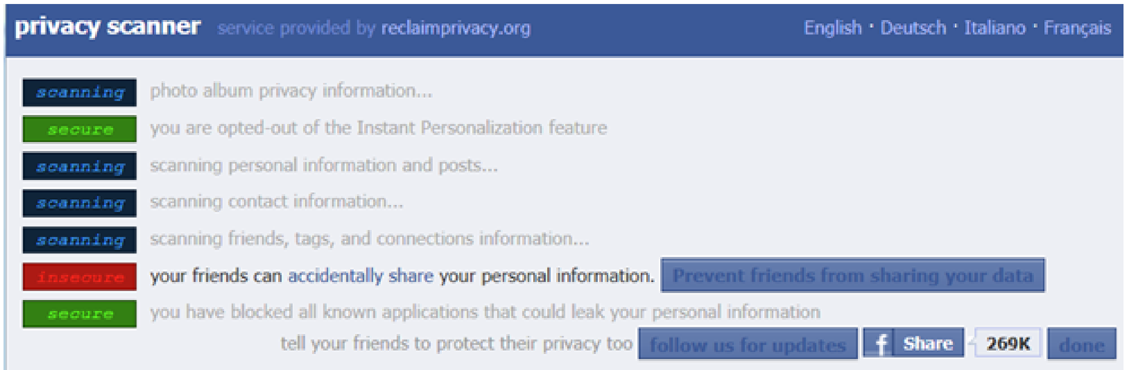
Question 1. Do you want to share RELATIONSHIP STATUS with ___ ?

[redacted]	● YES ○ NO	[redacted]	○ YES ● NO
[redacted]	○ YES ● NO	[redacted]	○ YES ● NO
[redacted]	○ YES ● NO	[redacted]	○ YES ● NO
[redacted]	○ YES ● NO	[redacted]	○ YES ● NO
[redacted]	● YES ○ NO	[redacted]	○ YES ● NO
[redacted]	○ YES ● NO	[redacted]	● YES ○ NO
[redacted]	○ YES ● NO	[redacted]	● YES ○ NO
[redacted]	○ YES ● NO	[redacted]	● YES ○ NO
[redacted]	○ YES ● NO	[redacted]	○ YES ● NO
[redacted]	● YES ○ NO	[redacted]	○ YES ● NO
[redacted]	○ YES ● NO	[redacted]	○ YES ● NO
[redacted]	● YES ○ NO	[redacted]	○ YES ● NO

Figure 6.3: Privacy Wizard.

[5] http://www.reclaimprivacy.org
[6] http://www.privacydefender.net

- *Facebook Privacy Scanner* is a bookmarklet[7] that can scan a Facebook account to inspect users' privacy settings and shows to users which parts of their profile are secure and which ones are publicly available (Figure 6.4).



privacy scanner service provided by reclaimprivacy.org

English · Deutsch · Italiano · Français

scanning photo album privacy information...

secure you are opted-out of the Instant Personalization feature

scanning scanning personal information and posts...

scanning scanning contact information...

scanning scanning friends, tags, and connections information...

insecure your friends can accidentally share your personal information.

secure you have blocked all known applications that could leak your personal information

tell your friends to protect their privacy too

Figure 6.4: Privacy Scanner.

- *Privacy Defender*, another Facebook application, takes a step further as it not only examines user privacy settings but also changes them directly according to the user preferences. However, following the new changes in Facebook's privacy settings, Privacy Defender no longer works with the current version of Facebook.
- *Reflective Policy Assessment* (RPA) is a visualization tool that help users examine their profile from the viewpoint of another user in their extended neighbourhood in the social graph [9]. This tool could be implemented on the client side (*e.g.* as a third-party Facebook application).

These add-ons heavily rely on the existing privacy settings of the SNS provider. Therefore, they are also limited by these same settings and if the SNS does not provide enough flexibility regarding privacy preferences they cannot really help. For instance, as the current privacy settings of MySpace are very simple, a recommendation add-on would not be really useful for this SNS.

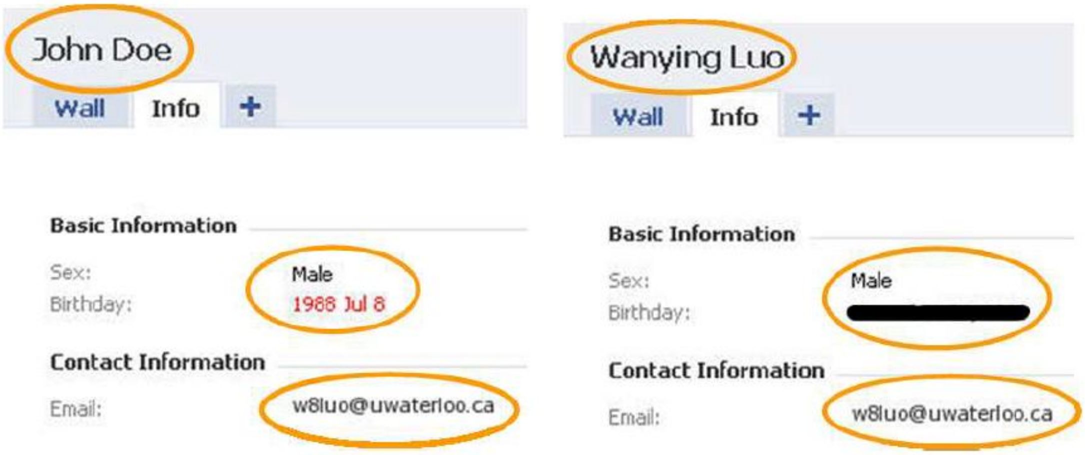
[7] A bookmarklet is an unobtrusive JavaScript stored as the URL of a bookmark in a web browser or as a hyperlink on a web page (source: Wikipedia).

6.2.2 Encryption and Hiding

The second approach to protect the privacy of the user is to encrypt or to hide the data before uploading it to SNS server, therefore not trusting the SNS in handling the personal data directly.

- *NOYB* (acronym for None Of Your Business) [50] is based on the observation that some SNS can operate on “fake” data. As a consequence, privacy can be preserved by restricting the ability to recover the real data from the fake data to authorized users only. In NOYB, the user data is first encrypted, and afterwards the encrypted text is encoded in a way to make it look like legitimate data. The online service can operate on the encrypted data, but only authorized users can decode and decrypt the result. A proof-of-concept version of NOYB was implemented in the form of a Firefox plugin. The key exchange channel, necessary to send the corresponding decryption keys to friends, is independent from the SNS and may be implemented in the form of email, through the use of a third party or a peer-to-peer network. Each user maintains one master key, from which the Firefox plugin generates keys to encrypt each field from the profile. The master key is sent to the user’s social network (friends, friends of friends etc.) via the key exchange channel. This method raises the issue of revocation when the user wants to “unfriend” another user, which may potentially require an update of the key distributed to all the friends of a particular user.
- *FaceCloak* [69] follows the steps of NOYB by enforcing user privacy on the SNS by providing fake information to the SNS and by storing sensitive information in encrypted form on a separate server. FaceCloak goes a step forward comparing to NOYB as it can also protect the data posted to a Facebook application (Figure 6.5). FaceCloak is implemented as a Firefox extension and only replace simple profile information such as name, birthday and gender as generating fake information that looks genuine for more complex data (such as activities and interests) can be difficult. Moreover, FaceCloak supports incremental deployment and the users can decide which information to make public or to encrypt. However, this appli-

cation does not allow users to customize access control for each group of friends. In addition, if the SNS detects that a user's information (*e.g.*, birthdate or email address) is fake, it could easily suspend his account.



John Doe

Wall Info +

Basic Information

Sex: Male

Birthday: 1988 Jul 8

Contact Information

Email: w8luo@uwaterloo.ca

Wanying Luo

Wall Info +

Basic Information

Sex: Male

Birthday: [redacted]

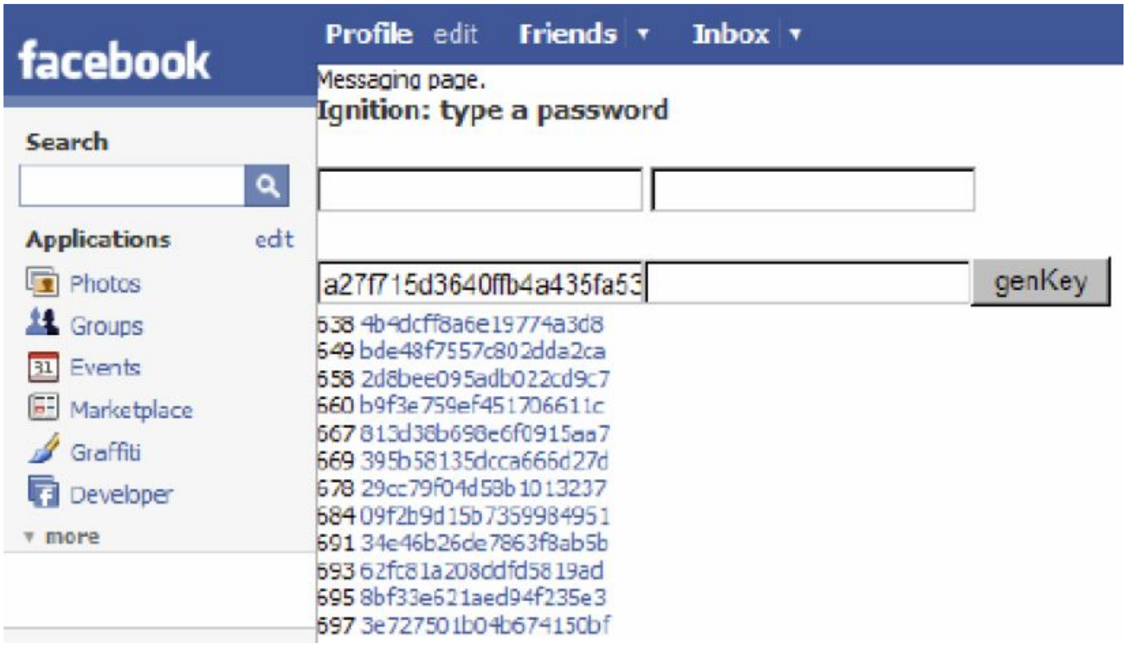
Contact Information

Email: w8luo@uwaterloo.ca

(a) View of account owner (b) View of unauthorized members

Figure 6.5: FaceCloak: A Facebook account under protection.

- *FlyByNight* [68] is a Facebook application for encrypting sensitive data that relies on asymmetric cryptography (Figure 6.6). When a user first registers, he needs to generate a public/private key pair and provide a password, which will be used to encrypt his private key. The key generation and cryptographic operations are performed by a JavaScript program located on the client side. The encrypted private key is then transmitted to his friends via Facebook servers and stored in a key database on the flyByNight server. FlyByNight also supports a "one-to-many" operation that encrypts a single message for a group of friends using *proxy cryptography*. In a nutshell, proxy cryptography allows a party to take a message encrypted with the key of a particular and to re-encrypt it with the key of another user without learning the content of the message [58].



Messaging page.
Ignition: type a password

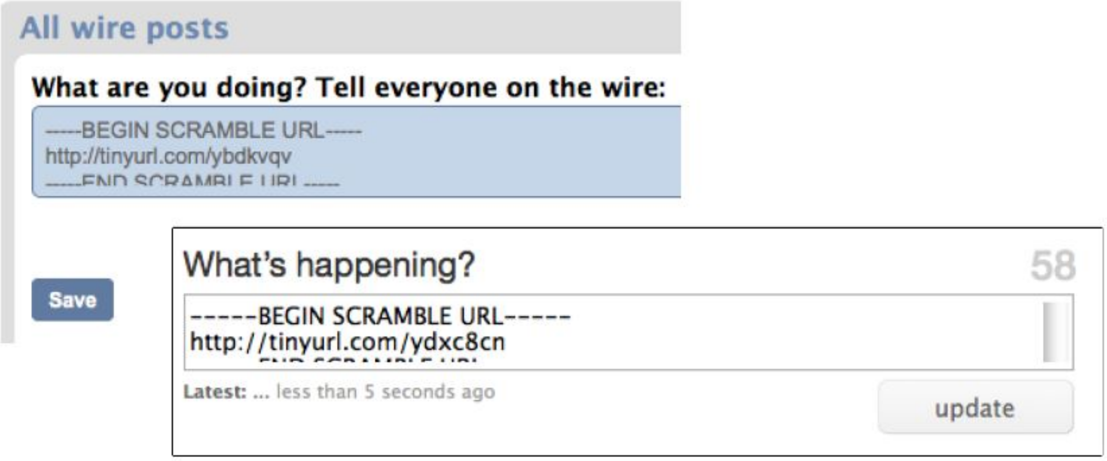
a27f715d3640ffb4a435fa53

```
638 4b4dcff8a6e19774a3d8
649 bde48f7557c802dda2ca
658 2d8bee095adb022cd9c7
660 b9f3e759ef451706611c
667 813d38b698e6f0915aa7
669 395b58135dcca666d27d
678 29cc79f04d58b1013237
684 09f2b9d15b7359984951
691 34e46b26de7863f8ab5b
693 62fc81a208ddfd5819ad
695 8bf33e621aed94f235e3
697 3e727501b04b674150bf
```

Figure 6.6: FlyByNight.

- *Scramble!* [13] is a Firefox extension allowing users to encrypt and share their own data within any SNS (Figure 6.7). Scramble! relies the OpenPGP encryption mechanism. Users can choose to store large amount of encrypted data inside SNS or only list “tiny url” snippets, that point to the location of encrypted data into any third-party server. Users’ public keys are distributed “manually” through e-mail, website or key servers. Unfortunately, to the best of our knowledge, the current version of Scramble! does not work with the latest version of Firefox (version 8.1).

- *FaceVPSN* [31] (acronym for Facebook Virtual Private Social Network) is inspired from the concept of *Virtual Private Network* (VPN) used to secure traditional computer networks (Figure 6.8). While the users cannot stop the sharing of public information due to the design of Facebook, they can publish *pseudo-information* instead, which inevitably can be seen by third parties but does not impact the user privacy. When a user browses a profile of another user in the VPSN, a FaceVPSN


All wire posts
What are you doing? Tell everyone on the wire:
Save
What's happening?
58
Latest: ... less than 5 seconds ago
update

-----BEGIN SCRAMBLE URL-----
http://tinyurl.com/ybdkvqv

-----BEGIN SCRAMBLE URL-----
http://tinyurl.com/ydxc8cn

Figure 6.7: Scramble in (private) Twitter.

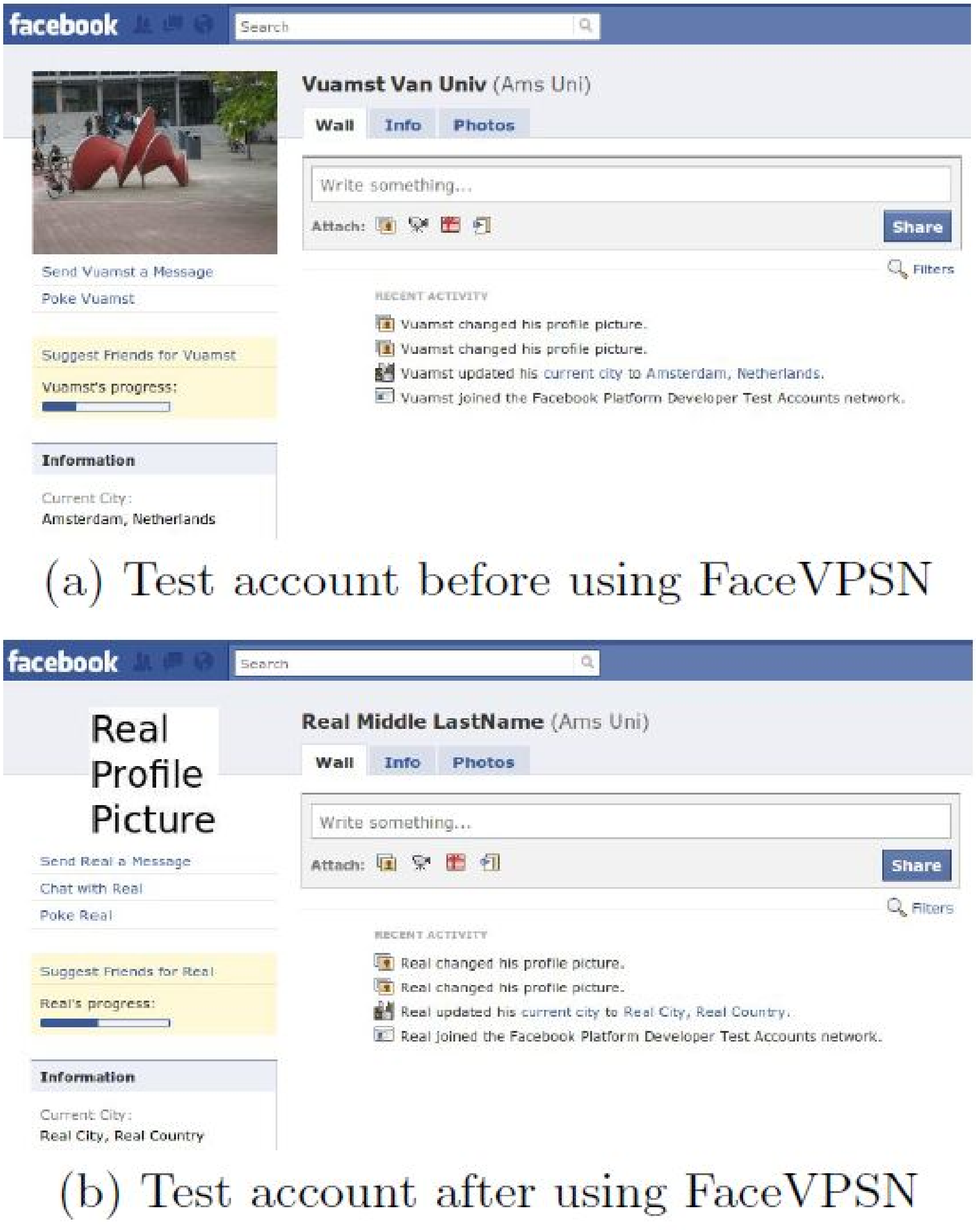
component (in the form of Firefox extension) is in charge of transparently displaying to the user the real information, instead of the one actually published on the host SNS.

The Encryption add-ons protect the data sovereignty of the users, because it is assumed that the SNS providers cannot decrypt the "fake" data. However, if they detect that the users' information (*e.g.*, birthdate or email address) is fake or encrypted, these user accounts could easily be suspended (as mentioned in the terms of use of some SNS). Therefore, it is not enough that the data remains confidential through encryption but it also needs to be indistinguishable from genuine data in the spirit of stenography.

6.2.3 Access Control

When the SNS cannot be trusted to store users' social network or its privacy settings are not fine-grained enough, the privacy add-ons can provide a separate access control mechanism.

- *Beato, Kohlweiss and Wouters* [12] have proposed to rely on cryptographic mechanisms in order to enforce access control in SNS. More precisely, they use the *OpenPGP* standard for key distribution (like Scramble!), which supports the en-



Vuamst Van Univ (Ams Uni)

Write something...

Send Vuamst a Message

Poke Vuamst

Suggest Friends for Vuamst

Vuamst's progress:

Vuamst changed his profile picture.

Vuamst changed his profile picture.

Vuamst updated his current city to Amsterdam, Netherlands.

Vuamst joined the Facebook Platform Developer Test Accounts network.

Current City:
Amsterdam, Netherlands

(a) Test account before using FaceVPSN

Real Middle LastName (Ams Uni)

Real Profile Picture

Write something...

Send Real a Message

Chat with Real

Poke Real

Suggest Friends for Real

Real's progress:

Real changed his profile picture.

Real changed his profile picture.

Real updated his current city to Real City, Real Country.

Real joined the Facebook Platform Developer Test Accounts network.

Current City:
Real City, Real Country

(b) Test account after using FaceVPSN

Figure 6.8: Profile Page in FaceVPSN.

cryption from one to multiple recipients. In this framework, each user has two OpenPGP keys, one public and one private. The system generates a one-time-only secret key to encrypt the data and then uses the public keys of the selected audience to encrypt this secret key. The encrypted secret key is transmitted together with the encrypted data to the recipient. The prototype is developed as an extension to Firefox and Elgg, an open source social networking platform that also forms the basis of Clique. The data owner takes care of the access control enforcement on the client side (using the Firefox extension with authorized recipients' public key), and as a direct consequence the SNS (Elgg) is oblivious to who has access to which information as long as the requests are made across anonymous channels such as *TOR*[8] for instance. More precisely, the Firefox plugin first parses the webpage and searches for encrypted text. Afterwards, if the user possesses the associated access rights, the plugin automatically decrypts the content and presents it unencrypted.

- *Lockr* [97] provides an access control mechanism for SNS in which the identity of a user is represented by a pair of public and private key. Before he can access an object, a user has to either present a *social attestation* (*i.e.*, a certificate of a social relationship with another user) or his public key must be registered in the *Social Access Control List* of the owner of this object. Within the framework of Lockr, the users have a universally accessible address book for maintaining a single copy of a user's social network, as well as an access control scheme that facilitates the sharing of personal data. The shared content is stored on a third party server. In the current implementation of Lockr, the address book is provided by a Facebook application called *LockrCenter* and the shared pictures are stored on *Flickr*[9]. In this implementation, the authorized user will receive a hard-to-guess URL of the picture. One of the drawbacks of this add-on is that it currently only works with pictures and heavily depends on the functionalities provided by Flickr.
- *Persona* [10], a prototype application integrated within Facebook, offers flexible and fine-grained access control for user data by using *Attribute-Based Encryption* (ABE). In this type of encryption, users are identified by public keys and their pri-

[8] `http://www.torproject.org`

[9] `http://www.flickr.com`

vate key is associated with a set of attributes describing the profile of their groups. A user will be able to decrypt a piece of data if and only if his attributes satisfy the privacy policy of the group in which this piece of data is shared. Persona applications are accessible as Facebook applications and can interact with Facebook's API, thus providing privacy-enhanced applications through the familiar Facebook interface. Users protect their private data by storing it on third party servers rather than directly on the SNS. Only fellow Persona users that were given the necessary keys for access rights will be able to access the data. Currently, Persona has been integrated within Facebook as an application, and the users logs into that application through a Firefox extension, which interprets the special markup language used by Persona applications. However, choosing a separate server to host data is not easy and requires significant investment in terms of energy and time that makes the system not easily accessible for the majority of SNS users.

- *Web-Traveler* [93] proposes a policy-driven approach to control the access to pictures posted on the SNS. In particular, users have to specify access control policies for their content as they upload it on the SNS. There are two kinds of policies (positive and negative), which specify 5 types of operations: tag, comment, view, download and upload. An image recognition component is used to detect the similarity between the uploaded image and other images in the database. More precisely, each image in the database is described by an index, which is a form of fingerprint of its visual characteristics. The comparison process is executed using this index. Another important feature of Web-Traveler is that it allows the enforcement of policies across websites. However, the Web-Traveler architecture cannot be implemented on an existing SNS platform without an important number of modifications to the system core.

Privacy add-ons are a first step towards giving users more control over their privacy on SNS and raising their awareness on this subject. However, the users still have to comply with the privacy policies and terms of use coming from SNS providers and SNS applications.

6.3 Distributed SNS

More complex approaches have been proposed to provide decentralized solutions that let users set up their own personal servers to fully control the information they share and how they connect with friends. Paul, Buchegger and Strufe [80] distinguish two groups of distributed SNS: *web-based* SNS and *peer-to-peer* (P2P) SNS. Web-based systems rely on a distributed web server infrastructure and require the acquisition of webspace or the deployment of web servers while the peer-to-peer systems take advantages of the substrate of a P2P network in order to allow for the publication, search, and retrieval of profiles and their attributes. In this section, we present several distributed SNS, which up to now have been mainly developed in the research community and are not yet fully deploy in the real world.

- *Safebook* [35] adopts a decentralized architecture relying on the cooperation among a number of independent parties, which are also the users of the SNS. Safebook has a three-tier architecture with a direct mapping of layers to the SNS levels (Figure 6.9):
  - The user-centered social network layer implementing the SNS level.
  - The P2P substrate implementing the SNS services.
  - The Internet acting as the communication level.

  As a result, each party in Safebook is represented by a node that is viewed as a host node in the Internet, a peer node in the P2P architecture and a member node in the SNS layer. More precisely, the nodes in Safebook belong to two different overlays:
  - A set of *Matryoshkas*, which are concentric rings of nodes built around each user's node in order to provide trusted data storage, data retrieval and communication obfuscation.
  - A *P2P substrate*, providing lookup service (for instance through *Distributed Hash Tables* (DHT)).

  As all the published data of a user is replicated to its mirrors (the nodes in the innermost shell of his Matryoshka), it is quite difficult to track how his data is disseminated and to execute his right of oblivion when he decides to leave Safebook.

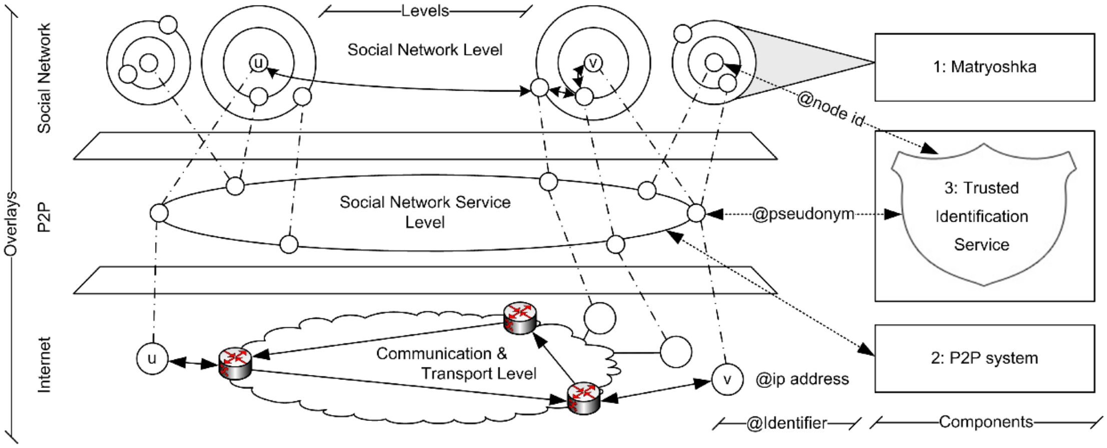


Figure 6.9: Safebook architecture.

- *PeerSoN* [22] achieves decentralization thanks to an external P2P system, called *OpenDHT*, and assures access control through encryption (not yet implemented). PeerSoN has a two-tier architecture: a look-up service and peers containing the user data, such as user profiles. The look-up service stores the meta-data required to find particular users as well as the particular data they store. For example, this meta-data could be their IP address, information about the files they stored and notifications for users. A peer that wants to communicate with another peer invokes the look-up service to retrieve the necessary information to locate the relevant peers and then connect directly to them. As a result, a user can only visit the profile of his friends when they are online, thus providing a low level of availability compared to centralized SNS.
- *PrPl* [85] (acronym for Private-Public) is a decentralized architecture that lets users participate in SNS while keeping the ownership of their data. With PrPl, each user uses a *Personal-Cloud Butler* service to store their profile and also share information with fine-grained access control mechanisms. In practice, a user can choose to run the butler on any server of his choice. Each butler provides a fed-

eration of data storage, meaning that it keeps a semantic index to data that can reside, possibly encrypted, in other storage services. PrPl relies on the standard decentralized *OpenID* management system [10].

- *Vis-à-vis* [86] is a distributed framework for SNS based on the idea of a *Virtual Individual Server* (VIS). A VIS is defined as a virtual machine running in a cloud service that can store their owner's sensitive data and grant access for that data by other parties. The VIS is considered trusted and is allowed to store unencrypted user data. Each user has a key pair whose private key is stored securely on his VIS, while the public key and the IP address of his VIS are distributed via email or an existing SNS to friends of the user. Vis-à-vis also has a notion of groups, which are location-based and can be accessed through clients such as mobile phones or web browsers. The framework is designed to interoperate with existing SNS and allows users to integrate Vis-à-vis group by embedding a group descriptor into the Facebook group. When a user loads the group page on their web browser, a Vis-à-vis browser extension interprets the document received from Facebook, identifies the group descriptor, and rewrites the page to include information downloaded from the appropriate VISes. Currently Vis-à-vis only focuses on providing secure location information sharing for groups.
- *Mr. Privacy* [45] is a social application framework built on top of email, which is used both as a communication channel and personal database. When a message is sent to multiple users, each user receives a separate copy. As a result, once an item is sent from one user to another, it cannot be invalidated and erased from the framework, thus increasing the risk of privacy breaches and not guaranteeing the right to be forgotten.
- *eXO* [67] is a distributed system offering fundamental social networking services such as mechanisms for indexing content and related metadata and efficient algorithms for *search-for-users* and *search-for-content* queries. eXO consists of a large number of nodes, each of which runs a routing protocol for a structured overlay DHT network. In eXO, each user connects to a specific node with a unique

[10] `http://openid.net/`

network identifier. The content shared by a user is originally kept on the user's node but it can be replicated on other nodes in order to increase availability.

- *SuperNova* [89] is a super-peer based SNS architecture that tries to solve the problem of data availability in P2P network by providing incentives for other nodes to store personal data of other users. For instance, when users do not have enough friends to replicate their data, they can use the storage services provided by a "super-peer". Any user of the P2P network can volunteer to become a super-peer, thus increasing its reputation or gaining revenue from advertising.
- The Diaspora [11] project was summarized by its creators as a "distributed network, where totally separate computers connect to each other directly, allowing users to connect without surrendering their privacy". This project is now opened for public testing [12]. The concepts of pod and seed are central to the architecture of Diaspora:
  - A *pod* is a server on which Diaspora is running. The users can set up a pod by themselves or use a public/ private pod.
  - A *seed* is a profile or an account that contains all the data of a specific user. The user's seed interacts with the seeds of his friends to keep each other up to date. Seeds are hosted on pod servers.

  In the architecture of Diaspora, the users are able to move their seeds between pods and they can leave a pod if they do not trust it anymore.
- Socialriver [13], another distributed SNS still at the conception stage, consists of users' "streams" of activity including blogs, photos and other shared data. SocialRiver is built on top of *Wordpress*, an open source content management system, often used as a blog publishing application. Users have control over their private information and have the ability to block sites that use other software that do not implement adequate privacy policies and settings.

[11] `https://joindiaspora.com/`

[12] `http://dias.org`

[13] `http://socialriver.org/`

6.3.1 Privacy Watch

Privacy Watch is an hybrid (centralized/distributed) system based on the *Privacy Framework for SNS* (see Section 4.2) and the concept of *User Privacy Policy* (UPP) (see Section 4.3. Privacy Watch relies on the UPP as an easy and flexible way for users to inform and enforce (in the form of a contract) their privacy concerns to other users, third parties and the SNS service provider. In Privacy Watch, the user can determine how much information he wants to share with the SNS provider by specifying his privacy level (ranging from *No Privacy* to *Full Privacy*). For instance, novice and casual users can choose No Privacy or Soft Privacy and delegate the responsibility of the access control management to the SNS provider. In contrast, if the user chooses the level of Full Privacy, the SNS server will only be trusted in storing an encrypted version of the personal information of the user, which can be consulted at any time by one of his friends. An auxiliary third party, such as an independent mail server, is responsible for storing and exchanging privacy policies and encryption keys between a user and his friends (see Chapter 5). Moreover, by combining watermarking methods with access control logs, it is possible to partially monitor the dissemination of information that belongs to the user.

6.4 Comparison

In this section, we compare different privacy add-ons and privacy-enhanced SNS with respect to the privacy criteria described in Chapter 4, by taking Facebook as the baseline for "standard" SNS. Note that the reputation management criterion is not mentioned in the comparison as none of the studied solutions has implemented it yet.

6.4.1 Centralized SNS

Table 6.I describes the comparison between three centralized SNS: Facebook, Google+ and Clique. Most centralized SNS such as Google+ and Clique now have nearly the same *access control mechanisms* as Facebook with fine-grained privacy settings for each piece of data (per post). The users can share their posts and their data to specific audiences by listing the friend names or groups of friends. With respect to the *search customization*, Google+ allows users to specify which part of their personal profiles is take into account during the search process, while Facebook also lets users decide who can look up their profile by name or contact info. Both Facebook and Google+ support tag review in the sense that the users can approve or remove tags pointing to their profiles (*i.e.*, tag removal).

Facebook's *Friend group*, Google+'s *Circles* and Clique's *Collections* are mechanisms that create groups of friends sharing similar interests or the same kind of social relationship. Users of Facebook and Google+ can use an *inline menu* (*i.e.*, privacy setting integrated into the post) to specify who can access their posts. On Clique, the access control policy of a piece of data is not directly entwined with it like on Facebook and Google+, which makes it difficult to navigate through its privacy settings.

Nowadays, all centralized SNS already provide *explicit privacy policy* on their website for the users. Recently, Facebook rewrote and simplified its privacy policy in order to made it easier for users to understand it. Additionally, the concept of *privacy lens* is implemented by both Facebook and Google+. Unfortunately, a recent survey of the global strategic branding firm Siegel+Gale [14] reveals confusion and frustration among consumers regarding Facebook and Google privacy policies. The survey of more than 400 participants shows that users have little understanding of how Facebook and Google track and store user information and activity, and how information is shared and with whom [91]. Moreover, in their terms of use, Facebook and Google+ require their users to give them a "non-exclusive, transferable, sub-licensable, royalty-free, worldwide license" (Facebook) or "a perpetual, irrevocable, worldwide, royalty-free, and non-exclusive license" (Google+) on all the content they post on the SNS, therefore not respecting the sovereignty principle. In addition to the absence of reputation system, these three SNS do not provide *accountability* support for their users.

[14] `http://www.siegelgale.com`

Table 6.I: Centralized SNS.

	Access control	Usability	Transparency	Data sovereignty	Accountability
Facebook	- Per post and by groups / friends - Search customization (who) - Tag approval	- Inline menu	- Easy-to-understand privacy policy - Privacy lens	- No	- No
Google+	- Per post and by groups/ friends - Search customization (which part) - Tag approval	- Inline menu	- Complex privacy policy - Privacy lens	- No	- No
Clique	- Per post and by groups/ friends	- Separate menu	- No	- No	- No

6.4.2 Privacy add-ons

Table 6.II compares several privacy add-ons for centralized SNS. These add-ons provide simple and easy-to-implement solutions for users with privacy concerns. However, they cannot completely satisfy all the privacy criteria mentioned in Section 4.4 because they still rely on the existing infrastructure of the SNS provider and thus are limited by the functionalities provided by the architecture. Moreover, these privacy add-ons are bound by the privacy policy and terms of use of the SNS.

Specifically, the recommendation add-ons do not enhance the *access control* mechanisms of centralized SNS but help users to optimize the privacy settings on their profile. Reflective Policy Assessment visualizes the extended neighbourhood of the user's social graph and allows him to inspect her profile from the view point of another user. While Privacy Wizard infers privacy settings on new posts based on user habits, Privacy Defender proposes three different privacy categories for the users to choose: *My friends*, *My Social Network*, and *Everyone but not everything*. Taking a step further, Privacy Scanner can actively modify users' privacy settings to prevent their friends from sharing their data with unauthorized people. Unfortunately, Privacy Defender and Privacy Scanner are not fully compatible with the latest Facebook privacy settings. Therefore, to the best of our knowledge, their users do not have access to this feature at the moment.

As most Encryption and Hiding add-ons are developed as a Firefox extension (with the exception of FlyByNight), they do not have access to the privacy settings of the SNS providers. As a result, the users have to manually manage their own *Access Control Lists* (ACL) and exchange keys or XML file containing real data (in the case of FaceVPSN) through separate channels such as email or dedicated key server. Once this initialization is performed, the process of encryption/decryption is managed automatically by the add-ons. As user data is encrypted and hidden from the SNS providers, these add-ons ensure that user data only belongs to them and not to the SNS. However, because the encrypted data is stored on a third party server, when that server is down, it is impossible to retrieve the real data. Another limitation of the Encryption and Hiding add-ons is that they can only encrypt text data and cannot be applied yet to other media. More precisely, NOYB and FaceCloak can only encrypt and "hide" the information from a user profile (such as name and birthday) while FaceVPSN shields only publicly available information in Facebook (*e.g.*, name, profile picture and current city).

The boundary between Encryption and Hiding add-ons and Access Control add-ons seems to be quite fuzzy as most Access Control add-ons use encryption to provide data sovereignty for users. There are two main categories of approaches for Access Control add-ons. In the first approach, the add-ons try to hide their existence from the SNS providers, which is used only for friend discovery or data storage. The add-ons following this approach are the add-ons developed by Beato, Kohlweiss and Wouters, as well as Lockr and Persona. These add-ons manage users' ACL locally through a Firefox extension. The contact lists are provided by an application or a plugin installed on the SNS servers. Lockr and Persona take a step further as the encrypted data is stored on a third party server. For instance, Lockr uses Flickr to store pictures of the users. The second approach, which requires active cooperation from the SNS, is taken by Web-Traveler. In this approach, the SNS is trusted with unencrypted data storage, but an access control policy is attached to each piece of data. In this situation, the SNS can determine the provenance of user data and can prevent the violation of his access control policies. The main limit of this approach is that users rely on the good will of SNS providers.

6.4.3 Distributed SNS

Table 6.III shows the comparison between Facebook, Privacy Watch and other distributed SNS. Distributed SNS appear to solve the problem of *data sovereignty* inherent to centralized SNS and give the users more freedom by allowing them to deploy their own social network. These systems have participated in an attempt to defeat the monopoly of centralized SNS represented by Facebook but currently none of the proposed systems have been adopted at such a large scale.

Diaspora is the most well-known distributed SNS at the moment even though it is still at a alpha version and users join only by invitation. To create a Diaspora account, a user needs to build a profile from scratch or import his name, photos and posts directly from their Facebook account. Users install their unencrypted profile on independently hosted servers and can move their profile whenever they want. The current privacy setting of Diaspora is limited to “per aspect" (*e.g.*, users can specify the sharing permission for groups of friends only). Nevertheless, all the functionalities of Diaspora are not yet fully implemented and the hosted server provides no privacy policy at the moment. Therefore, we think that Diaspora is not sufficiently mature for us to really assess its privacy features.

Regarding *access control*, each system has different types of target users and provides different access control level. For instance, Safebook users seem to have the best supported access control as the user data is organized in atomic attributes for which particular *Access Control Policy* (ACP) can be set. Friend discovery is made through a P2P substrate in which the searchable keys are the hashed properties and node identifier of users. Currently it seems that users cannot specify which properties are searchable or who can search for themselves. The eXO system is designed so that its users have total control on their contents and resources. Users can mark their content as public or private to define which users can access. Public content items are indexed and searchable. Additionally, owners can reject access requests made by other users, even for public content. PeerSoN users manage their own ACL and distribute encryption keys to authorized friends. Due to the fact that the look up service stores necessary metadata to find users and their data, the users are not able to customize the search process. As PrPl focuses on resource sharing services, including photo browsing and music streaming, its users can specify a ACP on each service as well as render a service searchable or not. Vis-à-vis is a distributed system for location sharing in which users can create groups to share their location with fine granularity. In SuperNova, a user profile is divided into three part: public, protected and private. Protected data is classified into different categories before being encrypted. The decryption keys are then distributed by the users to authorized friends. Users of Mr. Privacy system identify themselves by their email address and as a consequence, it is quite easy to identify and search for a user in the system (unless the email address is completely unrelated to the name of a user).

With respect to the criteria of *Usability*, *Transparency* and *Accountability*, we are not able to determine to which extent the distributed systems satisfy these three criteria at the moment. For instance, to the best of our knowledge, these systems have not yet implemented the *Privacy lens* functionality. Additionally, the criteria of *Explicit privacy policy* from the SNS is not applicable to distributed systems.

With respect to data sovereignty, Safebook, PeerSoN, eXo and SuperNova system propose to use local and shared resources of the P2P overlay while PrP, Vis-a-Vis and Mr Privacy store data on dedicated servers. In both cases, the data belong only to the users. However, as the user data is replicated on other peer nodes or stored on third party server, it is quite difficult to ensure in practice the *right to oblivion*.

In conclusion, the privacy add-ons provide simple and mostly easy-to-implement solutions for users with privacy concerns. However, they cannot completely satisfy all the privacy criteria mentioned in Section 4.4 as they still rely on the existing infrastructure of the SNS provider and thus are limited by the functionalities of this infrastructure. Moreover, these privacy add-ons are bound by the privacy policy and terms of use of the SNS provider. For instance, most current SNS, such as LinkedIn, MySpace and Facebook, claim ownership of personal information put on their SNS and do not erase user data when users choose to delete their accounts. To summarize, current centralized

SNS focus on interaction and sharing information between users without much concern about their privacy. Another drawback of centralized systems is that they can be very vulnerable to security and privacy breaches as data is stored in a centralized database, thus making it a single point of potential failure.

The distributed SNS concept comes to the rescue by offering to users the possibility of increasing their control on the sovereignty of their data. However, these systems suffer from the traditional disadvantages of distributed approaches such as redundant resources and no centralized control (which in terms of privacy can of course be also seen as an advantage). One of the main difficulties is that in a P2P network, it becomes more difficult to search for friends and relatives unless a good look-up service is implemented. Another difficulty inherited from P2P system is the question of availability. User contents need to be replicated to other nodes to increase the availability and reduce waiting time. Moreover, most of the proposed solutions have a high computation and communication complexity and are only suitable for advanced users because they require some technical expertise to be effectively deployed and adopted. Therefore, casual and normal users may possibly prefer a system offering an acceptable trade-off between privacy and ease of use. This actually is one of the motivations behind Privacy Watch, our own privacy-enhanced SNS. With respect to the privacy criteria defined in Section 4.4, Privacy Watch currently fulfills most of them. Our solution, Privacy Watch, is an alternative between these two main approaches and provides a balance between privacy and ease of use depending on the privacy level chosen by the user. One merit of Privacy Watch is that the users do not have to install a separate server to host their profile (as it is the case in some solutions). Moreover, the SNS provider and third parties (advertisers, application providers) still get some profit from pieces of information that the users choose to make publicly available.

In this chapter, we study multiple privacy-enhanced solutions for SNS and compare them with our own solution Privacy Watch according to the privacy criteria described in Section 4.4. The conclusion will be presented in the next chapter.

Table 6.II: Privacy addons for centralized SNS.

	Access control	Usability	Transparency	Data sovereignty	Accountability
RPA	- No	- Visualization	- Privacy Lens	- No	- No
Privacy Wizard	- No	- Derive privacy settings	- N/A	- No	- No
Privacy Scanner	- No	- Prevent friends from sharing user data	- Privacy overview	- No	- No
Privacy Defender	- No	- 3 privacy tiers	- Privacy overview	- No	- No
NOYB	- User profile	- Easy to setup - Manual key exchange	- No	- Partially - Fake data on SNS	- No
FaceCloak	- Simple profile information - ACL	- Easy to setup - Manual key exchange	- No	- Partially - Fake data on SNS and real data on 3rd server	- No
FlyByNight	- Text only - SNS privacy settings	- Easy to setup	- No	- Partially - Encrypted data and encrypted key on SNS and 3rd server	- No
Scramble!	- Text only - ACL	- Easy to setup - Manual key exchange	- No	- Partially - Encrypted data on SNS	- No
FaceVPSN	- Publicly available information	- Easy to setup - Manual info exchange	- No	- Partially - Fake data on SNS	- No
Beato, Kohlweiss and Wouters	- Text only ACL	- Easy to setup	- No	- Partially - Encrypted data on SNS	- No
Lockr	- Only for photos - ACL and Social Attestation	- Easy to setup	- No	-Partially - Social network on SNS, photo on Flickr	- No
Persona	- ACL - Attribute-based encryption	- Easy to setup	- No	- Partially - Encrypted data on 3rd servers	- No
WebTraveller	- ACL - Integrated with SNS privacy	- Easy to setup	- No	- Partially	- Enforcement of user policies

Table 6.III: Distributed SNS.

	Access control	Usability	Transparency	Data sovereignty	Accountability
Diaspora	- Per post and by groups	- Inline menu	- No	- No	- No
Safebook	- Per attribute and by friends - ACP	- Join by invitation only - Register via through the identification services	- N/A	- Nodes replicated at trusted contact	- N/A
PeerSoN	- ACL - Decryption keys	- Set up own servers	- N/A	- Decentralized on user's server	- N/A
PrPl	- Per services - ACP	- Easy to develop apps - OpenID	- N/A	- Personal-cloud butler on user server	- N/A
Vis-à-vis	- By group - Fine-grained	- Integrated with SNS - Separated VIS	- SNS policy - VIS policy	- Unencrypted data on hosting VIS - Profile data on SNS	- N/A
Mr. Privacy	- N/A	- Email, easy to use	- Privacy policy from email provider	- Multiple copies of user data are sent to friends	- No
eXO	- ACL - Search customization	- N/A	- N/A	- Public data is indexed and may be replicated, private part is stored only on source node	- N/A
SuperNova	- Per data category - Decryption keys	- Client-based key distribution	- N/A	- Nodes replicated at friend nodes and super-peers	- N/A
PrivacyWatch	- UPP for each piece of data	- Flexibility - Easy initialization	- Privacy lens - Understandable privacy policy - Matching of privacy policies	- Encrypted data - Hybrid architecture	- Right to oblivion - Incorporation of provenance - Tag blocking

CHAPTER 7

CONCLUSION

Since their introduction, Social Networking Sites (SNS) such as MySpace, Facebook, Hi5 and LinkedIn have attracted millions of users and have become established places for keeping contact with old acquaintances and meeting new ones. Because of the numerous interactions between users, large amounts of personal information circulate on the SNS. However, due to *lacks of user awareness and proper privacy protection tools*, huge quantities of user data, including personal information, pictures and videos are quickly falling into the hands of authorities, strangers, recruiters, and even the public at large. Privacy settings of the current SNS are not flexible enough to protect user data. In addition, users have no control on what others reveal about them. Many third party applications and marketers can take advantage of the users' personal information without their knowledge or agreement. By using SNS and accepting their privacy policy, the user has volunteered to relinquish their ownership on their own data. That's why the proposed solutions based on current SNS cannot solve all user privacy issues.

In September 2008, a special issue of the Scientific American has raised the question about the future of privacy in a Facebook age: "Can we safeguard our information in a high-tech and insecure world?" To answer this question, in this thesis, we present an approach that both increases *privacy awareness* of the users and *maintains the sovereignty* of their data when using SNS.

The first contribution of this thesis is the *classification of multiple types of risks* as well as *user expectations* regarding privacy in SNS (see chapter 3). Specifically, we first identify three main *privacy risks* in SNS: security, reputation and credibility, and profiling risks. Secondly, we conduct a *preliminary study* on privacy issues in SNS. Even though the survey might not cover the whole spectrum of SNS users, it confirms the existence of these three privacy risks and highlight different *privacy requirements and privacy concerns* among SNS users.

To address these privacy concerns, afterwards, we introduce the *Privacy Framework* *for SNS* and the concept of *User Privacy Policy* (UPP) (see chapter 4). Specifically, since privacy revolves around user data, we categorize *user data*, *user privacy concerns* as well as *groups of trust*. Based on these categorizations, we derive four *privacy levels* (No Privacy, Soft Privacy, Hard Privacy, Full Privacy) and three *tracking levels* (Strong Tracking, Weak Tracking and No Tracking). Through the use of UPP, the data owners can demand anyone who will access their data to abide by their condition, such as no disclosure to other parties.

While SNS and privacy may seem *a priori* to have two opposite goals, the fact that most of the current SNS do not respect the data minimization and the data sovereignty principles is not because it is impossible but rather is a design choice made by the SNS providers. Therefore in order to reconcile SNS and privacy, the third contribution of the thesis is a taxonomy of different *privacy criteria* that an SNS can integrate into its design to enhance the privacy of its users (see Section 4.4). Moreover, we are also the first to coin the term of a *Privacy-enhanced Social Networking Site* (PSNS). An PSNS is a social networking site fulfilling the properties of *privacy awareness and customization*, *data minimization* and *data sovereignty*.

Furthermore, we present also *Privacy Watch*, a theoretical proposal of a PSNS platform that combines the concept of provenance and accountability to help SNS users maintain sovereignty over their personal data (see chapter 5). One important contribution of Privacy Watch is that it could partially enforce the privacy policies (UPP) stated by the different actors of the SNS (such as SNS provider, applications and other users). Indeed it is very easy for an actor to state a particular privacy policy, but in reality nothing really forces him to respect it once he has been able to access this piece of information. For instance, a user might do a copy of a particular sensitive picture of a friend without his consent. However, by combining watermarking methods with accountability mechanism, the users of Privacy Watch can review and partially control how their personal information flows both inside (through the Access Controller) and outside the SNS (through the Personal Tracker).

Finally, we *study* the different solutions that have been proposed to enhance the privacy of users of SNS and *evaluate* these solutions according to the privacy criteria defined in Section 4.4. Compared with these solutions, the most important advantage of Privacy Watch is that it provides a balance between privacy and ease of use depending on the privacy level chosen by the user (see chapter 6). Moreover, the users do not have to install a separate server to host their profile (as it is the case in some solutions). Moreover, the SNS provider and third parties (advertisers, application providers) still get some profit from pieces of information that the users choose to make publicly available. Additionally, as Privacy Watch is built as a generic PSNS platform, existing SNS can be modified to follow the architecture of Privacy Watch, albeit with significant code modification. However, this choice is entirely depended on SNS providers.

Privacy Watch currently fulfils most of the required privacy criteria for SNS except for a few that we plan to implement as future work, for instance the *report spam/abuse mechanism* and the *reputation system*. The role of the reputation system is to help the user determine to what extent he can trust a potential friend. With the reputation system, the user will be kept well informed about how many times a potential 'friend' has violated the UPP and how others view and trust this 'friend'.

Another shortcoming of Privacy Watch is that the watermarking methods currently only work with pictures, whereas a large amount of user data on SNS is in a text format. In future work, we intend to tackle the problem of maintaining sovereignty on text data in SNS.

In particular, it would be illusory to hope for an SNS in which no privacy breach can occur because online "friends" can never be fully trusted. Indeed, a so-called "friend" of a user can always save a picture he has accessed to inside the SNS and then post that picture on an external website outside the boundaries of the system. However, with the accountability information and the UPP integrated inside that picture, it is possible to detect and to trace the origin of a privacy breach once it has occurred. Thus, the SNS users are able to claim back their privacy by asking the responsible person to erase this data or by providing evidences to a third party such as the SNS provider or a judge. We believe that individuals would be less inclined to cause a privacy breach, if they know that they might possibly be accountable for it in the future.

Another important issue to consider is the *credibility of evidence* produced by this system in case of litigation. Indeed as cybercrime and data protection regulations differ from country to country, it is a complex task to make the UPP a binding contract and to incorporate all the required data. For instance, after posting a picture of herself "drunken" because of grape juice to share with friends as a joke, Alice may discover at a later date that the picture was used in an advertising campaign against alcohol. Based on the provenance data embedded in the photo Alice could in principle find out that Carol, one of her friends, was the one responsible for disclosing her picture without respecting Alice's privacy requirements. One important question is whether or not this provenance data would be sufficient to convince a judge that Carol violated Alice's UPP and to begin working through an appropriate means of remediation. Overall, privacy comes at a price. However, that price is acceptable as it provides user better protection against the underlying risks in social networking activities.

BIBLIOGRAPHY

[1] Aïmeur, E., Brassard, G., Fernandez, J. M., Onana, F. S. M., and Rakowski, Z. (2008). Experimental demonstration of a hybrid privacy-preserving recommender system. In *Proceedings of the Third International Conference on Availability, Reliability and Security*, ARES'08, pages 161–170, Barcelone.

[2] Aïmeur, E., Brassard, G., and Onana, F. S. M. (2006). Privacy-preserving demographic filtering. In *Proceedings of the 2006 ACM symposium on Applied computing*, SAC'06, pages 872 – 878, Dijon, France.

[3] Aïmeur, E., Gambs, S., and Ho, A. (2009). UPP: user privacy policy for social networking sites. In *Proceedings of the Fourth International Conference on Internet and Web Applications and Services*, ICIW'09, pages 267–272, Los Alamitos, CA, USA. IEEE Computer Society.

[4] Aïmeur, E., Gambs, S., and Ho, A. (2010). Towards a Privacy-Enhanced social networking site. In *Proceedings of the Fifth International Conference on Availability, Reliability and Security*, ARES'10, pages 172–179, Los Alamitos, CA, USA. IEEE Computer Society.

[5] Aïmeur, E., Gambs, S., and Ho, A. (2011). Maintaining sovereignty on personal data in social networking sites. In *Proceedings of International Conference on Privacy and Accountability*, pages 1–8, Berlin, Germany.

[6] Aïmeur, E., Gambs, S., and Ho, A. (2012). A survey of privacy-enhanced social networking sites. *Social Science Computer Review*, submitted.

[7] Aïmeur, E. and Schonfeld, D. (2011). The ultimate invasion of privacy: Identity theft. In *Proceedings of the Ninth Annual International Conference on Privacy, Security and Trust*, PST'11, pages 24–31, Montreal, Canada. IEEE.

[8] Allen, A. (2011). Facebook message warns girl about STD infection. http://www.myfoxspokane.com/news/kcpq-facebook-message-

warns-girl-about-std-infection-20110818,0,925517.story. Published: [online], Last accessed: 1/5/2012.

[9] Anwar, M. and Fong, P. W. L. (2012). A visualization tool for evaluating access control policies in Facebook-style social network systems. In *Proceedings of the 27th Annual ACM Symposium on Applied Computing*, SAC '12, pages 1443–1450, New York, NY, USA. ACM.

[10] Baden, R., Bender, A., Spring, N., Bhattacharjee, B., and Starin, D. (2009). Persona: An online social network with user-defined privacy. *ACM SIGCOMM Computer Communication Review*, 39(4):135–146.

[11] Barnes, J. (1954). Class and committees in a norwegian island parish. *Human Relations*, 7(1):39–58.

[12] Beato, F., Kohlweiss, M., and Wouters, K. (2009). Enforcing access control in social network sites. In *Proceedings of the Second Hot Topics in Privacy Enhancing Technologies*, HotPets'09, pages 1–8, Seatle, USA.

[13] Beato, F., Kohlweiss, M., and Wouters, K. (2011). Scramble! your social network data. In *Proceedings of the Eleventh International conference on Privacy enhancing technologies*, PETS'11, pages 211–225, Berlin, Heidelberg. Springer-Verlag.

[14] Bednall, D., Hirst, A., Ashwin, M., Icoz, O., Hulten, B., and Bednall, T. (2009). Social networking, social harassment and social policy. In *Proceedings of the Conference on Australian and New Zealand Marketing Academy*, ANZMAC'09, pages 1–8, Melbourne, Australia.

[15] Benenson, F. (2009). The official unofficial Creative Commons Facebook application - Creative Commons. http://creativecommons.org/weblog/entry/14563. Published: [online], Last accessed: 1/5/2012.

[16] Bierman, N. (2010). Grieving family by his side, governor signs legislation. http://www.boston.com/news/local/massachusetts/articles/

2010/05/04/grieving_family_by_his_side_governor_signs_legislation/. Published: [online], Last accessed: 8/11/2011.

[17] Bilton, N. (2010). The price of Facebook privacy? Start clicking. http://www.nytimes.com/2010/05/13/technology/personaltech/13basics.html?_r=1. Published: [online], Last accessed:1/8/2010.

[18] Bisaerts, D. (2011). Social networks needs to comply to European privacy laws, says Viviane Reding. http://www.itsecurity.be/social-networks-needs-to-comply-to-european-privacy-laws-says-viviane-reding. Published: [online], Last accessed: 13/11/2011.

[19] Boyd, D. and Ellison, N. (2007). Social network sites: definition, history, and scholarship. *Journal of Computer-Mediated Communication*, 13 (1) article 11.

[20] Bray, T. (2005). RSS 2.0 and Atom 1.0 compared - Atom wiki. http://www.intertwingly.net/wiki/pie/Rss20AndAtom10Compared. Published: [online], Last accessed: 1/5/2012.

[21] Buchanan, T., Paine, C., Joinson, A. N., and Reips, U. (2007). Development of measures of online privacy concern and protection for use on the internet. *Journal of the American Society for Information Science and Technology*, 58(2):157–165.

[22] Buchegger, S., Schiöberg, D., Vu, L. H., and Datta, A. (2009). PeerSoN: P2P social networking - early experiences and insights. In *Proceedings of the Second ACM EuroSys Workshop on Social Network Systems*, SNS'09, pages 46–52, Nuremberg, Germany.

[23] Bulkley, W. M. (2009). Online compliments can haunt you, too. http://blogs.wsj.com/digits/2009/09/18/online-compliments-can-haunt-you-too/. Published: [online], Last accessed: 19/8/2009.

[24] Byers, S., Cranor, L. F., and Kormann, D. (2003). Automated analysis of P3P-enabled web sites. In *Proceedings of the 5th international conference on Electronic commerce*, pages 326 – 338, Pittsburgh, Pennsylvania. ACM.

[25] Carminati, B., Ferrari, E., and Perego, A. (2006). Rule-Based access control for social networks. In *On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops*, pages 1734–1744.

[26] Carroll, M. (2006). Creative commons and the new intermediaries. *Michigan State Law Review*, pages 45–65.

[27] Chaum, D. and Heyst, E. V. (1991). Group signatures. In *Proceedings of the 10th annual international conference on Theory and application of cryptographic techniques*, pages 257–265, Brighton, UK. Springer-Verlag.

[28] Clearinghouse, P. R. (2011). Online privacy: Using the internet safely. `https://www.privacyrights.org/fs/fs18-cyb.htm`. Published: [online], Last accessed: 1/5/2012.

[29] Cohen, R. (2003). Livewire: web sites try to make internet dating less creepy. `http://www.zephoria.org/thoughts/archives/2003/07/05/livewire_web_sites_try_to_make_internet_dating_less_creepy.html`. Published: [online], Last accessed: 1/5/2012.

[30] ComScore (2009). Social networking sites account for more than 20 percent of all U.S. online display ad impressions. `http://www.comscore.com/Press_Events/Press_Releases/2009/9/Social_Networking_Sites_Account_for_More_than_20_Percent_of_All_U.S._Online_Display_Ad_Impressions_According_to_comScore_Ad_Metrix`. Published: [online], Last accessed: 16/8/2009.

[31] Conti, M., Hasani, A., and Crispo, B. (2011). Virtual private social networks. In *Proceedings of the First ACM conference on Data and Application Security and Privacy*, CODASPY'11, pages 39–50, San Antonio, TX, USA.

[32] Cosenza, V. (2011). World map of social networks. `http://vincos.it/world-map-of-social-networks/`. Published: [online], Last accessed: 1/5/2012.

[33] Cranor, L. F. (2002). *Web privacy with P3P*. O'Reilly & Associates.

[34] Cranor, L. F., Guduru, P., and Arjula, M. (2006). User interfaces for privacy agents. *ACM Transactions on Computer-Human Interaction*, 13(2):135–178.

[35] Cutillo, L., Molva, R., and Strufe, T. (2009). Safebook: A Privacy-Preserving online social network leveraging on Real-Life trust. *IEEE Communications Magazine*, page 95.

[36] Dingledine, R., Mathewson, N., and Syverson, P. (2002). Reputation in privacy enhancing technologies. In *Proceedings of the Twelfth annual conference on Computers, Freedom and Privacy*, CFP'02, pages 1–6.

[37] Dwyer, C., Hiltz, S. R., and Passerini, K. (2007). Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. In *Proceedings of the Thirteenth American Conference on Information Systems*, AMCIS'07, pages CD–ROM only, Keystone, Colorado.

[38] Economist (2009). Marketing on social networks: Friends for sale. `http://www.economist.com/businessfinance/displaystory.cfm?story_id=14460087&fsrc=rss`. Published: [online], Last accessed: 19/8/2009.

[39] EPIC and Junkbusters (2000). Pretty poor privacy: an assessment of P3P and internet privacy. Technical report, Electronic Privacy Information Center and Junkbusters.

[40] EuropeanUnion (1995). Directive 95/46/EC of the European parliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[41] Facebook (2012). Facebook IPO 2012: The preliminary prospectus. Technical report.

[42] Fang, L. and LeFevre, K. (2010). Privacy wizards for social networking sites. In *Proceedings of the Nineteenth International Conference on World Wide Web*, WWW'10, pages 351–360, Raleigh, USA.

[43] Feinberg, T. and Robey, N. (2008). Cyberbullying. *Principal Leadership*, 9(1):10–14.

[44] Ferraiolo, D. F., Kuhn, D. R., and Chandramouli, R. (2007). *Role-based access control*. Artech House Publishers.

[45] Fischer, M., Purtell, T., and Lam, M. (2011). Email clients as decentralized social apps in mr. privacy. In *Proceedings of the Fourth Hot Topics in Privacy Enhancing Technologies*, HotPets'11, pages 1–10, Waterloo, Canada.

[46] Freed, L. J. (2011). Parent guide to internet safety. Technical report, Federal Bureau of Investigation.

[47] Freedman, A. (1996). *Computer desktop encyclopedia*. American Management Assoc., Inc.

[48] Furht, B. and Kirovski, D. (2006). *Multimedia watermarking techniques and applications*. Auerbach Publication.

[49] Goble, C. (2002). Position statement: Musings on provenance, workflow workflow and (semantic web) annotations for bioinformatics. In *Proceedings of the Workshop on Data Derivation and Provenance*.

[50] Guha, S., Tang, K., and Francis, P. (2008). NOYB: privacy in online social networks. In *Proceedings of the First Workshop on Online Social Networks*, WOSN'08, pages 49–54, Seattle, WA, USA. ACM.

[51] Gürses, F. S. (2010). *Multilateral Privacy Requirements Analysis in Online Social Network Services*. PhD thesis, Katholieke Universiteit Leuven, Belgium.

[52] Hage, H., Aïmeur, E., and Onana, F. S. M. (2008). Anonymous credentials for privacy-preserving e-learning. In *Proceedings of the International MCETECH Conference on e-Technologies*, MCETECH 08, pages 70–80, Montreal. MCETECH.

[53] Heckathorne, W. (2010). Speak now or forever hold your tweets. Technical report, Harris Interactive.

[54] Ho, A., Maiga, A., and Aimeur, E. (2009). Privacy protection issues in social networking sites. In *Computer Systems and Applications, 2009. AICCSA 2009. IEEE/ACS International Conference on*, pages 271 –278.

[55] Hochheiser, H. (2002). The platform for privacy preference as a social protocol: an examination within the U.S. policy context. *ACM Transactions on Internet Technology (TOIT)*, 2(4):276 – 306.

[56] Huggins, M. (2007). A definitive list of social networking websites to help you succeed. `http://www.matthuggins.com/a-definitive-list-of-social-networking-websites-to-help-you-succeed/`. Published: [online], Last accessed: 16/9/2009.

[57] Indratmo and Vassileva, J. (2007). A usability study of an access control system for group blogs. In *Proceedings of the International Conference on Weblogs and Social Media, Boulder*, pages 1–4.

[58] Ivan, A. and Dodis, Y. (2003). Proxy cryptography revisited. In *Proceedings of the Network and Distributed System Security Symposium (NDSS)*.

[59] Jackson, B. (2010). Facebook class-action lawsuit involves nearly half of all canadians. `http://www.itbusiness.ca/it/client/en/home/News.asp?id=58238&PageMem=3`. Published: [online], Last accessed: 29/7/2010.

[60] Javelin (2011). 2011 identity fraud survey report. Technical report, Javelin Strategy & Research.

[61] Kang, T. and Kagal, L. (2010). Enabling Privacy-Awareness in social networks. In *Intelligent Information Privacy Management Symposium at the AAAI Spring Symposium*, volume 2010.

[62] Kemp, S. (2011). Social, digital and mobile in china. `http://wearesocial.sg/blog/2011/12/social-digital-mobile-china/`. Published: [online], Last accessed: 1/5/2012.

[63] Kornblum, J. and Marklein, M. B. (2006). What you say online could haunt you. `http://www.usatoday.com/tech/news/internetprivacy/2006-03-08-facebook-myspace_x.htm`. Published: [online], Last accessed: 16/8/2009.

[64] Krasnova, H., Günther, O., Spiekermann, S., and Koroleva, K. (2009). Privacy concerns and identity in online social networks. *Identity in the Information Society*, 2(1):39–63.

[65] Lake, C. (2007). Quechup launches worldwide spam campaign. `http://www.e-consultancy.com/news-blog/364182/social-network-launches-worldwide-spam-campaign.html`. Published: [online], Last accessed: 16/9/2009.

[66] Laycock, J. (2008). Are your social networking connections hurting your reputation? `http://www.searchengineguide.com/jennifer-laycock/are-your-social-networking-connections-h.php`. Published: [online], Last accessed: 16/8/2009.

[67] Loupasakis, A., Ntarmos, N., and Triantafillou, P. (2011). eXO: Decentralized autonomous scalable social networking. In *Proceedings of the Fifth Biennial Conference on Innovative Data Systems Research*, CIDR'11, pages 85–95, Asilomar, USA.

[68] Lucas, M. M. and Borisov, N. (2008). FlyByNight: mitigating the privacy risks of social networking. In *Proceedings of the Seventh ACM Workshop on Privacy in the electronic society*, WPES'08, pages 1–8, New York, NY, USA. ACM.

[69] Luo, W., Xie, Q., and Hengartner, U. (2009). FaceCloak: an architecture for user privacy on social networking sites. In *Proceedings of the IEEE International Conference on Privacy, Security, Risk and Trust*, PASSAT'09, pages 26–33.

[70] Madden, K. (2010). 12 ways to get fired for Facebook. http://msn.careerbuilder.com/Article/MSN-2349-Workplace-Issues-12-Ways-to-Get-Fired-for-Facebook/?sc_extcmp=JS_2349_home1&SiteId=cbmsnhp42349&ArticleID=2349&gt1=23000&cbRecursionCnt=1&cbsid=7c931356ceb748d798d9f2ff4919c8e2-336657052-RE-4. Published: [online], Last accessed: 9/2/2011.

[71] Madden, M. and Smith, A. (2010). Reputation management and social media. Technical report, Pew Research Center's Internet & American Life Project.

[72] McCallister, E., Grance, T., and Scarfone, K. (2010). Guide to protecting the confidentiality of personally identifiable information. Technical Report NIST Special Publication 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information.

[73] Nations, D. (2007). The top social networking sites. http://webtrends.about.com/od/socialnetworking/a/social_network.htm. Published: [online], Last accessed: 1/5/2012.

[74] Nemati, H. (2008). *Information security and ethics: concepts, methodologies, tools, and applications*. Idea Group Reference.

[75] NIST (2000). Commerce department announces winner of global information security competition. http://www.nist.gov/public_affairs/releases/g00-176.cfm. Published: [online], Last accessed: 1/5/2012.

[76] Ofcom (2008). Social networking: A quantitative and qualitative research report into attitudes, behaviours and use. Technical report, Office of Communications of United Kingdom.

[77] O'Neill, M. (2012). What happens to your digital life when you die? http://socialtimes.com/what-happens-to-your-digital-life-when-you-die-video_b88686. Published: [online], Last accessed: 1/5/2012.

[78] Opsahl, K. (2010). A bill of privacy rights for social network users. https://www.eff.org/deeplinks/2010/05/bill-privacy-rights-social-network-users. Published: [online], Last accessed: 13/11/2011.

[79] Paul, I. (2012). Girls around me app voluntarily pulled after privacy backlash. http://www.pcworld.com/article/252996/girls_around_me_app_voluntarily_pulled_after_privacy_backlash.html. Published: [online], Last accessed: 1/5/2012.

[80] Paul, T., Buchegger, S., and Strufe, T. (2011). Decentralized social networking services. In *Trustworthy Internet*, pages 187–199. Springer Milan, Milano.

[81] Prashanth (2010). Top 10 reverse image search engines. http://www.comptalks.com/top-10-reverse-image-search-engines/. Published: [online], Last accessed: 1/5/2012.

[82] ProvenSEO (2011). Breaking Google+ privacies through "Re-share" function. http://www.provenseo.com/2011/07/breaking-google-privacies-through-re-share-function/. Published: [online], Last accessed: 8/10/2011.

[83] Roos, D. (2007). How online social networks work. http://communication.howstuffworks.com/how-online-social-networks-work.htm. Published: [online], Last accessed: 1/5/2012.

[84] Seitz, J. (2005). *Digital watermarking for digital media.* Information Science Publishing.

[85] Seong, S., Seo, J., Nasielski, M., Sengupta, D., Hangal, S., Teh, S. K., Chu, R., Dodson, B., and Lam, M. S. (2010). PrPl: a decentralized social networking infrastructure. In *Proceedings of the First ACM Workshop on Mobile Cloud Computing & Services: Social Networks and Beyond*, MCS'10, pages 1–8, San Francisco, California. ACM.

[86] Shakimov, A., Lim, H., Caceres, R., Cox, L. P., Li, K., Liu, D., and Varshavsky, A. (2011). Vis-à-Vis: privacy-preserving online social networking via virtual individual servers. In *Proceedings of the Third International Conference on Communication Systems and Networks*, COMSNETS'11, pages 1–10, Bangalore. IEEE.

[87] Shamir, A. (1985). Identity-based cryptosystems and signature schemes. In *Advances in Cryptology - CRYPTO '84*, volume 196, pages 47 – 53. Berlin: Springer Verlag.

[88] Sharma, D. (2007). Social networking god: 350+ social networking sites. `http://mashable.com/2007/10/23/social-networking-god/`. Published: [online], Last accessed: 1/5/2012.

[89] Sharma, R. and Datta, A. (2011). SuperNova: super-peers based architecture for decentralized online social networks. *ArXiv e-prints*.

[90] Shoemaker, C. (2002). Hidden bits: a survey of techniques for digital watermarking. `http://www.vu.union.edu/~shoemakc/watermarking/watermarking.html`. Published: [online], Last accessed: 1/5/2012.

[91] Siegel+Gale (2012). Survey finds Facebook and Google privacy policies even more confusing than credit card bills and government notices. *MarketWatch*.

[92] Sophos (2011). Security threat report: 2011. Technical report, Sophos.

[93] Squicciarini, A. C. and Sundareswaran, S. (2009). Web-Traveler policies for images on social networks. *World Wide Web*, 12(4):461–484.

[94] Stevens, T. (2009). Teacher suspended for gun pictures on Facebook. http://www.switched.com/2009/02/06/teacher-suspended-for-facebook-gun-pictures/. Published: [online], Last accessed: 27/8/2009.

[95] Stickney, R. (2010). Hospital will fire workers in Facebook scandal. http://www.nbcsandiego.com/news/health/Hospital-Fires-Emps-in-Facebook-Scandal-95794764.html. Published: [online], Last accessed: 9/2/2011.

[96] Swallow, E. (2011). How recruiters use social networks to screen candidates. http://mashable.com/2011/10/23/how-recruiters-use-social-networks-to-screen-candidates-infographic/. Published: [online], Last accessed: 13/11/2011.

[97] Tootoonchian, A., Saroiu, S., Ganjali, Y., and Wolman, A. (2009). Lockr: Better privacy for social networks. In *Proceedings of the Fifth International conference on Emerging networking experiments and technologies*, CoNEXT'09, pages 169–180, Rome, Italy. ACM.

[98] UCAN, P. R. C. . (2011). Social networking privacy: How to be safe, secure and social. https://www.privacyrights.org/social-networking-privacy. Published: [online], Last accessed: 1/5/2012.

[99] Valdes, M. and McFarland, S. (2012). Job seekers get asked to provide Facebook logins. http://www.globalnews.ca/Canada/job+seekers+get+asked+to+provide+facebook+logins/6442604067/story.html. Published: [online], Last accessed: 1/5/2012.

[100] VisionCritical (2010). Online social network: Trust not included. Technical report, Vision Critical.

[101] Wang, Y. and Vassileva, J. (2009). A User-Centric authentication and privacy con-

trol mechanism for user model interoperability in social networking sites. *Adaptation and Personalization for Web 2.0*, pages 110–119.

[102] Weitzner, D. J., Hendler, J., Berners-lee, T., Connolly, D., Ferrari, E., and Thuraisingham, B. (2005). Creating the policy-aware web: Discretionary, rules-based access for the World Wide Web. In *Web and Information Security*. IRM Press.

[103] Whitehouse, A. (2010). How to protect photos online. `http://www.guardian.co.uk/technology/askjack/2010/oct/14/protect-photos-online`. Published: [online], Last accessed: 1/5/2012.

[104] Winfrey, L. (2011). Google plus accounts being deleted in bulk, taking the rest of your google accounts with them. `http://zoknowsgaming.com/2011/07/25/google-accounts-deleted-bulk-rest-google-accounts/`. Published: [online], Last accessed: 7/10/2011.

[105] Ybarra, M. L. and Mitchell, K. J. (2008). How risky are social networking sites? A comparison of places online where youth sexual solicitation and harassment occurs. Technical report.