Masking in Social Network Sites – Translating a Real-World Social Practice to the Online Domain

Maskierung innerhalb von sozialen Netzwerken –
Übersetzung von Praktiken der realen Welt in die Online-Welt

Bibi van den Berg, Ronald Leenes, Tilburg University, Tilburg Institute for Law, Technology, and Society (TILT)

Summary Research shows that most social network sites contain serious privacy risks for users. Many of these risks revolve around users' inability to know exactly who the "audience" is that witnesses their online behaviours. In this article we argue that in the offline world individuals regularly use the strategy of "masking" to hide their visibility when the composition of their audience is unknown. We claim that "masking" should also be facilitated in social network sites to enhance users' privacy-protection. However, SNSs' platform design, focused on self-presentation, makes its implementation difficult.

►►► Zusammenfassung Die meisten sozialen Netze stellen bedeutende Datenschutzrisiken für die Benutzer dar. Viele dieser Risiken hängen damit zusammen, dass Benutzer nicht genau den „Zuschauerkreis“ kennen, welcher ihr Online-Verhalten beobachten kann. In der realen Welt verwenden Menschen die Strategie der „Maskierung“ um ihre Anwesenheit zu verstecken, falls der Zuschauerkreis unbekannt ist. Wir behaupten, dass die „Maskierung“ auch in sozialen Netzen als Datenschutztechnik dem Benutzer zur Verfügung stehen sollte. Dies ist jedoch schwierig, da Soziale Netze auf Selbstdarstellung ausgerichtet sind.

Keywords K.4 [Computing Milieux: Computers and Society]; K.4.1 [Computing Milieux: Computers and Society: Public Policy Issues]; Privacy ►►► **Schlagwörter** Datenschutz, soziale Netzwerke, Maskierung

1 Introduction

Millions of users worldwide use the internet to communicate and interact with others and to present themselves to the world via a variety of channels¹.

These include, among others, personal and professional home pages, forums, online communities, blogs, dating sites, and social network sites such as Facebook, Friendster, LinkedIn and MySpace. In this article we will discuss some of the privacy issues surrounding the pre-

sentation of personal content (e. g., text, pictures, sounds, movies) and personal information (e. g., name, address, work or leisure affiliations) in social network sites.

We will begin this article with an overview and discussion of the various privacy and security issues that have been pointed out by researchers over the last couple of years with respect to social network sites (Sect. 2). When reviewing the totality of these issues, we conclude that in social network sites one of the commonest risks for users' privacy originates from the fact that they lack knowledge of the makeup of the "audience" – users do not know (exactly or sufficiently) who can view the content they post in such communities.

¹ See for instance <http://www.thebluedoor.com/2010/01/social-media-and-web-20-statistics.shtml> for some (recent) numbers. Or see the lovely map by XKCD, which shows applications as countries, whose size reflects usage <http://xkcd.com/802/>.

Whenever individuals do not know the makeup of the “audience” for whom they are performing in the offline world, they tend to resort to a simple mechanism to protect their privacy, which we call “masking”. In the third section of this article we will discuss what masking is and how it is utilised as a social practice. We argue that adding a virtual version of this common social practice to social network sites would enhance the privacy-friendliness of these systems, especially in users’ behaviours in so-called “groups”, a sub-domain of social network sites. However, adding such a feature is difficult to accomplish, because the design and central purposes of social network sites undermine or defeat masked interaction. We illustrate these difficulties by discussing some of our attempts within our alternative, more privacy-friendly social network site called Clique (see <http://clique.primelife.eu/>) (Sect. 4).

2 Privacy in Social Network Sites: Overview and Discussion

One of the fastest growing online fora for self-presentation and social interaction of the past few years are “social network sites”. In June 2008 these sites attracted “an average of 165 million unique visitors a month” [1]. In the same year two of the biggest social network sites worldwide, MySpace and Facebook, had over 100 million and over 80 million users respectively [2]. In 2010 Facebook alone has over 500 million active users.² In these online domains users can present themselves using a so-called “profile”, and they can engage in interactions with a network of “contacts”³ also active in the same environment. One of the most commonly used definitions of social network sites was developed by boyd and Ellison, who write that these are “web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system. The nature and nomenclature of these connections may vary from site to site” [4].

Sharing personal content and personal information are key elements of social network sites. Individuals join these networks for two main reasons: self-presentation and relationship management [5]. Users present information about themselves via various means, for instance

through text (blogs, descriptions of their current activities etc.), through pictures, movies and sound clips, and through listing their ‘favourites’ – a broad category of pre-defined and user-generated labels to help categorise themselves, ranging from clothing and other commercial brands, to music and movies, to locations and activities. Thus, an image of each particular user emerges. Most, though not all, information is added to the profile by users themselves. Other users can also add information to an individual’s profile, thereby further refining the image created.

One of the most fascinating aspects of this emerging field of self-presentation is the fact that users put so much and such personal information about themselves in their profiles [6; 7]. For instance, by mid 2007 users shared over 1 billion images and approximately 40 million videos via online platforms including social network sites, and photo and video networks such as Flickr and YouTube [1]. It is not surprising, therefore, that much of the research revolving around social network sites as an emerging phenomenon has focused on the privacy and security issues involved in individuals’ self-presentations and the sharing of personal content and personal details (cf. [2; 8; 10; 11]). Acquisti and Gross write: “...one cannot help but marvel at the nature, amount, and detail of the personal information some users provide, and ponder how informed this information sharing is” [8]. And in an article on the privacy risks for individuals using Facebook Grimmelmann dryly points out: “Facebook knows an immense amount about its users. A fully filled-out Facebook profile contains about 40 pieces of recognizably personal information, including name; birthday; political and religious views; online and offline contact information; sex, sexual preference and relationship status; favorite books, movies, and so on; educational and employment history; and, of course, picture. [...] Facebook then offers multiple tools for users to search out and add potential contacts. [...] By the time you’re done, Facebook has a reasonably comprehensive snapshot both of who you are and of who you know” [2].

Research has shown that the overwhelming majority of members use their real name on their Facebook profile: a staggering 94.9% according to Tufekci [7], and an even higher number, 99.35%, was found in a 2009 study by Young and Quan-Haase [6]. This level of truthfulness can be understood in light of Facebook’s policy to actively, and quite strictly, discourage the use of fake names. Another explanation could be that users want to avoid the fact that their friends cannot find them online. As boyd writes: “While teens are trying to make parental access more difficult, their choice to obfuscate key identifying information also makes them invisible to their peers. This is not ideal because teens are going online in order to see and be seen by those who might be able to provide validation.” [9].

Apart from using a real name, however, the question remains why users choose to disclose such a detailed and

² See <http://www.facebook.com/press/info.php?statistics> [last accessed on 26 October 2010].

³ Confusingly, in many current-day social network sites a person’s contacts are called ‘friends’, regardless of the actual relation (friend, relative, colleague, acquaintance, and so on) the person has to these others. Following James Grimmelmann, we prefer to use the term ‘contacts’ for the collection of connections that a person gathers in a social network site, since “...it’s more neutral about the nature of the relationship than the terms used by many sites, such as ‘friend’” [2]. After all, as Grimmelmann rightly notes social network site “... ‘friends’ include not just people we’d call ‘friends’ offline but also those we’d call ‘acquaintances’ [...] Contact links are a mixture of what sociologists would call ‘strong ties’ and ‘weak ties.’” [idem]. (The terms ‘strong ties’ and ‘weak ties’ are a reference to Granovetter’s work on interpersonal ties [3]).

truthful picture of themselves, involving a wide range of personal details. What makes them behave this way?

Many explanations can be given, but we restrict ourselves to some of the most often heard ones. Acquisti and Gross point towards a number of reasons, such as: “[c]hanging cultural trends, familiarity and confidence in digital technologies, [and] lack of exposure or memory of egregious misuses of personal data” [8]. Grimmelmann argues that the reason is actually much more straightforward: people misunderstand the risks involved in presenting detailed and personal information online. This misunderstanding takes a number of forms. For one, users are often unaware of who has access to their personal profile and to the content they place online, because the architecture and design of social network sites is such that it provides individuals with a false sense of security and privacy. These sites “systematically [deliver] them signals suggesting an intimate, confidential, and safe setting” [2], an environment that is private, “closed to unwanted outsiders.” [idem]. Second, users falsely believe that there is safety in numbers, in two senses of the expression. They believe that when everyone else around them massively starts using social network sites, these sites must be safe to use, because otherwise others would avoid them (a line of reasoning that runs the obvious risk of being flawed if everyone follows it), and they believe the risks they run are very limited since there are so many members in social network sites that chances are in fact really small that some incident will befall them as individuals [2]. Or, as boyd argues, “[m]ost people believe that security through obscurity will serve as a functional barrier online. For the most part, this is a reasonable assumption. Unless someone is of particular note or interest, why would anyone search for them? Unfortunately for teens, there are two groups who have a great deal of interest in them: those who hold power over them – parents, teachers, local government officials, etc. – and those who wish to prey on them – marketers and predators” [9].

Taking things to a more general level, one can argue that there are four fundamental issues surrounding privacy and (unintended) information disclosure online [10; 11].⁴ These can be summarised as follows:

- It is difficult or even impossible for users to know what the composition or the size of the audience is for whom they are presenting their personal information and content.
- Since information on the internet can easily be recorded, copied and stored, it gets a level of persistence that most information in the real world lacks. This means that information may (unintentionally) reach audiences in the (far) future.

⁴ These issues of course also exist in the offline world: people may be embarrassed, others' perception of them may be biased, and job opportunities may be restricted when information that was deemed private becomes public. In this article, however, we focus on social network sites.

- Information shared in one internet environment may easily be transported (copied, linked) to other contexts. Thus, information that had one meaning in the original context may gain a different meaning in another context, possibly reflecting back on the individual in unintended and unforeseen ways.
- Our online self-presentations are the result of content and information posted by both ourselves and others, and made up of an amalgam of images ranging from deliberate and explicit self-presentations to more implicit “traces of self”, of which users are generally not especially aware. Controlling these self-presentations and the possible deductions others may make on the basis of them is difficult, if not wholly impossible, for individual users.

These four issues are highly relevant to social network sites. For one, when posting content or personal information in a profile, individuals do not know (exactly) who will be able to access this information. The audience, to phrase it differently, is not transparent. While some social network sites allow users a degree of control over the visibility of the information placed in profiles (e.g. changing personal information to “visible to friends only”), the default privacy settings are usually set to “public”, which means that individuals' profiles and the information contained in them can be viewed by anyone accessing the social network site. This means, Acquisti and Gross conclude, “that the network is effectively an open community, and its data effectively public” [8].

Second, since information can be copied, saved and stored at very low cost, the chances of information still being available online somewhere years after being placed online are significant. Information may therefore return to the stage and affect individuals long after publication. This means that the audience is unlimited both in terms of its size and makeup (in contrast to audiences in the physical world), but also in terms of temporality. In the words of Tufekci, the temporal boundaries shift in such a way that “the audience can now exist *in the future*. [...] Not only are we deprived of audience management because of spatial boundaries, we also can no longer depend on simultaneity and temporal limits to manage our audiences” [7, emphasis in the original].

Third, when presenting disparate identities in various online domains, there is a risk of information from one of these domains, for instance a personal or professional home page, seeping into another, such as someone's social network site profile. Since different behavioural rules guide these various domains, mixing and merging information about the person behind all of these various roles can lead to serious problems. Tufekci gives a very simple, yet illuminating example: “...a person may act in a way that is appropriate at a friend's birthday party, but the photograph taken by someone with a cell phone camera and uploaded to MySpace is not appropriate for a job interview, nor is it necessarily representative of that

person. Yet that picture and that job interview may now intersect” [7].

Last, and this is related to the previous point, in social network sites who we are is expressed by an online representation of ourselves, which may be composed of, for instance, a profile with personal details, stories and pictures. While we have some level of control over the type and content of information we put online, our control only goes so far. Other users can add or change information in a person’s personal profile, put pictures or information about the person on their own or other people’s profiles, and tag pictures to reveal the identities of those portrayed in them. Tufekci’s example in the previous paragraph is a case in point: placing a picture of another person online affects the image of that person to the audience viewing it, and hence may have an effect on the (current and future) self-presentations and impressions of that individual.

When reviewing these four privacy issues in online environments in general, and in social networks in particular, one item surfaces time and again: due to the nature of online performances, it is unclear to the person performing who sees what information about him or her, and at what point in time.⁵ The first issue, the inability to know (fully or sufficiently) who the audience is, is really the central theme in all other privacy issues in online environments as well. The lack of control, the transportability of information, and its persistence over time all point toward the fact that individuals have no way of knowing (exactly) who witnesses or watches their online behaviours. The stage metaphor that is often used to explain ‘role performance’ and the process of constructing and expressing identities [12–15], is very apt here: in online performances the actor is performing on a brightly lit stage, in front of an audience that is seated in the dark. Those seated in the first few rows may be (partially) visible, because the stage lights will shed some light on their faces. However, after the first few rows, there is just darkness and the actor on stage does not know whether there are people seated there, how many people are seated there, or who these people are exactly. The same goes for online performances, such as those in social network sites: when posting content on a profile page, or interacting with others in groups, the individual may have a grasp of some of the people who may access this content – the members of his contact list are those seated in the first few rows of the theatre. But it remains unclear to him who occupies the seats in the darkness, or whether anybody is there at all.

To investigate this issue in more detail we have turned to social scientific literature, to come to a better understanding of how individuals deal with such “darkened theatre situations” in real life. We aimed to uncover

whether we could find a social mechanism from the real world to cope with such situations, and to see whether we could translate that mechanism to the online world, and to social network sites in particular. In the next section we will present the real-world strategy we found, called “masking”.

3 Masking

The “stage metaphor” that we discussed in the previous paragraph originates with the 20th century Canadian sociologist Erving Goffman. In his influential book “The presentation of self in everyday life” Goffman presents his perspective on the ways in which identities are constructed and expressed in interactions between human beings in everyday contexts [12]. According to Goffman, whenever individuals engage in interactions with others they perform roles, the goal of which is to present an image of themselves which is favourable, not only to the personal goals they are attempting to achieve within the context in which they find themselves (strategic interaction), but at the same time also meets with the approval of those with whom they engage in the interaction – in their presentations, individuals seek ‘public validation’ [16]. To Goffman, impression management is key in such self-presentations.

Each person performs a wide variety of roles in his everyday life, relating to both the places s/he visits, and the other people present there [15; 17; 18]. For instance, when at work, individuals will display different sides of themselves than when they are at home, or when they buy groceries at a local store, or when they visit a movie theatre, and so on and so forth. However, the location a person finds himself in is not the only relevant parameter; so is the presence (or absence) of specific other people in that location. Individuals will show different sides of themselves when they are at home with their family than when they are hosting a party for their colleagues in that same home. Moreover, they will show different sides of themselves when they know (the members and composition of) the audience than when they do not. The presentation of selves, then, is situated or contextual – it relates to where one is, and who else is there [14; 15].

One of the key elements of Goffman’s perspective on identity is the fact that individuals attempt to present self-images that are both consistent and coherent. To accomplish such a consistent and coherent situated self-image, performers engage in what Goffman calls “audience segregation”, “...so that the individuals who witness [them] in one of [their] roles will not be the individuals who witness [them] in another of [their] roles” [12]. With segregated audiences for the presentation of specific roles, performers can “maintain face” before each of these audiences. Their image will not be contaminated by information from other roles performed in other situations before other audiences, particularly not by information that may discredit a convincing performance in the current situation [12]. For example,

⁵ This is also true in the offline world: what is private and what is public is often flexible and negotiable, but online the issues are aggravated due to characteristics of the internet: information flows, lack of (physical) boundaries, and persistence.

a person whose professional role consists of displaying a role of authority, such as a political leader or a judge, may try to shield aspects of his private life from the public, such as the fact that in his relationship his partner is the one in charge and he is not an authoritative person at all when at home. He shields this information from those he may encounter in his professional life to prevent his professional authority being undermined if the audience were to know about this aspect of his personal life.

While Goffman's idea of audience segregation did not originally relate directly to privacy, it is easy to see that audience segregation and privacy are, in fact, closely related. Helen Nissenbaum has argued that privacy revolves around "contextual integrity", which means that individuals' personal integrity ought to be maintained across and between the various contexts they engage in each day [19–21]. Nissenbaum starts from the following observation: "Observing the texture of people's lives, we find them [...] moving about, into, and out of a plurality of distinct realms. They are at home with families, they go to work, they seek medical care, visit friends, consult with psychiatrists, talk with lawyers, go to the bank, attend religious services, vote, shop, and more. Each of these spheres, realms, or contexts involves, indeed may even be defined by, a distinct set of norms, which governs its various aspects such as roles, expectations, actions, and practices" [20]. Following Michael Walzer [22], Nissenbaum argues that what privacy is, is the fact that we respect the contextual boundedness of the (personal) information individuals share in each of these distinct realms. Phrased differently, according to this view privacy revolves around a person's ability to keep audiences separate and to compartmentalise his or her (social) life. Moreover, it revolves around individuals' ability to choose to shield information in some contexts and in interactions with some contacts, while sharing it in and with others. Here we find a key element for the situation we have described in the previous section: the fact that, in social network sites, individuals do not (entirely) know the makeup of the audience.

One strategy that individuals may use in everyday life to accommodate for the fact that they perform before various audiences is the mechanism of audience segregation that we discussed above. Audience segregation is a strategy that may be used in all situations in which individuals know, or can reasonably deduce, who is in the audience and what the extent of the audience is, which is the case in most everyday situations. Knowing these two things is required for individuals to be able to maintain divisions in their self-presentations. However, in real life there are also situations in which individuals do not know, or cannot reasonably deduce, the extent and the makeup of their audience. The most obvious example, which we introduced above, is that of an actor performing a role on stage, while the audience sits in darkness. Since the actor on stage cannot see who, or even how many people, are in the audience, he has

to resort to some means of "insulating" himself from the image he portrays on stage, lest the audience deduce information about himself (his "real" self?) that he is unwilling to share. In many cultures around the world we provide actors with an easy and very effective means to mark the distance between themselves as a "real" persona and the person they portray on stage: using masks. The mask is both a marker for being "out of one's own character", for pretence, and a means of protecting or shielding the person "behind" the pretence. Goffman has described this practice using the term "role distance" [23], which refers to "...those instances in which persons place distance between their self and their current self-in-role" [24]. We call the strategy of protecting one's "real" face from an unseen and/or invisible audience "masking".

While the theatre provides us with an example of masking in a literal sense, this strategy is not limited to the theatrical world. Think, for instance, of the practice of writing articles, poems or novels using a pseudonym – in the past, for instance, at times female writers chose to write under a pseudonym "in order to sidestep readers' gender-related prejudices and stereotypes" [25]. Moreover, pop stars and other idols sometimes mask their real identities by adopting a stage name. And think also of criminals who change their identities to keep themselves from getting caught, or of the use of so-called "noms de guerre" adopted by military and intelligence personnel to protect their true identity. What these examples show is that masking is a strategy that is far more common than one might think.

That masking is particularly relevant in the context of the internet is evident as well. Many of us use nicknames, screen-names and user-names to present ourselves (but not too much of ourselves) on websites, in forums and online games, when shopping online, downloading, and accessing information and online services. Moreover, the internet has turned out to be a particularly popular domain in which to conceal one's gender or assume another one [26; 27]. One central reason for concealing one's gender, especially by women, is the avoidance of harassment. Research has shown that concealing one's gender in online environments often does not succeed entirely – information from individuals' real-world gender may seep through and subtly reveal their offline sex, for instance through their use of language or the topics they discuss. Nevertheless, Mowbray convincingly argues that shielding one's gender in online environments may be effective, even if the offline gender is revealed, at least to some people. She writes: "In order for gender masking to afford protection from harassment, the user's gender does not have to be hidden from everyone – just from harassers. Online harassers tend to go for easy pickings, and so are likely to harass the nearest person who is 'obviously' female, rather than taking the trouble to find out whether a masked character is controlled by a female user" [25].

Note that there is a fine line between masking and deception – especially when viewed from the perspective of the audience. While audiences tend to accept an actor wearing a mask on a stage, to hide his “real” identity, they do not want to feel misled by the actor. Using a mask as a shield is socially acceptable – especially when the audience realizes that it is not the “real” identity that matters in a situation, but rather the projected one. Using a mask to be dishonest, to deceive the audience, is not socially acceptable, however. This is a thin line to walk, and we will return to this issue when we discuss masking as a mechanism in social network sites below.

4 The Challenge of Implementing Masking

As we argued above audience segregation and masking are common strategies in everyday life. Within the EU funded FP7 project PrimeLife⁶, we try to implement these real-world social practices to the online domain of social network sites in a testbed social network site called Clique⁷.

Audience segregation is implemented in Clique through the fact that users can create multiple “faces”, in which they can display different sides of themselves [28]. For example, they can create a “professional face”, a profile they use to engage in work-related interactions with professional contacts, a “private face”, a profile page they use to connect with close friends and family, a “hobby face”, to connect with members of the same sports club. Moreover, in Clique audience segregation is achieved even within each profile page [28; 29]. Users can cluster contacts into different “collections” (e.g., “colleagues”, “former colleagues”, “international work relations”), and each time they post content on their profile they can set the targeted audience for that information. These two tools greatly increase the amount of control they have over the audience that views each posting.

Audience segregation is a usable notion in social network sites in relation to self presentation. On their profile page, the user displays their self, or their identity. Their identity is at the centre stage. The mechanisms provided for audience segregation in Clique are mechanisms for access control to content posted by the user on their profile page contributing to their different faces. They provide the user tools to effectively separate their audiences by only providing access to content to the intended audience. The user controls their audience by means of audience segregation.

Masking is useful in situations where little control over the audience exists. As we have said, it may be used in particular when it is difficult or impossible for the individual to know who is, or how many people are, in the audience watching his performance. In these cases the individual can choose to distance or insulate himself from his performance to a certain extent by wearing a literal or metaphorical mask.

Since users have to log onto social network sites using a username and password and the username may be a pseudonym, this could be labelled a rudimentary form of masking. However, more often than not the screen-names and usernames that individuals use in social network sites do, in fact, correspond to their real names (see above). Most user- and screen-names in social network sites therefore function as identifiers rather than masks.

There is, however, an area within social network sites where masking could be a very helpful tool: that of group communication. Group communication in social network sites bears similarities with forums and other so-called ‘collaborative workspaces’. In user groups, members discuss a shared topic of interest (e.g., a hobby, a social or political theme or ideal) or they discuss a shared institution (e.g., a school, a town) or a brand (e.g., Apple, Nike). The same applies to many online forums. Moreover, just like in forums, users of social network sites can join or leave groups, start discussion threads, read posts by others, and comment on the remarks of others. They lack an overview of the size and makeup of the group, as is the case in forums, and must therefore operate as if they are actors on a stage in a darkened theatre.

User groups serve a different function in social network sites than profile pages. Social network sites have two main goals: self-presentation and relationship management [3]. Richter and Koch have argued that social software, i.e. the conglomerate of platforms that make up the second generation of the internet (“web 2.0”), roughly consists of three goals: (1) “management of self”; (2) “relationship management”; and (3) “information management”. These three goals can be represented in a triangle such as the one displayed below in Fig. 1 [28].

As the figure shows, web 2.0 functionalities such as wikis and forums can be found closer to the top of the triangle, since self-presentation and relationship management are less important in these domains than sharing information and (co-)creating content. In social network sites, on the other hand, presenting self-images and managing relationships is much more important than sharing (non-personal) information or collectively creating new

Figure 1 The functional triangle of social software, based on [3].

⁶ See <http://www.primelife.eu/>.

⁷ See <http://clique.primelife.eu/>.

content, which is why this type of social software is closer to the bottom of the triangle.

The incorporation of user groups in social network sites can be understood as an attempt to increase the functionality of the platform and thus increase its utility for its users. It incorporates forum functionality into a social network. In many user groups, especially in very large ones, individuals have very little insight into who else is participating in the same group, or even if they do, then it is likely that they do not know many people in the group. Also, members come and go – they can join or leave the group without the individual user's consent or even awareness. Moreover, only the administrator can manage the group – s/he can add or delete content and even participants, and has an overview of who sees which content. When posting messages or participating in a discussion, therefore, individual members of the group cannot (fully) know who the audience is they are performing for and how many people make up that audience. This is all the more problematic, as we have seen above, since information disclosed in groups has permanence, which means that future members of the group can also read back old threads, thereby enabling them to access information that was not posted with them in mind at the time of sharing.

In parallel with the real-world situation of wearing a mask in a theatre performance, or when publishing a book using a pen name, group members in social network sites could also benefit from being able to keep some distance between the self they present in groups, before an unknown and unknowable audience, and their 'real' selves as presented in the rest of the social network site. Put differently, to protect the privacy and security of group members in social network sites these sites could benefit from the introduction of a virtual version of masking.

In many online forums users post their content using a *pseudonym* or nickname. They create a user account with a fake name and a password in order to get access to the (posting facilities) of the forum, but do not leave detailed, authentic information about themselves on a forum profile page. Thus, their real names and identities are shielded in the majority of cases. The opposite is true of social network sites. Could using pseudonyms for group communication in social network sites be an adequate form of masking in these domains as well?

Although this may seem like a straightforward solution at first, unfortunately it is not a viable solution. As we have explained above, social network sites provide rich, detailed and authentic information about the majority of their users, who use their real identities to engage in self-presentations and connect with others. When users of social network sites participate in the groups that form a *subcategory* of the social network site on which they have built an information-rich profile page, therefore, information about their "real" selves is unavoidably going to seep into their "performance" in the group. Protecting users' privacy by implementing tools for audience segre-

gation into their profile pages could easily be undone by users' participation in groups, in which the audience is unknown and principally unknowable.

And there are more problems with the use of pseudonyms as a means to mask users' "real" identities in group communication. For one, users would have to be forced to use a pseudonym when signing up for a group. While this could be accomplished by making them complete a wizard⁸ quite easily, users could still decide to use a recognisable or detectable name, if they did not see the urgency or importance of using a pseudonym, or did not care. This would defeat the purpose of using a masking tool.

What is more, posting under a pseudonym explicitly undercuts the goals of social network sites: self-presentation and relationship management. This is why this facility is not offered on existing social network sites such as Facebook or LinkedIn. As a matter of fact, users' names are explicitly mentioned and made clickable (directing those interested to the profile page) with every post that is made within a group. While this is understandable in light of the aforementioned goals of social network sites, it may threaten users' privacy.

We conclude that while masking is a common and important social mechanism used in everyday interactions in which the (makeup of the) audience is unknown to the performer, it is difficult to create a virtual version of this mechanism for social network sites, despite the fact that it would greatly enhance the privacy-friendliness of these sites.

5 Conclusions

In this article we have provided an overview of a number of privacy issues that regularly occur in social network sites such as Facebook, MySpace and Friendster. We have argued that many of these issues revolve around the fact that, when presenting information about themselves on the profile pages of such sites, users lack knowledge of the makeup and size of their audience. It is as if they are performing on a brightly lit stage, with the audience seated in the dark. The actors do not know who is watching them, or even whether there is an audience out there at all.

We have shown that from time to time this situation arises in the offline world as well, and that individuals have developed a social mechanism to deal with performing before such an unknown audience: "masking". In a theatre, actors use masks to shield their "real" identities from the audience and to display only a projected identity. Similarly, authors use pseudonyms, pop stars use stage names and spies use undercover identities.

We have argued that social network sites could benefit from a virtual version of the offline practice of masking, and especially the sub-domain of "user groups" in social network sites. After all, in user groups the individual

⁸ A wizard is a small application that guides the user through a certain task.

member cannot be certain about the makeup and size of the audience, and hence his or her privacy would benefit from participation using a mask of some kind. However, we have shown that it is difficult to implement a virtual version of masking in social network sites, including our own test bed network called Clique, because pseudonymous group participation undercuts the central goals of social network sites: self-presentation and relationship management. Thus, while masking is a commonly used social mechanism in the offline world, translating it to the online domain is not a straightforward task. We have shown that this is caused by the odd role played by forum functionality within social network sites.

References

- [1] Ala-Mutka, K., et al. (2009). The impact of social computing on the EU information society and economy. IPTS/JRC: Seville (Spain).
- [2] Grimmelmann, J. (2008). Facebook and the social dynamics of privacy [draft version], 1–52.
- [3] Granovetter, M. (1973). The Strength of Weak Ties. *American Journal of Sociology*. **78**(6), May 1973, pp. 1360–1380.
- [4] boyd, d. and N. B. Ellison (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*. **13**(1), p. 210–230.
- [5] Richter, A. and M. Koch (2007). Social software: Status quo und Zukunft. *Technischer Bericht*, 2007, **2007-01**, p. 1–49.
- [6] Young, A. L. and A. Quan-Haase (2009). Information revelation and internet privacy concerns on social network sites: A case study of Facebook, paper presented at C&T '09. ACM: University Park, Pennsylvania (USA). p. 265–274.
- [7] Tufekci, Z. (2008). Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology and Society*. **28**(1), p. 20–36.
- [8] Acquisti, A. and R. Gross (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook, in Proceedings of the 6th Workshop on Privacy Enhancing Technologies. Cambridge, UK.
- [9] boyd, d. (2008). Why youth (heart) social network sites: The role of networked publics in teenage social life, in MacArthur Foundation Series on Digital Learning – Youth, Identity, and Digital Media Volume, D. Buckingham, Editor. MIT Press: Cambridge (MA). p. 119–142.
- [10] Palen, L. and Dourish, P. (2003). Unpacking ‘privacy’ for a networked world, paper presented at Computer-Human Interaction (CHI) Conference 2003. Ft. Lauderdale (FA). p. 129–137.
- [11] Solove, D. J. (2007). The future of reputation: Gossip, rumor, and privacy on the Internet. New Haven: Yale University Press.
- [12] Goffman, E. (1959). The presentation of self in everyday life. Garden City (NY): Doubleday.
- [13] Goffman, E. (1997). The self and social roles, in The Goffman reader, C. C. Lemert and A. Branaman, Editors. Blackwell Publishers: Cambridge (MA). p. 35–43.
- [14] Van den Berg, B. (2008). Self, script, and situation: Identity in a world of ICTs, in The future of identity in the information society: Proceedings of the third IFIP WG 9.2, 9.6/11.6, 11.7/FIDIS International Summer School on the Future of Identity in the Information Society, S. Fischer-Hübner, et al., Editors. Springer: New York (NY). p. 63–77.
- [15] Van den Berg, B. (2009). The situated self: Identity in a world of Ambient Intelligence. 2009, Rotterdam (The Netherlands).
- [16] Branaman, A. (1997). Goffman’s social theory, in The Goffman reader, C. C. Lemert and A. Branaman, Editors. Blackwell Publishers: Cambridge (MA). p. xlv–lxxxii.
- [17] Meyrowitz, J. (1985). No sense of place: The impact of electronic media on social behavior. New York (NY): Oxford University Press.
- [18] Meyrowitz, J. (2005). The rise of glocality: New senses of place and identity in the global village, in The global and the local in mobile communication, K. Nyíri, Editor. Passagen Verlag: Vienna (Austria). p. 21–30.
- [19] Nissenbaum, H. (1998). Protecting privacy in an information age: The problem of privacy in public. *Law and Philosophy*. **17**(5–6), p. 559–596.
- [20] Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*. **79**(119), p. 119–159.
- [21] Nissenbaum, H. (2010). Privacy in context: Technology, policy, and the integrity of social life. Stanford, Calif.: Stanford Law Books.
- [22] Walzer, M. (1983). Spheres of justice: A defense of pluralism and equality. New York (NY): Basic Books.
- [23] Goffman, E. (1961). Encounters: Two studies in the sociology of interaction. Indianapolis (IN): Bobbs-Merrill.
- [24] Chris, J. J. (1999). Role distance and the negational self, in Goffman and social organization: Studies in a sociological legacy, G. Smith, Editor. Routledge: London; New York (NY). p. 64–81.
- [25] Mowbray, M. (2001). Does online gender masking work? *International Journal of Communication*. **11**, p. 105–120.
- [26] Turkle, S. (1995). Life on the screen: Identity in the age of the Internet. New York (NY): Simon & Schuster.
- [27] Turkle, S. (1996). Parallel lives: Working on identity in virtual space, in Constructing the self in a mediated world: Inquiries in social construction, D. Grodin and T. R. Lindlof, Editors. Sage Publications: Thousand Oaks (CA). p. 156–176.
- [28] Van den Berg, B. and R. Leenes (2010). Privacy-enabled communities, Deliverable 1.2.1 of the PrimeLife Research Project. Available at: http://www.primelife.eu/images/stories/deliverables/d1.2.1-10.04.23-privacy_enabled_communities-public.pdf.
- [29] Leenes, R. E. (2010). Context is everything: sociality and privacy in Online Social Network Sites, in: M. Bezzi, P. Duquenoy, S. Fischer-Hübner, M. Hansen, G. Zhang (eds.): Privacy and Identity, IFIP AICT 320, Heidelberg, Berlin, New York: Springer, 2010, pp. 48–65.

Received: August 1, 2010

Bibi van den Berg has a PhD in philosophy of technology and holds a postdoc position at the Tilburg Institute for Law, Technology and Society (TILT) of Tilburg University. Her research focuses on privacy and identity in social network sites, and legal and ethical issues in robotics.

Address: Tilburg University (FRW, TILT), P.O. Box 90153, Room M728, 5000 LE Tilburg, The Netherlands,
e-mail: bibi.vandenbergt@tilburguniversity.nl

Ronald Leenes is a full professor of Regulation by Technology at the same institute. His research interests include privacy and identity management, regulation of and by technology, ID fraud, and biometrics.

Address: Tilburg University (FRW, TILT), P.O. Box 90153, Room M708, 5000 LE Tilburg, The Netherlands,
e-mail: r.e.leenes@tilburguniversity.nl