Literature Overview - Privacy in Online Social Networks

Michael Beye[1], Arjan Jeckmans[2], Zekeriya Erkin[1], Pieter Hartel[2], Reginald Lagendijk[1] and Qiang Tang[2]

[1] Information Security and Privacy Lab, Faculty of EEMCS, Delft University of Technology
[2] Distributed and Embedded Security, Faculty of EEMCS, University of Twente

Abstract. In recent years, Online Social Networks (OSNs) have become an important part of daily life for many. Users build explicit networks to represent their social relationships, either existing or new. Users also often upload and share a plethora of information related to their personal lives. The potential privacy risks of such behavior are often underestimated or ignored. For example, users often disclose personal information to a larger audience than intended. Users may even post information about others without their consent. A lack of experience and awareness in users, as well as proper tools and design of the OSNs, perpetuate the situation.
This paper aims to provide insight into such privacy issues and looks at OSNs, their associated privacy risks, and existing research into solutions. The final goal is to help identify the research directions for the Kindred Spirits project.

Keywords: Online Social Networks, privacy

1 Introduction

In recent years, Online Social Networks (OSNs) have seen significant growth and are receiving much attention in research. Social Networks have always been an important part of daily life, but now that more and more people are connected to the Internet, their online counterparts are fulfilling an increasingly important role.

Aside from creating an actual network of social links, many OSNs allow their users to upload multimedia content, communicate in various ways and share many aspects of their lives. Because of the public nature of many social networks and the Internet itself, content can easily be disclosed to a wider audience than the user intended. Limited experience and awareness of users, as well as the lack of proper tools and design of the OSNs, do not help the situation. We feel that users are entitled to at least the same level of privacy in OSNs, that they enjoy in real-life interactions. Users should be able to trade some information for functionality without that information becoming available beyond the intended scope. For example, a user of a self-help OSN like PatientsLikeMe, who suffers from a given medical condition might not want everyone to know about this, but at the same time the user would like to meet people with the same condition. This is the context of the Kindred Spirits project, and its aim is to provide users the ability to meet and interact with other (similar) people, while preserving their privacy.

This paper aims to provide insight into privacy issues and needs faced by users of OSNs and their origins. The insights gained help plot a course for future work. To this

end, we look at OSNs as they currently exist (Section 2), the associated privacy risks (Section 3), and existing research into solutions (Section 4). The ultimate goal is to identify open topics in research through reflection on existing proposals (Section 5).

2 Online Social Networks

Let us begin by framing the concept of Online Social Networks, and observe why OSNs are as widely used as they are today. This will help us understand the needs of OSN users, the environments they navigate, and potential threats as discussed in further sections.

2.1 Definition of OSNs

Boyd and Ellison's widely used definition [6] captures the key elements of any OSN:

Definition 1. *An OSN is a web-based service that allows individuals to:*

1. *construct a public or semi-public profile within the service,*
2. *articulate a list of other users with whom they share a connection,*
3. *view and traverse their list of connections and those made by others within the service.*

The list of other users with whom a connection is shared is not limited to connections like friend (Facebook, MySpace) or relative (Geni), but also includes connections like follower (Twitter), professional (LinkedIn) or subscriber (YouTube).

2.2 The Rise of OSNs

The first OSN to see the light of day was SixDegrees in 1997. SixDegrees allowed users to create profiles, list and message their friends and traverse friends listings, thus fitting the definition above. Even though there were millions of users, users did not have that many direct friends and SixDegrees did not offer much functionality besides messaging. The website finally shut down in 2000 [6].

During and after this period other websites started adding OSN features to their existing content, essentially becoming OSNs, with various degrees of success. In the years that followed, new OSNs started from scratch and began to offer functionality beyond simply listing and browsing friends. Ryze and later LinkedIn tailored to professionals looking to exchange business contacts, while Friendster focussed on dating and finding new friends. Friendster became a mainstream OSN and was experiencing technical (performance and hardware) and social (fake profiles and friendship hoarding) difficulties because of its rapid growth. The technical difficulties and actions to combat the social difficulties eventually led to users moving to other OSNs. Despite this, Friendster is still popular, particularly in the Phillipines, Indonesia and Myanmar [46].

The popularity of Friendster encouraged the creation of other similar OSNs, like MySpace and Orkut. While Myspace has become popular among youth worldwide, Google's Orkut has attracted a predominantly Brazilian and Indian crowd [46]. Aside

from these clearcut "social OSNs", a wide variety of niche OSNs have emerged, each catering to a particular taste (see Section 2.4). Adding the social structure of an OSN can often enrich the underlying services, making them more useful and attractive to users, or binding users to providers. Currently OSNs are an integral part of the internet.

2.3 Data in OSNs

Boyd and Ellison's definition already suggests that OSNs operate on two types of user-related data:

Profiles. A profile is tied to a user and is their representation to the outside world. Usually this is a self description, or the description of an alter-ego (pseudonym, avatar).

Connections. A connection exists between two users and can be of several types, like friend, colleague, fan, etc. A collection of connections can be represented by a graph.

However, depending on the types of additional services the OSN offers, other forms of information related to users are often involved:

Messages. Messages in the broadest sense of the word. Any piece of data that is exchanged between a user and another user or a group of users, which may contain multi-media. This is the basis for additional OSN functionalities. Interaction between users has been recognized as a rich source of information on the underlying social network, even more so than friendship graphs [29].

Multi-media. Pieces of information that can be sent between users, but may also be uploaded to private or public data-spaces (e.g. photo album, blog, Facebook "Wall"). Examples are blog entries (text), photos (pictures), music or voice recordings (audio) and movie clips (video).

Tags. A tag can be defined as a keyword (meta-data) attached to content, by a user (either the uploader or other users). In Facebook terminology, 'tagging' refers to the specific case where a user identifies the people depicted in a photo, and tags the photo with their names, thus explicitly linking these people to the picture.

Preferences. Many OSNs provide their users with some type of matching or recommendation functionality for either content or peers. Often, users explicitly specify preferences, which may or may not be publicly visible. Sometimes, preferences are derived implictly from user behaviour.

Groups. A collection of users. Usually groups also share some resource, attributes or privileges, for example: a collaborative document, common preferences or backgrounds, or access to a common space.

Behavioral information. Browsing history and actions undertaken by the user while performing tasks within the OSN. Benevenuto et al. note that this type of meta-data is particularly rich [5]. Information such as preferences, friendships or even implicit data such as physical location can be inferred from it. Behavioral data is also found in traditional websites, although behavior there is not related to navigating a social network.

Login credentials. Most OSNs require, or allow, the user to login to make use of the service. This login information is contained in the login credentials. This is something that can also be found in traditional websites.

As said, not all OSNs involve information from all of the above categories. This mostly depends on the media-richness of a particular OSN, the functionality it offers to users, and its business model. Some information is only available to the OSN (i.e. its software or operators), while other information is also available to (a subset of) the OSN users. Furthermore some information is implicitly supplied to the OSN, by actions taken within the OSN, while other information is explicitly supplied, by providing this information.

2.4 Types of OSNs

Hardly any classifications for OSNs exist in scientific literature, although some pseudo-scientific blogs and marketing resources offer relevant thoughts on the matter. Some sources look at topical focus [37,48], others at topical specificity (or breadth of the user base) [35,49]. Yet other sources classify OSNs based on the openness of the network [42], or the type of networking that goes on [36,38,39].

In the following section we will attempt to structure our understanding of what OSNs mean to their users. We will look at the purpose or functionality that an OSN aims to offer to its user base. Examples of OSNs are given and these are named by the way they advertise themselves, some explicitly add .com. A broad distinction can be made between OSNs that focus on connections and those that focus on content.

Connection OSNs Connection OSNs focus more on the connections users have and exploit this mainly by (re-)connecting users and by providing a social contact book.

Dating. Dating sites are websites that aim to help users find the love of their life, many of which incorporate OSN aspects these days. Each user has login credentials and usually a profile to attract potential lovers. Connections are typically in the form of love interests, but friendship links are also common; groups may also exist. Traversing the OSN is often based on searching or recommendations rather than through navigating existing connections. Messages exchanged between users are often kept private to these users, although in some cases comment sections, viewable by connections, are offered. Behavioral information can be kept by the OSN to provide better recommendations. Examples are PAIQ, Match.com and Plentyoffish.com.

Business. These OSNs aim to provide professionals with useful business contacts. Searching for profiles does not always require signing up. Profiles display a users capabilities and work field as well as a means to contact that user. This is usually done through the OSN via messages. Users can also add other users to their network (connection) so that other professionals can see who the user is working or has contact with. An example of this class is LinkedIn, which requires a subscription for premium services.

Enforcing real-life relationships. These OSNs are not aimed at finding new friends, but (re)connecting with existing friends or acquaintances. Examples include family-oriented OSNs, college or ex-classmate focussed networks, such as MyLife, Oddnoklassniki and Plaxo.

Socializing. Fitting the more traditional view of social networks. Here users can connect with current friends and find new ones. All types of information found in an OSN are also found in this class, often a lot of this information is public. The revenue for the OSN provider often comes from advertisements and selling information about the OSN, but can sometimes be combined with a subscription for additional functionalities (as with Hyves). In order to attract and keep users this type of OSN usually has a lot of additional functionalities such as social and competitive games. For a user the value of such an OSN is often largely determined by the number of friends on the OSN. Some wellknown examples of this class are Hyves, Facebook, Orkut and MySpace.

Content OSNs Content OSNs focus more on the content provided or linked to by users.

Content sharing. Sharing of user-generated content can happen within a selected group, such as friends or family, or a far wider audience. Content that is shared is usually multimedia, because this is too big to e-mail to all parties involved. Uploading content most often requires users to sign up and log in; sometimes viewing content also requires logging in, or knowledge of a hard-to-guess obfuscated URL. Sometimes messages or tags can be added to the shared content, and especially in more open systems, content recommendation may be an integral part of the system. User profiles, if any, are usually brief. Examples are Picasa and Photobucket.

Content recommendation. In some cases users do not upload (multi-medial) content, but focus more on recommending existing (usually professional) content. Book-review sites like WeRead.com, and URL-tagging communities like Delicious are prime examples where content is discovered and tagged or rated, but not created or uploaded.

Entertainment These OSNs are tied to a gaming community. The profile usually depicts a gaming avatar and connections to gaming friends. Messages can be passed to other users and sometimes groups can be formed. Behavioral information is mostly used to track games played and achievements unlocked within these games, this information is then displayed on the profile. Entertainment OSNs might make money by selling games and game add-ons, or through subscriptions. Examples are Xbox Live and Playfire.

Advice sharing. Offering a place for people to share their experience or expertise in a certain area with others, or to seek help and advice can be a focus for some OSNs. For example mothers-to-be (BabyCenter), medical patients (PatientsLikeMe) or students (TeachStreet) can help one another. Other examples include Advogato, the now discontinued Cake Financial and ScienceStage.

Hobbies. Many OSNs focus on audiences that have similar interests and hobbies. This may involve recommendation and advice sharing elements, but the main difference

is that the audience is more homogenous and the topic of the OSN mainly makes up its character and appeal. Examples are AthLinks and Care2.

"News" sharing. Blog-related OSNs, or ones that focus on world news or gossip. Examples are Buurtlink.nl, Twitter, Blogster and GossipReport.com.

← OSN types	Data types →	Profiles	Connections	Messages	Multi-media	Tags	Preferences	Groups	Behavioral information	Login credentials
Connection OSNs	Dating	●	•	●	•	·	●	•	●	●
	Business	●	●	●	•	·	•	●	●	●
	Enforcing real-life relationships	●	●	●	•	·	•	●	●	●
	Socializing	●	●	●	•	·	•	●	●	●
Content OSNs	Content sharing	•	•	●	●	●	•	•	●	●
	Content recommendation	●	·	•	●	●	●	•	●	●
	Entertainment	•	•	●	●	•	●	●	●	●
	Advice sharing	●	•	●	•	•	•	●	●	●
	Hobbies	•	•	●	•	•	•	●	●	●
	"News" sharing	•	•	●	●	•	•	•	●	●

Table 1. Data types typically found in different types of OSN.

2.5 Summary

Users can have different reasons to use an OSN. In any case, to get the desired functionality (recommendations, attracting an audience, getting advice, etc.), they will need to provide some information to the OSN. The type of user data in question depends on the functionality of the OSN, and its media-richness. Table 1 gives an impression of which combinations may typically be expected. In this table ● represents likely, • represents possible and · unlikely

Due to the tradeoff between functionality and privacy, the potential sensitivity of data and the open nature of online systems, privacy is definitely an issue.

3 Privacy in OSN Literature

Making sure the OSN can perform desired behavior is one thing, but when sharing a wealth of (personal) data, one should also consider what *undesired* behavior might take place. In this section, we will look into privacy, its role in OSNs, and potential threats

to users' privacy.

The word privacy has many subtly different meanings, ranging from personal privacy (which includes seclusion and bodily privacy) to information privacy, each with their own definition. Privacy on the Web in general revolves mostly around *Information Privacy*, as defined below in the IITF wording that Kang uses [15]:

> Information Privacy is "an individual's claim to control the terms under which personal information–information identifiable to the individual–is acquired, disclosed or used."

In a Web2.0 setting, where users collaborate and share information, privacy of personal information becomes very relevant. In OSNs, users have a scope in mind when they upload information (see Palen and Dourish' classification below). Privacy involves keeping information in its intended scope. Such a scope is defined by the size of the audience (breadth), by extent of usage allowed (depth), and duration (lifetime). When information is moved beyond its intended scope (be it accidentally or maliciously), privacy is breached. A breach can occur when information is shared with a party for whom it was not intended (disclosure). It can also happen when information is abused for a different purpose than was intended, or when information is accessed after its intended lifetime. We also see this reflected in data protection laws, such as the Data Protection Act 1998 in the United Kingdom [33], where limitations are imposed to the extent and duration of use of personal data.

Palen and Dourish [23] classify three privacy boundaries with which individuals are struggling.

1. The disclosure boundary (managing the tension between private and public),
2. The identity boundary (managing self representation with specific audience, e.g. one will behave differently at work than when among friends),
3. The temporal boundary (managing past actions with future expectations; user behavior may change over time).

Weiss [30] compares the traditional approach to privacy with the new privacy demands created by OSNs. In the traditional Web, privacy is maintained by limiting data collection, hiding users' identities and only granting access to authorized parties. The reality of OSNs is that data and identity are closely linked, and often visible to large groups of people. This makes privacy and information management a lot harder and gives rise to privacy issues as discussed further on in this section. Within an OSN privacy is the balancing act between control over information and performance of OSN functionalities. With more user information becoming available online it is harder for a user to monitor and control this.

Most social networks offer privacy settings that are simple to use, but coarse. They often require the user to set the visibility for each profile item to either private, friends-only, or public. Sometimes a few more options are given. In the end it boils down to a list of items and check boxes to either opt-in or opt-out of disclosing these items to certain

groups, limiting user control. Gross and Acquisti [13] show in a case study that most users do not change the default privacy settings as provided by the OSN. Furthermore these users share a large amount of information on their profile. Tufecki [27] concludes in his case study that privacy-aware users are more reluctant to join social networks. However once a privacy aware user joins he is willing to disclose a lot of information and a user's privacy is regulated mostly through visibility, i.e. the privacy settings of the OSN. This privacy aware user aims to remain in control. Furthermore users are more pre-occupied with the current visibility of their information and do not look towards future implications. It seems that users implicitly trust social network providers to handle user data in a fair and conscientious way.

Currently there are no specific regulations for OSNs and they are treated as an information service, an online database of information. The EU article 29 data protection working party [28] would like to see this changed, so that OSN service providers are treated as data controllers under the data protection directive. This will impose additional obligations when processing user data. Adhering to these obligations should make OSNs more privacy friendly, ideally without hampering the services offered to the users.

3.1 Protection from users vs. protection from providers

In short, we can distinguish two main classes of privacy threats: those that involve disclosure to other "users" (registered or not), and those that originate from the OSN service provider's side. The main difference between these parties is the type of information they can access. A user or outsider can generally only view public information. The OSN provider can usually view *all* data in the system, including private uploads, browsing behaviour, IP adresses, etc. Trust plays a big role in the relationship between a user and the service provider.

Because the type of access differs greatly, both categories of threats require their own specific defense mechanisms. To protect user data from fellow users, awareness and proper tools for managing and enforcing access policies play a leading role [2,9,17]. This does not work towards solving issues that involve untrusted service providers. Obscuring and hiding sensitive data from the providers [1,14,26], or removing them from the picture entirely [7,8,25] are the general approaches here, as we will see in the next section.

3.2 User-related privacy issues

In many cases, privacy is breached by fellow OSN users, or unregistered visitors. This may be intentional (snooping, hacking), or accidental (mismanagement of privacy settings by the user, lingering data), and can have serious consequences. Let us take a look at different privacy threats that involve disclosure to other users.

Stranger Views Private Information Users can falsely assume some information to be kept private, when in reality it is not. This can be due to design flaws on the part of the OSN service provider (e.g. private photos, videos and blogs being hacked on

Myspace [41]), or a lack of understanding or attention of the user himself to the privacy controls. Also, it could stem from data retention problems, where a resource may be deleted or disabled, but references to it (thumbnails, messages on friends' pages etc.) remain visible to the outside world. When a stranger views such private information, this is in conflict with the *disclosure boundary*. The user has lost control over to whom his information is disclosed. Issues such as this are related to your profile, connections to fellow users, messages, multi-media, tags or group memberships. Rosenblum [24] shows that information in OSNs is far more accessible to a widespread audience than perceived by its owners, and can even end up in the media [40]. Even internet security experts can make mistakes with disclosing information [51].

Unable to Hide Information from a Specific Friend or Group Sometimes you would like to hide some information from a specific friend or a group of friends. Perhaps you would not like to let a friend know that you are planning a surprise party for his birthday, or hide the pictures of your night out from your parents. In real life, we easily manage the different social contexts that we belong to, but in OSN's the lines that seperate them tend to blur [17]. Not all OSNs supply the option to hide information on such a fine-grained level. This problem is related to Palen and Dourish' *identity boundary* as users do not have the control to act differently towards one user or group of users, than towards others.

Other Users Posting Information About You While you can control what information you want to post to an OSN, you have no control over what other users post in the same OSN. Often, messages contain information about multiple users in the OSN. This problem is related to the *disclosure boundary*, because information is made more public than intended. It can occur when another user posts information about you which you do not want to be uploaded to the OSN, or when information disclosed privately to another user is made available to a larger audience. This can even be a deliberate act [47].

3.3 Provider-related Privacy Issues

A completely different type of privacy threat involves the relationship between the user and OSN provider, and in particular the trust that the user puts into the provider. This goes beyond user control of information, because the provider usually designed or configured the systems underlying the OSN. Thus the provider has full access to any user-related data, including browsing behaviour and message logs. The associated threats are detailed below.

Data Retention When posting information to an OSN it is often impossible or very difficult to remove that information. Facebook for example does not provide users with the means to delete their profile, and has actively blocked third-party software that attempts to remedy this [43]. Even data that is apparently erased still resides elsewhere on the OSN, for example in backups, to be found by others. This is a violation of the

temporal boundary as information is available longer than intended. An example of this is given by Bonneau [34] who tracked the availability of deleted photos. Also Facebook would like to store content forever [50].

OSN Employee Browsing Private Information The OSN provider has full access to the data and an employee of the OSN provider might take advantage of this. This is in conflict with the implicit trust that is required in the OSN. All information supplied to the OSN is at risk in this issue, up to and including behavioral information. Interviews suggest that some Facebook employees can view user information and it is left to the company to police this [45].

Selling of Data The wealth of information that is stored on the OSN, is likely to be of value to third parties and may be sold by the OSN. User preferences, behaviour and friendship connections can all be interesting for marketing purposes and research into social dynamics. Data sales can easily be in conflict with the implicit trust the user has in the OSN. One example of an OSN that provides user data to third parties is PatientsLikeMe. To quote their website:

> "PatientsLikeMe offers pharmaceutical companies the opportunity to reach and learn from thousands of patients with chronic diseases. Follow their symptoms, treatments, outcomes and attitudes. Evaluate real-world safety and efficacy data, and conduct targeted clinical trial recruitment. These are just a few examples of how our portfolio of services drives value at each stage of the drug development process."

Targeted Marketing Multiple pieces of information in the OSN can be combined to provide a high value profile of the user. This high value profile can then be used or exploited to present targeted marketing to the user. This again is a conflict of the implicit trust the OSN has, as information is used in a different manner than as intended by the user. An example of a company which uses OSN data for targeted marketing is TrustFuse [44].

> "All of this information could come in handy for Rapleaf's third business, TrustFuse, which sells data (but not e-mail addresses) to marketers so they can better target customers, according to TrustFuse's Web site"

3.4 Summary

Because OSNs contain massive amounts of useful and interesting data about large numbers of users, they form an interesting target for third parties, both private and commercial. Either through browsing/spidering, hacking attacks or simple data-sales, this information could end up in the wrong hands. The fact that the users are not always the source of revenue for an OSN (in the case of advertisement revenue and data sales), can lead to conflicting interests for users and providers. Given the diverse and often extensive information available on OSNs, and the fact that threats may come from other

users or even the service provider itself, the threats are myriad. Table 2 attempts to give a comprehensive overview. Concern in this table is high (●), medium (•), or low (·). Despite the fact that prevention of these threats is no simple matter, many research areas in existing literature focus on alleviating some of the aforementioned threats.

← Privacy concerns	Data types →	Profiles	Connections	Messages	Multi-media	Tags	Preferences	Groups	Behavioral information	Login credentials
User related	Stranger views private info	●	●	●	●	•	●	●	•	·
	Unable to hide info from specific friend / group	●	●	●	●	•	·	·	·	·
	Other users posting information about you	·	·	●	●	●	·	·	·	·
Provider related	Data retention	●	●	●	●	●	●	●	●	·
	OSN employee browsing private info	●	●	●	●	●	●	●	●	•
	Selling of data	●	●	●	●	·	●	·	●	·
	Targeted marketing	●	·	·	·	·	●	·	●	·

Table 2. Privacy concerns for user data in OSNs.

4 Existing Research

In this section we will see what research has been done to mitigate privacy issues and tailor to the privacy needs of users.

4.1 Anonymization

As pointed out in Sections 2 and 3.3, sales of information pertaining to the OSN is often a major source of revenue for the service provider. If this were to be done without any further consideration for privacy, users might take offense (leaving the network, thus hurting revenue), or take justified legal action. Through *anonymization*, OSN providers may try to remove the privacy issues associated with data sales, by *obscuring the link between users and data sold*.

Basic anonymization simply removes any identifying or identifiable information from the data. However, different re-identification attacks [3] can be mounted to fill in the missing info from the data sold, e.g. by exploiting the structure of the network. More thorough anonymization techniques have been proposed, for example mixing attributes, or modifying the graph structure in such a way that its properties stay mainly intact, while making re-identification hard or impossible [31]. Zhou et al. [32] give a good overview of this field and its problems. Recently the field of anonymization is

shifting towards differential privacy [10], which aims to make users in released data computationally indistinguishable from most of the other users in that data set.

These anonymization techniques are usually simple to implement, and need to be performed only once on a given snapshot of the OSN before sales to third parties. The drawback is that it is hard to *prove* these methods to be secure, as opposed to classical cryptographic operations. This mainly stems from the fact that information is partially hidden or obfuscated, but other parts must remain intact to be interesting for after-sale use. Because OSNs are such complex systems, it is nearly impossible to predict which additional information may become available to attackers. This makes it hard to prevent data from being combined to retrieve part of the private information that was obscured through anonymization.

4.2 Decentralization

Decentralization research in OSNs revolves around the assumption of untrusted OSN service providers, and tries to remove the issues in which implicit trust in the OSN is abused. Decentralization can happen to different degrees. An example with slight decentralization would be to give users a direct link to one another for chatting. In this way the chat data never passes through the server. An extreme case would be removing the OSN alltogether and have all traffic take place through peer-to-peer networks. Generally the more decentralized the solution the better the protection from aforementioned privacy issues. Buchegger and Datta [7] list the possible advantages and challenges for shifting to a decentralized OSN. A major obstacle is that all users will be made responsible for availability of information; either the user should be online or peers or a trusted proxy should keep data available on their behalf. Another of the main challenges in this area of research lies in version control. Given the churn of users and the rate at which data is updated, these are not simple problems to overcome in decentralized OSNs.

Tootoonchian et al. [26] propose to decouple social relationships from the social data. Social data will still reside on social networks but the relationships will be in the form of attestations. An attestation can prove to an OSN that two users have a social relationship. These attestation can then be used for access control and do not require the user to sign up for every social network.

Freedman and Nicolosi [11] propose a method for verifying social proximity (friend of a friend) and give the list of bridging friends to one of the parties. In this scheme one of the parties looks forward, while the other looks backwards. With both using a one-way transform, one party compares these relationships. In this directional scheme, the party that is the target of the friend relationship has to consent. This party also has to give up more of his privacy, he sends out a key and receives an attestation. Considering that this party is not the initiator of the relationship this is a skewed trade-off.

Mezzour et al. [21] propose another method which works for longer paths. This method works by using a token flooding phase in which tokens are spread throughout the social graph. The user whom first sent these tokens can use a look-up to discover the path between him and the other user. Revocation of any of the relationships in the flooded path would require another flooding phase.

A decentralized structure works strongly towards taking power away from the OSN service provider, thus reducing the trust issue. Also, scalability in decentralized solu-

tions is often good. However, the structure must take into account untrusted peers. Also, decentralization seems contrary to the business model of many OSN service providers. The biggest problem may lie in the technical feasibility of a fully decentralized OSN. Providing data availability and integrity is hard in this setting, because of the churn of both users and their data.

4.3 Privacy Settings and Management

The research in this field is devoted to finding methods to either give the user more control over their privacy settings, or make it easier for the user to manage such settings. In doing so, privacy settings and management research hopes to mitigate the problems of unauthorized data access by users and the inability of users to hide information from a specific friend or group.

Baatarjav et al. [2] propose a system that selects privacy settings according to some basic profile information. This profile information is used to predict expected user preferences, based on statistical data. Banks and Wu [4] propose using interaction history to facilitate privacy settings between users, using trust as a currency. This proposal has not been worked out in detail.

Another approach is suggested by Maximilien et al. [20], where a privacy score based on the sensitivity and visibility of profile items is computed. This privacy score can then be compared among peers, and the privacy settings of peers can be mimicked if needed. Goecks et al. [12] have created an overview of the challenges and problems of configuring privacy settings based on such collaboration. Most notable is *information cascade*, which is a snowball effect that can lead to the adoption of unwanted privacy settings by many users. Because this process increases the score of the unwanted configuration, this eventually leads to herding behaviour where all users share the same unwanted setting. In an extension of their system, they add an "expert set" of advanced users that has higher priority over regular users.

Development of solutions to provide gradual and fine-grained and transparent information disclosure and privacy settings adjustment forms an interesting research topic. The central question in this area of research is how to give the user appropriate tools for such fine-grained control, without overburdening the user or the system.

User awareness of privacy can be enhanced by showing the user the consequences of his actions. According to Lipford et al. [18] this can be done by showing the user their profile as seen by others. Onwuasonanya et al. [22] study the behaviour of users when given the ability to define subgroups among their online friends. An existing system that combines both of these features (and other privacy tools) is Clique, part of the Primelife project. This experimental OSN allows its users to create multiple "faces" to use in different social contexts. Each face has their own collections of contacts (e.g. friends, colleagues and family) and each piece of information can be made visible to any combination of people [17]. Users can check if the desired result is achieved by viewing their profile from the perspective of other users.

The proposed solutions are often comparatively cheap to implement, and are mainly realized by OSN service providers making the right design choices. However, they require user awareness and acceptance in order to reach their full potential. Also, data

collection and retention are key to many OSNs' revenue, so acceptance by OSN service providers may be an even bigger issue.

4.4 Encryption

Encryption can be used as a tool to provide confidentiality and as the basis for integrity. Depending on how encryption is applied this can mean protection from unauthorized users or the service provider. It can be coupled with either decentralization or privacy settings and management.

Lucas and Borisov [19] propose to encrypt certain parts of a user's profile using public key cryptography. Keys are derived from user-supplied passwords in order to maintain access flexibility. A potential problem with this approach is the resulting low entropy of the keys.

Guha et al. [14] argue that encrypted messages on a profile are easy to spot by the social network provider, which could result in sanctions if the provider disapproves of encryption. Their approach uses substitution of "information atoms" (e.g. age, or name-and-gender) to hide information. Keys and related material are exchanged out of band. The number of channels that are used for this scheme is high. Also outside users have no way to distinguish between users that are hiding their information and users that are not. This makes profiles meaningless to such users, and could lead to cases of mistaken identity.

The advantage of cryptographic approaches is that they can solve many issues, if used properly. Through cryptography, one can protect data from other users, as well as the OSN. In addition, the security of such techniques can often be proven or verified comparatively easily. However, key management is a big issue, especially if there is a high amount of churn in friendship relations and group membership. Also, cryptography often involves expensive operations, for the user, the service provider, or both. Especially in large OSNs, scalability can easily become an obstacle.

4.5 Awareness, Law and Regulations

Research in this (mainly non-technical) field focusses on enhancing user awareness of the privacy issues that exist within OSNs and compliance of both users and service providers to established laws and social conducts. It can aid users in specifying and respecting privacy boundaries, and alleviate the issue of "other users posting information about you".

Kang and Kagal [16] propose a social mechanism to prevent data abuse by showing on a profile what is acceptable to do with the data and what is not. There is no further technical support for this.

Onwuasoanya et el. [22] propose to require the user to group his friends and consequently be able to set different privacy settings for each group. The aim is to provide users a simple and intuitive way to manage their privacy settings, thus increasing user awareness.

The system that Goecks et al. [12] propose, uses social collaboration to make it easier for users to set their privacy settings and make them more aware if their choice is different from the norm.

These non-technical approaches lack the power to actively enforce the changes they propose. Policies and regulations are not mandatory, and awareness is something that needs time to be raised. Specific laws dealing with personal information as related to the Internet and OSNs are likely to be an important and much needed tool, but often take long to be developed. Also, laws are used to solve matters *after* things go wrong, whereas technical solutions attempt to *prevent* violations.

4.6 Summary

Table 3 shows which research discipline addresses which privacy concern, a ● if it is addressed and a · if it is not addressed. None of the disciplines mentioned in this section offer complete privacy for OSN users. Because the privacy problem is in fact multi-faceted, so should the solution. Not only should technical solutions be developed to tackle the various privacy issues; service providers should be encouraged to implement such solutions, and users need to be made aware of the benefits of using them.

← Privacy concerns	Relevant defenses →	Anonymization	Decentralization	Privacy settings and management	Encryption	Awareness, law and regulations
User related	Stranger views private info	●	·	●	●	●
	Unable to hide info from specific friend / group	·	·	●	●	·
	Other users posting information about you	·	·	●	·	●
Provider related	Data retention	●	●	·	●	●
	OSN employee browsing private info	·	●	·	●	●
	Selling of data	●	●	·	●	●
	Targeted marketing	●	●	·	●	●

Table 3. Privacy concerns and relevant defenses.

5 Relation to the Kindred Spirits Project

Within the Kindred Spirits project, matching of similar users and content recommendation are seen as central operations in OSN's. This makes "content recommendation" and "dating" OSNs the most relevant scenarios for the project. Main data types to protect

from privacy-intrusions would thus include profiles, preferences, behavioural information and messages. The centeral operations to be performed on this data are clustering/matching, and filtering/search.

The problems to be adressed by the Kindred Spirits project are not limited to the realm of "user-related" threats. We feel that a user's privacy from the OSN service provider should also be guaranteed, and that this is in the interest of both users and service providers. The latter can benefit by improving their image for competitive advantage and avoiding problems related to data-protection laws.

The technical solutions we have seen in Section 4 focus on specific (categories of) problems. A solution to the general problem of lack of privacy in OSNs can be assumed to involve several of the aforementioned techniques. The identified topics in existing research relate to the Kindred Spirits project as follows:

Anonymization Anonymization research is mainly useful after information has been supplied to the OSN. In the case of Kindred Spirits we aim to hide some information from the OSN. It seems that anonymization research does not match with Kindred Spirits.

Decentralization In the Kindred Spirits project more control is given to the user and some information should be hidden from the OSN. Some degree of decentralization fits this picture, and may be used in our research.

Privacy settings and management Kindred spirits should be able to find each other. In order to make this happen, users will have to specify which data they want to use for the matching process and also how important their privacy is in this process. In order to convey this, some form of privacy management is needed. Research into gradual and fine-grained privacy-management fits one of the central hypotheses of the Kindred Spirits project.

Encryption In order to hide information from the OSN, while still making use of a central infrastructure, encryption is necessary.

Awareness, law and regulations This field of research complements the Kindred Spirits project as it will work towards OSN users becoming more privacy-aware, and OSN service providers adopting a more serious attitude towards preservation of privacy. However this field is also outside the scope of the Kindred Spirits project.

Considering the above, it seems natural for the research in the Kindred Spirits project to revolve around encryption and small scale decentralization, backed up by proper tools for managing privacy settings. The solutions should aim to protect profiles, preferences, behavioural information and messages, while still allowing the service provider to cluster or search the data.

In conclusion, the schemes and protocols developed in the Kindred Spirits project should facilitate (partial) hiding of user data from the OSN and other users through encryption, while maintaining the ability to find kindred spirits (matching between users) or provide media recommendations. When a match between users is found, further protocols should facilitate additional functionalities, such as gradual information disclosure, or exchanging recommendations in a privacy-friendly way.

References

1. J. Anderson, C. Daz, J. Bonneau, and F. Stajano. Privacy-enabling social networking over untrusted networks. In J. Crowcroft and B. Krishnamurthy, editors, *WOSN*, pages 1–6. ACM, 2009.
2. E.-A. Baatarjav, R. Dantu, and S. Phithakkitnukoon. Privacy management for facebook. In R. Sekar and A. K. Pujari, editors, *International Conference on Information Systems Security*, volume 5352 of *Lecture Notes in Computer Science*, pages 273–286. Springer, 2008.
3. L. Backstrom, C. Dwork, and J. Kleinberg. Wherefore art thou r3579x?: anonymized social networks, hidden patterns, and structural steganography. In *WWW '07: Proceedings of the 16th international conference on World Wide Web*, pages 181–190, New York, NY, USA, 2007. ACM Press.
4. L. Banks and S. F. Wu. All friends are not created equal: An interaction intensity based approach to privacy in online social networks. In *IEEE International Conference on Computational Science and Engineering*, pages 970–974, 2009.
5. F. Benevenuto, T. Rodrigues, M. Cha, and V. A. F. Almeida. Characterizing user behavior in online social networks. In A. Feldmann and L. Mathy, editors, *Internet Measurement Conference*, pages 49–62. ACM, 2009.
6. D. Boyd and N. B. Ellison. Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, 13(1):210–230, 2007.
7. S. Buchegger and A. Datta. A case for p2p infrastructure for social networks - opportunities and challenges. In *WONS 2009, 6th International Conference on Wireless On-demand Network Systems and Services*, pages 161–168, Snowbird, Utah, USA, February 2009.
8. S. Buchegger, D. Schiöberg, L. H. Vu, and A. Datta. Peerson: P2p social networking: early experiences and insights. In *SNS '09: Proceedings of the Second ACM EuroSys Workshop on Social Network Systems*, pages 46–52, New York, NY, USA, 2009. ACM.
9. B. Carminati, E. Ferrari, and A. Perego. Private relationships in social networks. In *ICDE Workshops*, pages 163–171, 2007.
10. C. Dwork. Differential privacy. In *Automata, Languages and Programming, 33rd International Colloquium, ICALP 2006, Venice, Italy, July 10-14, 2006, Proceedings, Part II*, pages 1–12, 2006.
11. M. J. Freedman and A. Nicolosi. Efficient private techniques for verifying social proximity. In *Proceedings of the 6th International Workshop on Peer-to-Peer Systems (IPTPS07)*, pages 1–7, Bellevue, WA, February 2007.
12. J. Goecks, W. K. Edwards, and E. D. Mynatt. Challenges in supporting end-user privacy and security management with social navigation. In L. F. Cranor, editor, *Symposium on Usable Privacy and Security*, ACM International Conference Proceeding Series, pages 1–12. ACM, 2009.
13. R. Gross and A. Acquisti. Information revelation and privacy in online social networks. In *WPES '05: Proceedings of the 2005 ACM workshop on Privacy in the electronic society*, pages 71–80, New York, NY, USA, 2005. ACM.
14. S. Guha, K. Tang, and P. Francis. Noyb: privacy in online social networks. In *Proceedings of the first workshop on Online Social Networks (WOSP)*, pages 49–54, New York, NY, USA, 2008. ACM.
15. J. Kang. Information privacy in cyberspace transactions. *Stanford Law Review*, 50(4):1193–1294, 1998.
16. T. Kang and L. Kagal. Establishing social norms for privacy in social networks. 2009.
17. R. Leenes. *Context Is Everything - Sociality and Privacy in Online Social Network Sites*, volume 320/2010, chapter 4, pages 48–65. Springer Boston, 2010.

18. H. R. Lipford, A. Besmer, and J. Watson. Understanding privacy settings in facebook with an audience view. In *UPSEC'08: Proceedings of the 1st Conference on Usability, Psychology, and Security*, pages 1–8, Berkeley, CA, USA, 2008. USENIX Association.
19. M. M. Lucas and N. Borisov. Flybynight: mitigating the privacy risks of social networking. In *Proceedings of the 7th ACM workshop on Privacy in the electronic society (WPES)*, pages 1–8, New York, NY, USA, 2008. ACM.
20. E. M. Maximilien, T. Grandison, K. Liu, T. Sun, D. Richardson, and S. Guo. Enabling privacy as a fundamental construct for social networks. In *Proc. International Conference on Computational Science and Engineering CSE '09*, volume 4, pages 1015–1020, Aug. 29–31, 2009.
21. G. Mezzour, A. Perrig, V. D. Gligor, and P. Papadimitratos. Privacy-preserving relationship path discovery in social networks. In J. A. Garay, A. Miyaji, and A. Otsuka, editors, *Cryptology and Network Security*, volume 5888 of *Lecture Notes in Computer Science*, pages 189–208. Springer, 2009.
22. A. Onwuasoanya, M. Skornyakov, and J. Post. Enhancing privacy on social networks by segregating different social spheres. *Rutgers Governor's School of Engineering and Technology Research Journal*, 3:1–10, 2008.
23. L. Palen and P. Dourish. Unpacking "privacy" for a networked world. In *CHI '03: Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 129–136, New York, NY, USA, 2003. ACM.
24. D. Rosenblum. What anyone can know: The privacy risks of social networking sites. *IEEE Security & Privacy*, 5(3):40–49, May 2007.
25. A. Shakimov, A. Varshavsky, L. P. Cox, and R. Cceres. Privacy, cost, and availability tradeoffs in decentralized osns. In J. Crowcroft and B. Krishnamurthy, editors, *WOSN*, pages 13–18. ACM, 2009.
26. A. Tootoonchian, S. Saroiu, Y. Ganjali, and A. Wolman. Lockr: better privacy for social networks. In *CoNEXT '09: Proceedings of the 5th international conference on Emerging networking experiments and technologies*, pages 169–180, New York, NY, USA, December 2009. ACM.
27. Z. Tufekci. Can you see me now? audience and disclosure regulation in online social network sites. *Bulletin of Science Technology Society*, 28(1):20–36, February 2008.
28. A. Turk. Opinion 5/2009 on online social networking. Technical Report 01189/09/EN WP 163, Article 29 Data Protection Working Party, 6 2009. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp163_en.pdf.
29. B. Viswanath, A. Mislove, M. Cha, and P. K. Gummadi. On the evolution of user interaction in facebook. In J. Crowcroft and B. Krishnamurthy, editors, *Workshop on Online Social Networks*, pages 37–42. ACM, 2009.
30. S. Weiss. The need for a paradigm shift in addressing privacy risks in social networking applications. In *The Future of Identity in the Information Society*, volume 262, pages 161–171. IFIP International Federation for Information Processing, 2008.
31. X. Ying and X. Wu. Randomizing social networks: a spectrum preserving approach. In *Proceedings of the SIAM International Conference on Data Mining*, pages 739–750. Society for Industrial and Applied Mathematics, 2008.
32. B. Zhou, J. Pei, and W. Luk. A brief survey on anonymization techniques for privacy preserving publishing of social network data. *Special Interest Group on Knowledge Discovery and Data Mining Explorations*, 10(2):12–22, 2008.

Web References

33. Uk parliament (1998) data protection act. hmso, london.

34. J. Bonneau. Attack of the zombie photos. online, 2009. http://www.lightbluetouchpaper.org/2009/05/20/attack-of-the-zombie-photos/.
35. E. Burns. Marketing to social networking sites, targeted. online, 4 2007. http://www.clickz.com/3625536.
36. D. Cardon. Le design de la visibilit : un essai de typologie du web 2.0. online, 2 2008. http://www.internetactu.net/2008/02/01/le-design-de-la-visibilite-un-essai-de-typologie-du-web-20/.
37. R. Dube and M. B. P. Adomaitis. What types of social networks exist. online, 3 2009. http://socialnetworking.lovetoknow.com/What_Types_of_Social_Networks_Exist.
38. D. Emmett. Taxonomy of social networks. online, 6 2009. http://davemmett.wordpress.com/2009/06/15/taxonomy-of-social-networks/.
39. L. Gannes. A taxonomy of social networks? online, 2 2007. http://gigaom.com/2007/02/09/social-network-taxonomy/.
40. N. Hernandez. President apologizes for questionable photos, 10 2007. http://www.washingtonpost.com/wp-dyn/content/article/2007/10/17/AR2007101702244.html.
41. A. Jacob. How to hack myspace private profile picture and video. online, 4 2007. http://www.clazh.com/how-to-hack-myspace-private-profile-picture-and-video/.
42. B. Lunn. Social network types, motivations, and the future. online, 9 2007. http://www.readwriteweb.com/archives/social_network_types_motivations.php.
43. P. MacNamara. Facebook blocks 'web 2.0 suicide machine'. online, 1 2010. http://www.networkworld.com/news/2010/010410-buzzblog-facebook-blocks-suicide-machine.html.
44. S. Olsen. At rapleaf, your personals are public. online, 8 2007. http://news.cnet.com/At-Rapleaf,-your-personals-are-public/2100-1038_3-6205716.html.
45. N. O'Neill. "anonymous" facebook employee interview: Fact vs fiction, 1 2010. http://www.allfacebook.com/2010/01/anonymous-facebook-employee-interview-fact-vs-fiction/.
46. Pingdom.com. Social network popularity around the world. online. http://royal.pingdom.com/2008/08/12/social-network-popularity-around-the-world/.
47. W. Riddle. Cyberbullied teen sues ex-classmates, their parents, and facebook, 3 2009. http://www.switched.com/2009/03/04/cyberbullied-teen-sues-ex-classmates-their-parents-and-faceboo/.
48. unknown. Types of online social networks. online. http://onlinebrandmanager.org/social-media/social-network-types/.
49. unknown. Types of social networking websites. online, 2010. http://www.hudsonhorizons.com/Custom-Website-Solutions/Social-Networking/Types-of-Social-Networks.htm.
50. C. Walters. Facebook's new terms of service: "we can do anything we want with your content. forever.", 2 2009. http://consumerist.com/2009/02/facebooks-new-terms-of-service-we-can-do-anything-we-want-with-your-content-forever.html.
51. D. M. Williams. Online identity expert loses control of nsfw r-rated online pics, 3 2009. http://www.itwire.com/your-it-news/home-it/23975-online-identity-expert-loses-control-of-nsfw-r-rated-online-pics.