# Context is everything

## Sociality and privacy in online Social Network Sites

Ronald Leenes

TILT – Tilburg Institute for Law, Technology, and Society, Tilburg University, the Netherlands, r.e.leenes@tilburguniversity.nl

**Abstract**. Social Network Sites (SNSs) pose many privacy issues. Apart from the fact that privacy in an online social network site may sound like an oxymoron, significant privacy issues are caused by the way social structures are currently handled in SNSs. Conceptually different social groups are generally conflated into the singular notion of 'friend'. This chapter argues that attention should be paid to the social dynamics of SNSs and the way people handle social contexts. It shows that SNS technology can be designed to support audience segregation, which should mitigate at least some of the privacy issues in Social Network Sites.

## 1. A devilish dilemma?

The satirical weekly the Onion featured[i] an interview with e-mom Gloria Bianco who explained how she as a modern mother copes with her teenage son. The 'interview' shows some of the interesting tensions of current social software:

> "Today now!: Now we've all heard the term Facebook, but we may not know that you may use it to keep tabs on your childrens' personal lives even when they're far away from home. E-mom Gloria Bianco: "You can. You're gone love this. It's so easy, all you do is create this profile and search for your son or daughter's name and add them to your list of friends. Within minutes you can be writing on their wall. … I look through all of my son Jeffrey's photo's every single day. ... Now I can see here he is with this young women with the low cut shirt showing a lot of skin. [interviewer: looks like he has a lot of fun] Girls like that like to have fun. ... By this feature called tagging I can find out the girl's name. ... Facebook won't allow me to see her entire profile, but I can get a good enough idea what she's like by looking at this trampy picture. ... You can see pictures posted by any of their other friends....".

Although the accompanying footage is amusing, the text itself is hardly satirical because it very much reflect current practice on social network sites. The quote illustrates one of the prominent issues of social software, the difficulty of separating audiences online. Information disclosed to friends, can just as easily be seen by moms, teachers, and bosses, which is certainly not always what the author intended.

With this enormous rise in possibilities for social interaction offered by online social network sites, also serious privacy issues have risen. People are judged by the image they paint of themselves on their profile page (and on those of others) and by what others contribute to their profile by means of comments, tags, media uploads, etc. The consequences of these judgments may be serious. Students have been expelled from universities, employees have been fired[ii], and even people have been killed[iii] as a result of the information disclosed by themselves and others on their profile pages.

Information that is suitable in one context may be entirely unsuitable in the next. This is what causes a devilish dilemma. One may prevent many of the privacy issues promulgated by online social networks by abstaining from using them, but this goes at the expense of sociability; it may become lonely when not engaging with friends online. On the other hand, choosing for a rich social online life currently seems to introduce a set of serious privacy issues that most people would rather live without. How should we cope with this dilemma? Do we have to choose between privacy and sociality, or is there a middle ground?

We believe that privacy and sociality can be reconciled in the sense that some of the privacy issues, namely decontextualisation, can (partially) be resolved. Doing so requires understanding of the social dynamics of online social network sites. James Grimmelmann [1] has argued that many policy options, including technical controls, won't work to restore the privacy imbalances in social network sites. In this chapter, I will argue that, although Grimmelmann gets it right regarding the social dynamics and reasons why users engage in online social networks sites, he may underestimate the potential of technology to mitigate privacy risks.

This chapter is organised as follows. First, I will set the stage by introducing the main features of social network sites and describe some of the prominent privacy issues in social network sites. Next, I will explore some of the reasons why users are on social network sites despite these issues. Then I will illustrate how, in our view, technical controls can help reconcile sociability and privacy. Finally, I will draw some conclusions and propose suggestions for further work.

## 2. Why bother about social network sites: privacy issues

Social network sites inhabit the world of web 2.0 applications. A common definition of social network, or networking, sites is provided by danah boyd and Nicole Ellison [2] who describe them as:

> 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.

As Grimmelmann [1] points out, this definition highlights three important aspects of social networks: identity, relationship, and community. Apart from these characteristics, there is a huge variety in goals, functionality, and appearance of the different applications that span the SNS universe. Some networks target a professional context, such as LinkedIn, while others, such as Myspace or Facebook, primarily aim at leisurely contacts. Some focus on text based interactions and blogging (e.g., Livejournal.com), others tend towards multimedia (e.g., Flickr.com). Some networks are geared to maintaining existing ties (e.g., Classmates.com, Sixdegrees,com. See also the chapter by Isabelle Oomen in this volume), others facilitate finding new contacts (e.g., Match.com) and creating new networks. More and more SNSs move away from a profile centered application towards a general gathering ground for networks of related individuals (friends) [3], combining the functionalities of different kinds of social software, such as blogs, twitter, and rss-feeds. Web 2.0 has supplemented, and in some places replaced, 'real world' interactions.

Online social networks and other social software have conquered the Internet in a relatively short time. Modern profile based social networks followed in the footsteps of Classmates.com which was founded in 1995. In November 2009, Facebook passed the 300 million user bar and the social networks combined easily have more than a billion users, each of whom spends a considerable amount of time maintaining their online presence and interacting with their friends (e.g., Myspace, Hyves, StudiVz, Facebook) and professional contacts (e.g., LinkedIn). In PEW study conducted in late 2006, they found that 55% of online teens aged 12-17 have created profiles on social network sites with 64% of teens 15-17.[iv] Hyves, the major Dutch SNS has about 9.5 million users (on a population of 16 million), StudiVZ, a popular German SNS for students (in a broad sense), claims to have over 15 million users.

These data provide a flattered image of the size of the networks, because many networks do not provide a way to completely terminate an account. A reason for this is that bigger networks are attractive for both potential users and advertisers. SNS providers therefore have an interest to keep accounts in their system.

Users of Social Network Sites spend a fair amount of their time online nurturing their profile and keeping in touch with their network. It is well known that many SNS users are very frank and open on their profiles and in their communication, to the point that many 'adults' wonder whether these teens have completely lost it. Consequently, there is extensive literature on the (privacy) risks associated to Social Network Sites, coming from both academics, such as [1, 4-6], and policy makers and advisory bodies, such as [7-9].

In PrimeLife heartbeat 1.2.5 [10], we have collected some 30 privacy and security issues in social network sites based on sources such as the ones mentioned in [1, 4-6] and [7-9]. Many of the issues can be understood as emanating from the underlying properties of mediating technologies [11]:

"1 Persistence: Unlike the ephemeral quality of speech in unmediated publics, networked communications are recorded for posterity. This enables asynchronous communication but it also extends the period of existence of any speech act.

2 Searchability: Because expressions are recorded and identity is established through text, search and discovery tools help people find like minds. While people cannot currently acquire the geographical coordinates of any person in unmediated spaces, finding one's digital body online is just a matter of keystrokes.

3 Replicability: Hearsay can be deflected as misinterpretation, but networked public expressions can be copied from one place to another verbatim such that there is no way to distinguish the "original" from the "copy."[v]

4 Invisible audiences: While we can visually detect most people who can overhear our speech in unmediated spaces, it is virtually impossible to ascertain all those who might run across our expressions in networked publics. This is further complicated by the other three properties, since our expression may be heard at a different time and place from when and where we originally spoke." [11]

These properties are certainly at play in social network sites. Let me briefly explore some of the specifics of these properties in the light of social network sites. Although SNS users have control over their own profile, it is generally difficult to eradicate their online existence entirely because in many cases it is difficult to delete their profile entirely.[vi] This means that information contributed to social network sites has a high degree of persistence.

Searchability provides an interesting issue because of the privacy–sociality tradeoff that is inevitable in social network sites. SNS profiles consist of a public part which is available to non SNS-members, as well as a part that can be restricted to a designated audience, typically consisting of the user's contacts labelled as 'friend'. Basically anyone can observe a public profile, provided one knows where to look. Google does not provide much help here, because it is blocked from indexing many SNS sites. In that sense, SNS's seem to have limited searchability and hence taken steps to mitigate a common privacy issue on the Internet at large. In practice this is not much of a problem because some SNS providers, such as Facebook and Hyves, require their users to register by their real names. In general there is an incentive for SNS users to be searchable; they want to attract (their) friends within a particular SNS. By choosing to make their profile non-public, users can limit access to their profiles. This prevents 'non-authorised' others (parents, teachers, bosses, etc.) from accessing their profile, but this comes at the expense of potential peers and friends being unable to find them, which clearly interferes with the social nature of the network.

The most important issue, however, seems to be the invisibility of audiences. Do SNS users have a thorough understanding of their audience? A study by Ralph Gross and Alessandro Acquisti [12] among Facebook users (in 2005) revealed that many users generously provide personal data in their profile, while hardly limiting access to their profiles. From their study it is unclear whether users don't understand their potential audience, or simply think that the benefits of disclosing their data outweigh the risks [12] (See also Oomen's contribution in this volume). Their later study [6] revealed that a large proportion of their sample is aware of the visibility of their profile, although a significant minority is not. Perhaps due to media attention, users appear to change their behaviour. SNS users are increasingly locking their profiles and culling their friends list (which lead to the new terms defriending/unfriending)[vii].

Given the persistence of information disclosed online, a culminating effect on top of the issue of opaque current audiences, is that also future audiences are unclear. Add to this that contexts may blur, and undesired and unexpected effects are guaranteed. What may seem appropriate information to put up for a particular audience on a profile page now, may be inappropriate information later on in a different context. Tufecki provides an example of this:

> "For 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."[13]

Judith Donath and danah boyd provide another example of why decontextualisation may be undesirable. One of the respondents in their study says:

> 'My issue with Tribe is that the boundaries between personal and professional are TOO fuzzy. I want to get to the person, rather than to the pitch. On the other hand, I really DON'T want to know that the person I'm getting ready to do business with is in an open marriage and into kinky redheads. I don't want to see half-naked pictures of them from Burning Man. It's not that I'm a prude, or offended by that stuff in general, it's just not stuff that I want to have pushed on me when I'm talking business'.[14]

A significant problem is that social networks invite or even encourage snooping. In fact, as Joinson [15] and Lampe et al. [16] show, surveillance and social browsing are important reasons for users to spend time on the social networks. And hence, the networks facilitate content decontextualisation.

We will return to this central issue of audience segregation and contextual integrity later. First we need some understanding of why a large proportion of contemporary teenagers engage in online social network sites when it is apparent that these provide privacy risks. The short answer is: People have compelling social reasons to use SNSs and those same social factors lead them to badly misunderstand the privacy risks involved.

## 3. If you're not on Myspace, you don't exist

For a more extensive answer to the question why on earth teenagers behave exhibitionistic online, we have to look at the social dynamics of social networks. One of the prominent researchers of 'teen sociality' in the information society is danah boyd. In her PhD thesis [17] and elsewhere [5, 11, 18] she has extensively described what moves teenagers to participate in online social network sites. A prominent reason is "because, that's where my friends are" [11]. Large scale online presence of teenagers is a network effect. The value of the network lies in its size and hence they become more attractive as they grow, and conversely, when people flock the network in large numbers the decline will progress non-linear.

There is more to it than just the network effect. The three primary characteristics of Social network sites: identity, relationship, and community [1, 11] are really at play. Teenagers are in a phase in their lives where they are particularly busy with constructing their identity. Identity construction involves playing roles: theatrical performances [19]. In their performances, individuals consciously present themselves to others (information given), but also provide unconscious signals (information given off). Identity in Goffman's analysis is constructed by the roles people play and the "front" they uphold. The front consists of the "setting", objects, furniture, backdrop, but also consists of a more personal side: clothing, social position, age, gender, body language etc. Maintaining a profile on a social network site is part of this identity construction. The users "write themselves literally into being" as Jenny Sundén expresses it [20]. The users adapt their identity and their profiles on the basis of the reactions of their peers. This process of performance, interpretation, and adjustment is what Goffman calls impression management [19]. Note that impression management is not only done by teens who are in their early stages of identity development, but is an important aspect of everyday social life for all of us, albeit that identity is more stable in later stages of life for most of us.[viii]

The SNS platforms contain different mechanisms to provoke active identity construction. For instance, many sites facilitate the users to customise significant aspects of the 'experience' by allowing them to change the backgrounds of their profile, and modify the CSS stylesheets employed on their pages. Simply browsing through the public profiles on any site will reveal a multitude of different styles, backgrounds etc; many may look utterly horrible, but so do many teenager bedrooms. In any case these customised backgrounds are individual expressions and hardly ever accidental. There are also other ways in which SNS platform providers promote activity on the profile pages. Most SNS platforms allow other users to post comments on a profile page. On Facebook this is called 'the wall'. These postings create communication between the profile owner and visitors because generally the owner will respond to the comments, for instance by updating or chancing the page. Facebook holds several patents, some of which are related to inducing users to actively nurture their pages and interact with other users.[ix]

The second important feature of social network sites that explains why SNS' attract (teenage) users is relationship. SNSs allow their users to attract others on a one-to-one basis; they can invite others to become their friend, for instance. Although the act of adding someone as a contact is a multivalent act [1] because it can mean anything from "I am your friend" to "I don't even know you(, but still want to be associated to you)", it signals a link between two individuals and shows that people care about each other. Therefore even simple communication between users, such as writing on someone's wall "I'm saying something to you on your comments so that you'll feel loved"[x] gives people the idea that they are appreciated. Profiles are also used to get into contact with potential soulmates, also for, or maybe even especially for those who are not the centre of attention in the offline world. danah boyd quotes a typical example of this:

> "I'm in the 7th grade. I'm 13. I'm not a cheerleader. I'm not the president of the student body. Or captain of the debate team. I'm not the prettiest girl in my class. I'm not the most popular girl in my class. I'm just a kid. I'm a little shy. And it's really hard in this school to impress people enough to be your friend if you're not any of those things. But I go on these really great vacations with my parents between Christmas and New Year's every year. And I take pictures of places we go. And I write about those places. And I post this on my Xanga. Because I think if kids in school read what I have to say and how I say it, they'll want to be my friend." – Vivien, 13, to Parry Aftab during a "Teen Angels" meeting, taken from [11]

The networks provide shy teenagers a platform to advertise themselves in a relatively safe way. They have control over their own page and can shield themselves (and remove) from insults more easily than in the real world.

The third characteristic that helps attract users to social network sites is community. Community is about doing things together and sharing thoughts and ideas with a group, but it is also about social position and social capital. The size of one's network, for instance, is clearly visible to outsiders and provides a marker of how well connected one is, and maybe how popular one is. The importance of a sizeable community is not absolute though. On Friendster the urge by some users to collect as many friends as possible has inspired the notion of "Friendster whore" [14], which carries a connotation of undesirable social behaviour. On the other end of the spectrum there is the careful pruning of networks, "defriending"[xi], to only include contacts that are valuable as social capital. Within one's network there are also all sorts of subtle processes. Some sites, such as Myspace, allow their users to list their top 8 friends. This represents clear indicators of the social position of people within one's network and inspires wall postings such as "Hey ZOE!!! WHAT THE HELL!!! Why aren't I on your top friends?"[xii]

The wall also functions in delineating social positions. At first glance, wall postings are awkward ways of communicating between individuals because they show only one side of a two-way communication channel. The reader, unless she has access to the profile page of the poster too, only gets to see the communication posted by the poster, not the responses by the profile owner. Email, or MSN, at first glance seems a more appropriate communication channel for such bilateral communication. However, on closer inspection, the wall – as its name already suggests –, has a social function that extends beyond the two primary actors in the communication. A wall post communicates certain content to the profile owner (and others who have access to the page), but it also shows others the author's affection to the profile owner and therefore provides a public display of this affection. Wall posting consequently are signals of one's social position within a network. The name "Wall" also reinforces the idea that social network sites are closed-off spaces, thus encouraging openness. Interestingly walls have two sides, an interior side and an exterior one. On the one hand the users may feel themselves enclosed, and hence safe, by the wall. One may also consider the wall to be the outside of a profile and writing on the wall something that happens on the exterior wall, much like spray painting graffiti (with its own cultural references and customs).[xiii]

Online social networks provide their users the tools for online identity construction and socialisation. As danah boyd wrote in a recent blog post:

> "Many youth spend little to no time in unstructured social settings, otherwise known as 'hanging out.' The practice of hanging out is consistently demonized by educationally-minded folks as a waste of time. Yet, it is in that space where youth learn to navigate social situations, make sense of impression management, and develop the social skills necessary to be productive adults. Social media has created an interesting rupture in the landscape. Youth turn to it to reclaim unstructured social encounters, to create a public space that allows them to simply hang out with their friends, peers, and cohort. The flirting, gossiping, and joking around that takes place is not proof that social media is useless, but

> proof that it's extremely valuable. Without other spaces in which to gather, youth have developed their own."[xiv]

Apart from being relevant for socialisation, SNSs feature both explicit and subtle mechanisms that attract users to participate, and since social networks sites are about sharing thoughts, experiences, ideas, media, etc, their users will disclose information.

## 4. None of this is real

That users have to share information on social network sites does not explain why they share so much information. Just as different SNS users will have different reasons for joining an SNS, there are different reasons why they may over-expose themselves. One obvious reason is that SNS users may underestimate and misunderstand the risks. Grimmelmann [1] lists a couple of heuristics that guide people in detecting harms that do not seem to work properly in online social networks. For example, users adhere to "safety in numbers"; they feel safe in the crowd and ask themselves why anyone would be interested in (harming) them specifically? The chances that their personal indiscretions will make it to the headlines of the newspapers indeed are limited, but there are sufficient numbers of people interested in them and especially in their behaviour, such as parents, teachers, and later their employers. And as already mentioned, given the fact that many subscribe under their real name, finding them in the crowd is not that hard.

Several studies have pointed out that users do not have an accurate risk perception of the privacy risks. Ralph Gross and Allesandro Acquisti, for instance, in two studies among Facebook users [6, 12] found that although a relative majority of their sample (4000 students at a US academic institution) are aware of the visibility of their profile, a significant minority is not. Their sample also turns out to be highly ignorant of Facebook's treatment of personal data. Zeynep Tufekci [13] found that non SNS users only have slightly higher levels of privacy concerns than users (average score 2.98 resp. 2.73 on a scale from 1 = not concerned at all to 4 = very concerned). The perceived likelihood that future employers, government, corporations, or romantic partners would see their profile did not affect the actual visibility of their profiles. The students in the samples did not find any of those scenarios very likely, except for future romantic partners. Although these latter findings do not suggest that the respondents underestimate the risks (as we do not know the actual risks very precisely), the fact that they consider "others" not interested in their profiles us telling in the light of news paper reports to the contrary (see the examples quoted in the introduction).

A common advise to counter the relative ignorance of the SNS users is to raise their awareness. This advice can be found in many policy recommendations, such as [7-9].

> "Recommendation SN.1 Encourage awareness-raising and educational campaigns: as well as face-to-face awareness-raising campaigns on the sensible usage of SNSs, SNSs themselves should, where possible, use contextual information to educate people in 'real-

> time'. Additional awareness-raising campaigns should also be directed at software developers to encourage security- conscious development practices and corporate policy."[7]

Sound as this advise may be, it is only part of the solution and may even address the wrong issue. This becomes clear when the social dynamics of the networks is scrutinized more closely. Not all SNS users are the same and hence their behaviour, although superficially equal, makes a difference when assessing it against privacy risks. One of the interesting conclusions that is drawn by various researchers, including [11, 18], is that SNS users that are aware of the fact that they operate in public space claim privacy in this public space. SNS users are not addressing the whole audience that has access to the information they publish, but rather they address their "friends" and implicitly expect others to stay out. As one kid in a kids' panel on the Revealed "I" conference 2007 in Ottawa formulated it: "Parents are not allowed in. It's my conversation". This idea may sound counter intuitive, after all is there privacy in a public space anywhere?[xv] But when compared with secret diaries which are also not supposed to be read by curious parents, this call for privacy is not at all odd. Although enforcement of a ban on unsolicited observing (public) profiles is untenable, promoting a social norm that also on social network sites it is inappropriate to overhear other people's conversation may make sense.

A final phenomenon to keep in mind when addressing privacy on social networks is that not everything is what it seems. Computers and the internet are ideal places where people can experiment with their identities and explore the boundaries of their personality [21], and this is even more so in social network sites as we have argued above. In actual practice many online profiles are fairly close to the offline identities of their creators. In other words, identity experiments are limited. There is, however, a group of SNS users that takes experimenting with their identities to the extreme. The most outspoken in this category are the Friendster Fakesters [18].

> "From the earliest days, participants took advantage of the flexibility of the system to craft 'Fakesters,' or nonbiographical profiles. Fakesters were created for famous people, fictional characters, objects, places and locations, identity markers, concepts, animals, and communities. Angelina Jolie was there, as were Homer Simpson, Giant Squid, New Jersey, FemSex, Pure Evil, Rex, and Space Cowboys." [18]

Fakesters create profiles that are totally unlike themselves for different reasons and their story makes an interesting read, but the point I want to make is that not everything in SNS profiles is real and therefore not all information provides privacy risks in the same way. Since for Fakesters it is all a game, they may disclose an abundant amount of personal information and not seem to care about privacy at all. We, outside observers, may think that the information is real, whereas in their view it is a scam and the dark sides of information (mis)use by others may not affect them. An issue of course is that judgments are made irrespective of whether the information is accurate and therefore also fake profiles may have real consequences for their creators.

## 5. Sociality or privacy?

I have provided a glance of why people, and especially teenagers, populate online social network sites and outlined some of the risks of exposing personal information on these sites. I want to use the remainder of this chapter to explore whether we have to choose between sociality and privacy, or whether we can have both. One of the key privacy issues on social network sites is the way social structures are handled. Whereas in real life we have family, friends, best friends, colleagues, team mates, lovers, ex-lovers, etc, most online social networks only recognise a very shallow subset. Linked-in only recognises professional contacts. Other networks, such as Facebook, Myspace, and Hyves, divide the world into "Friends", "Friends of friends" and the "rest", although admittedly they are all implementing more fine grained models. On the relationship level, most share similar model of interpersonal links – they are mutual, public, unnuanced, and decontextualised [14] which does not really go well with the nuances of relations in the real world. In social network sites, links are

- unnuanced, i.e., "there is no distinction made between a close relative and a near stranger";
- decontextualised, i.e., "there is no way of showing only a portion of one's network and content to some people";
- mutual, i.e., "if A shows B as a connection, then B has also agreed to show A as a connection"; and
- public, i.e., "they are permanently on display for others to see"

One way of improving on this is by facilitating "audience segregation" in social network sites. The concept of 'audience segregation' was coined by Canadian sociologist Erving Goffman [19]. As we have seen above, Goffman casts the process of identity construction in a stage metaphor. The social actor plays different roles for different audiences and chooses stage, props, and costume to perform for these audiences. Individuals aim to present consistent and coherent "faces" in the different contexts. Authors such as Goffman [19] and Rachels [22] have extensively argued that people need to be able to keep audiences apart in order to develop themselves and engage in meaningful relations. Part of keeping audiences apart is revealing only part of oneself in a specific context and hence show different faces in different contexts. Goffman describes "audience segregation" implies "… that the individuals who witness him in one of his roles will not be the individuals who witness him in another of his roles" [19, p. 137]. One of the reasons for this need is the possibility to maintain different roles, e.g., spouse/parent; employed professional/spokesperson for a professional, teacher/student, scout-master and spy. This aspect of control over one's image or presentation corresponds to Goffman's notion of information given (versus information given off). Individuals often maintain or are assigned different partial identities for specific contexts (e-government, e-commerce, social networks, et cetera) and roles (citizen, consumer, friend, relative, employee, student, et cetera). Audience segregation prevents their image to be contaminated by information from other roles performed in other situations before other audiences, particularly by information that may discredit a convincing performance in the current situation [19, p. 137].

The simplistic social model implemented in most online social network sites totally neglects this crucial social mechanism and accounts for many of the privacy issues in social network sites. The information that causes many of the real world issues was simply not intended for the audience that caused the problems.

Not only does the lack of possibilities to keep audiences apart lead to privacy issues, it also in the longer run changes people's behaviour that undermines having meaningful social relations. It leads to 'flat characters', users who in their aim to be acceptable to all audiences leave out the "interesting" stuff. This is what danah boyd calls social convergence.

> "Social convergence occurs when disparate social contexts are collapsed into one. Even in public settings, people are accustomed to maintaining discrete social contexts separated by space. How one behaves is typically dependent on the norms in a given social context. How one behaves in a pub differs from how one behaves in a family park, even though both are ostensibly public. Social convergence requires people to handle disparate audiences simultaneously without a social script. While social convergence allows information to be spread more efficiently, this is not always what people desire. As with other forms of convergence, control is lost with social convergence. [23, p. 18]

If we can re-introduce the notion of audience segregation into online social network sites, we may be able to reconcile privacy and sociality, provided that users maintain their presences on the social network sites and are capable and willing to disclose information to the proper audiences.

## 6. Technologically assisted sociality

The idea of implementing audience segregation into social network sites is not new. For instance, Donath and boyd already in 2004 proposed:

> "A more promising design solution is the ability to define a set of categories and designate each person as a member of one or more of these categories. One could then set which sections of one's profile or people in one's network were for viewing by particular acquaintances. Thus, to close friends one might still show everything, but one could have a category of 'work colleagues' who would see only work related information, and not be made aware of the more outrageous connections. This faceting of profile and network would not be apparent to anyone unless two people sat down and compared what each could see of a third; that is analogous to real world situations in which two people discuss a third whom they each know in a different context." [14, p. 78]

Others are less optimistic about this idea. Grimmelmann, for instance writes:

> "The fact is, there's a deep, probably irreconcilable tension between the desire for reliable control over one's information and the desire for unplanned social interaction. It's deeply alien to the human mind to manage privacy using rigid ex ante rules. We think about privacy in terms of social rules and social roles, not in terms of access-control lists and file permissions. … The deeper problems are social. There are no ideal technical controls for the use of information in social software. The very idea is an oxymoron; "social" and

> "technical" are incompatible adjectives here. Adding "FriendYouDontLike" to a controlled vocabulary will not make it socially complete; there's still "FriendYouDidntUsedToLike." As long as there are social nuances that aren't captured in the rules of the network (i.e., always), the network will be unable to prevent them from sparking privacy blowups. [1, pp. 1185-1186]

This is where we disagree with Grimmelmann, although we agree with him on the general principle that regulating social behaviour by technology is problematic. Having said that, let us outline how we try to implement audience segregation, or technologically assisted sociality, in social network sites in the EU funded PrimeLife project.

Grimmelmann seems to assume that technological controls by definition are complex and that there is no context at all which would require a very fine granularity, which "can also make problems of disagreement worse." [1, p. 1087], and defaults will not help either":

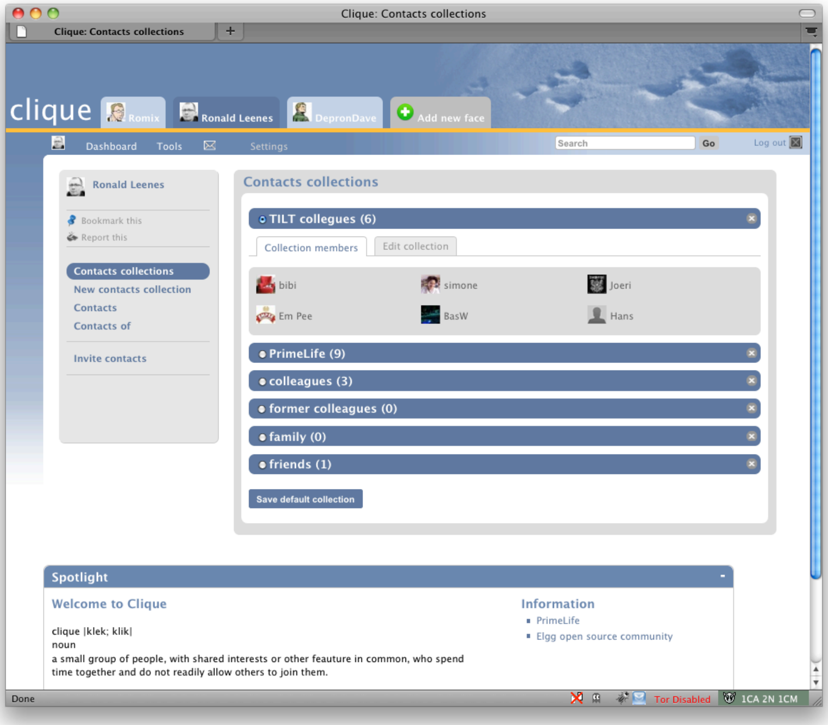
> "If I want to share information about myself—and since I'm using a social network site, it's all but certain that I do—anything that makes it harder for me to share is a bug, not a feature. Users will disable any feature that protects their privacy too much. The defaults problem nicely illustrates this point. Lillian Edwards and Ian Brown flirt with the idea that default "privacy settings be set at the most privacy-friendly setting when a profile is first set up," only to recognize that "this is not a desirable start state for social networking." If Facebook profiles started off hidden by default, the next thing each user would do after creating it would be to turn off the invisibility." [1, p. 1087]

We come from a different direction. We start from the assumption that mechanisms used in everyday off-line life can be implemented to assist people in their online life provided that the concepts are 'intuitive' to the user and the interface does not hamper them in their social activities. Additionally, we think we can 'Nudge' SNS users to act in a privacy savvy way without undermining sociality. This is done by [24] taking Thaler and Sunstein's Nudge 'methodology' into account: provide iNcentives, Understand mappings, Defaults, Give feedback, Expect error, Structure complex choices. The prototype application that implements our ideas is called Clique and is built on the open source SNS platform Elgg[xvi].

Our work builds on a number of premises. The first is that every user operates in different social contexts with distinct members. These contexts have a social meaning and can hence be labelled. For instance, I might want to distinguish between family, colleagues, professional acquaintances, and friends, whereas the reader might want to distinguish entirely different categories, depending on their personal goals and uses of a particular social network. We call these social groups "collections". Each of the collections consists of a number of known contacts of the profile owner.

The notion of labelled social group is not uncontested. Grimmelman cites the RELATIONSHIP project which aims to provide a "vocabulary for describing relationships between people", using terms like "lostContactWith", and "apprenticeTo" [1]. He cites Clay Shirky who argued the fundamental flaws of such enterprises because it is very hard to represent the enormous complexity of social relationships (where, for instance is "closePersonalFriendOf", or “usedToSleepWith”) and Facebook’s inability to represent this social complexity. Our point is that the platform provider certainly can not provide the entire social complexity; there is no need for them to do this in the first place. Individuals are fully capable of representing whatever works for them. They can decide on the necessary granularity as well as on the labels they want to stick to their social categories.

While users should be able to define their own audiences within the SNS, others should not be able to inspect how a user has compartementalised their world. I may call a certain collection “idiots”, but there is no need that the members of this collection are aware that they are considered idiots. Users should also be capable of deciding which of their contacts belong to the different collections. Of course this is not static, but we expect changes in the overall structure to be relatively scarce. Maintaining ones network by no longer involving ex-lovers into all communication is something that is done in the real world as well. Figure one, shows the collections that the author has defined for one of his identities (labelled Ronald Leenes) within the PrimeLife Clique prototype. Collections can be managed by dragging contacts in or out a particular collection. Figure one also shows another feature of the prototype,



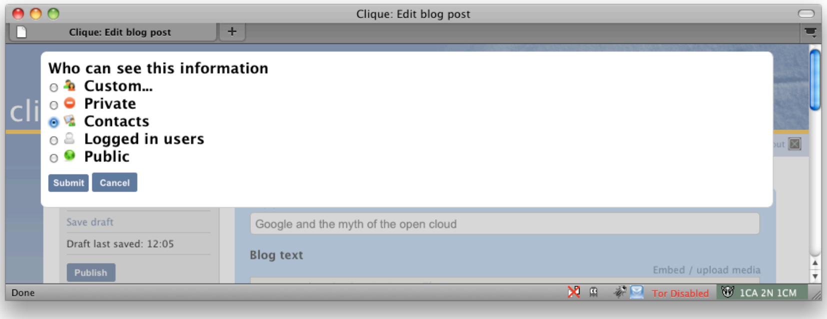
Welcome to Clique

clique |klek; klik|
noun
a small group of people, with shared interests or other feauture in common, who spend time together and do not readily allow others to join them.

Figure 1. The author’s contact collections and default collection (TILT colleagues).

the possibility to maintain different faces within the same SNS. The picture shows my professional face, one in which my real name is known. It also shows two contexts in which I operate under pseudonyms (Romix and DepronDave). These two identities represent me in my hobbies. Clique allows me to maintain my different spheres within the same software environment. This allows the user to manage a single address book and easily share data between these different spheres while still being able to control linkability.

Our second assumption is that we presume that each SNS user has a core audience in the SNS which basically reflects the primary reason for being present in the SNS. For a majority of SNS users, their core audience will consist of their immediate friends (Facebook, Hyves), for some networks, the core will more likely consist of professional contacts (Linked-in). This allows us to make assumptions about the users' behaviour. A sensible default is to assume that the user primarily wants to disclose information to this core audience, and if so, no special action should be required. This is implemented as follows. Posting information on the SNS requires the user to press the [publish] button. Subsequently a save information dialogue appears such as shown in figure 2. By default, custom will be selected and within custom the default collection – the user's core audience – will be pre-selected (as shown in figure 3). Under most circumstances this represents what the user wants to do, so pressing [submit] will do to publish the information on the SNS. Showing the user the currently selected audience (as in figure 3) will help prevent accidental data spills.



Who can see this information
○ Custom...
○ Private
● Contacts
○ Logged in users
○ Public

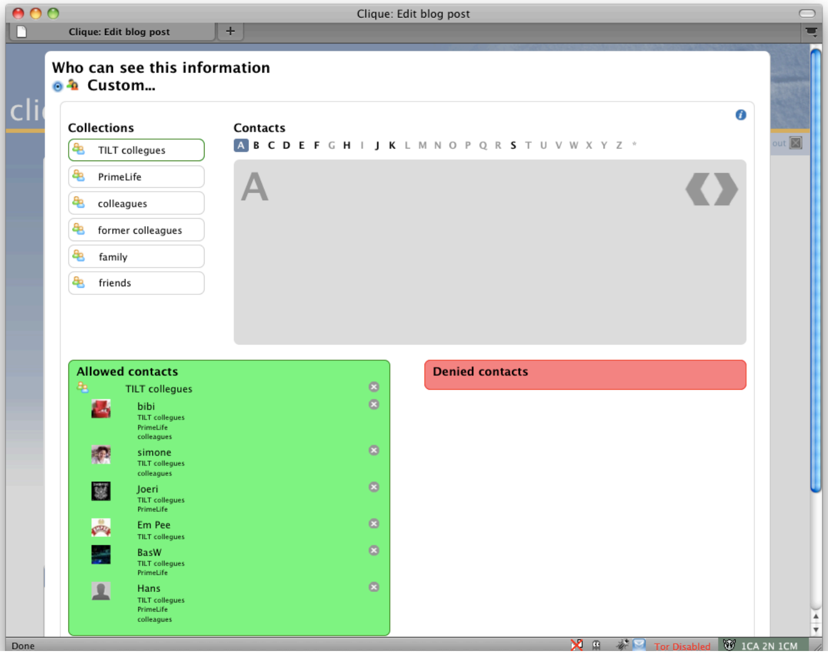
Draft last saved: 12:05

Google and the myth of the open cloud

Blog text

Figure 2. Save information dialogue.

This publication mechanism applies whenever the user creates or modifies any 'blob' of information on the SNS, such as posting a comment, writing a blog entry, or modifying a profile attribute. The save information dialogue allows the user to customise the audience by either selecting private, their own contacts, logged-in users, public, or make more fine grained choices in the Custom panel where they can drag contacts and collections in or out the audience for the particular blob of information (see figure 3). The mechanism as implemented nudges the user to disclose information to their likely intended audience (their preferred collection) without hindering making different choices.



Clique: Edit blog post

Who can see this information

Custom...

Collections

- TILT collegues
- PrimeLife
- colleagues
- former colleagues
- family
- friends

Contacts

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z *

A

Allowed contacts

TILT collegues

bibi — TILT collegues, PrimeLife, colleagues

simone — TILT collegues, colleagues

Joeri — TILT collegues, PrimeLife

Em Pee — TILT collegues

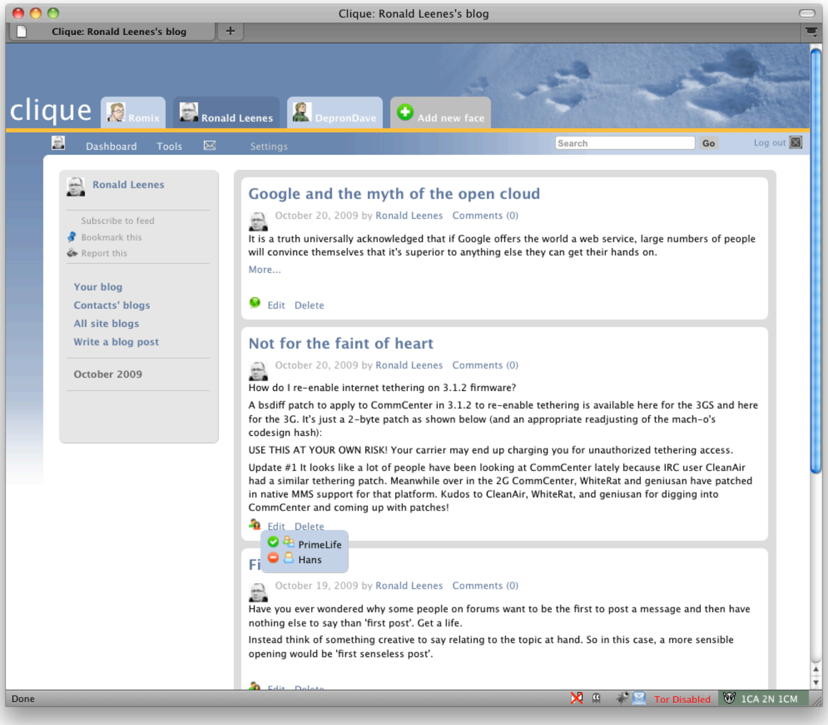
BasW — TILT collegues, PrimeLife

Hans — TILT collegues, PrimeLife, colleagues

Denied contacts

Figure 3. Default audience pre-selected in custom target audience dialogue panel.

The third assumption is that access control policies should be set on on all data disclosed in the SNS and should be as easy as possible. These policies should be as simple as possible. The access control mechanism in Clique allows the user to specify which collection and/or individuals have access to certain information. In the case of collections it should be able to exclude individual members from certain information. For instance, I may want to exclude a particular friend from discussions



Clique: Ronald Leenes's blog

Ronald Leenes

**Google and the myth of the open cloud**

October 20, 2009 by Ronald Leenes Comments (0)

It is a truth universally acknowledged that if Google offers the world a web service, large numbers of people will convince themselves that it's superior to anything else they can get their hands on.

More...

Edit Delete

**Not for the faint of heart**

October 20, 2009 by Ronald Leenes Comments (0)

How do I re-enable internet tethering on 3.1.2 firmware?

A bsdiff patch to apply to CommCenter in 3.1.2 to re-enable tethering is available here for the 3GS and here for the 3G. It's just a 2-byte patch as shown below (and an appropriate readjusting of the mach-o's codesign hash):

USE THIS AT YOUR OWN RISK! Your carrier may end up charging you for unauthorized tethering access.

Update #1 It looks like a lot of people have been looking at CommCenter lately because IRC user CleanAir had a similar tethering patch. Meanwhile over in the 2G CommCenter, WhiteRat and geniusan have patched in native MMS support for that platform. Kudos to CleanAir, WhiteRat, and geniusan for digging into CommCenter and coming up with patches!

Edit Delete

✓ PrimeLife

⊖ Hans

Fi

October 19, 2009 by Ronald Leenes Comments (0)

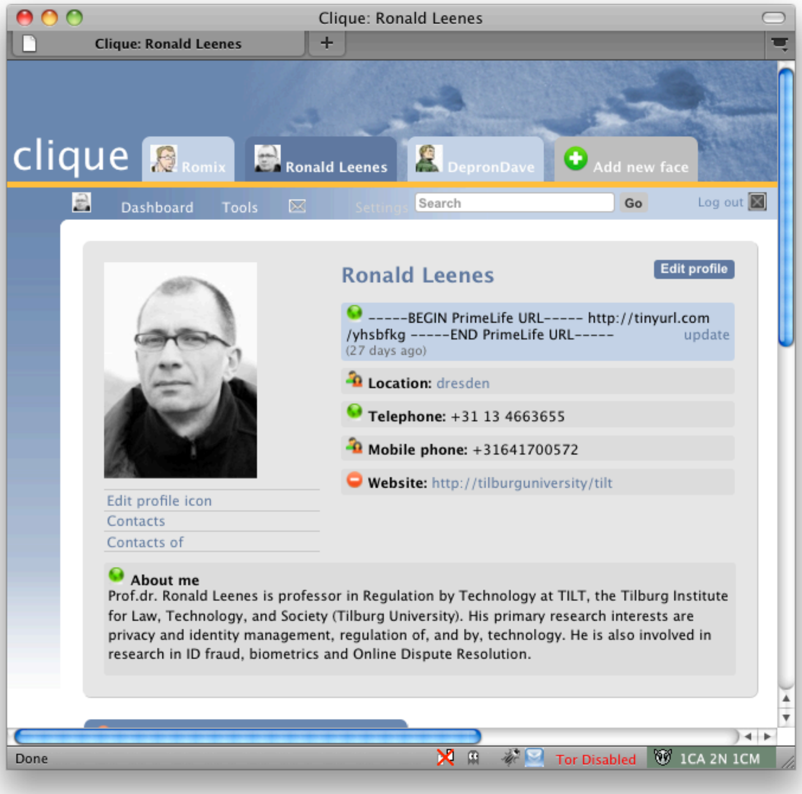
Have you ever wondered why some people on forums want to be the first to post a message and then have nothing else to say than 'first post'. Get a life.

Instead think of something creative to say relating to the topic at hand. So in this case, a more sensible opening would be 'first senseless post'.

Edit Delete

Figure 4. Visual audience indicators.

about a birthday present in order to maintain an element of surprise during her birthday party, something we also do in real life.
All information in the SNS contains visual indicators of the current audience. Figure 4 shows that the Google blog entry is open to the public at large (green globe icon), while the “Not for the faint of heart” post is restricted to a collection (two figures icon), in this case the PrimeLife members, minus “Hans”. Each item on the SNS can be assigned its own access control policy (see figure 5 for an example of the profile page).



Ronald Leenes

-----BEGIN PrimeLife URL----- http://tinyurl.com/yhsbfkg -----END PrimeLife URL-----
(27 days ago)

**Location:** dresden

**Telephone:** +31 13 4663655

**Mobile phone:** +31641700572

**Website:** http://tilburguniversity/tilt

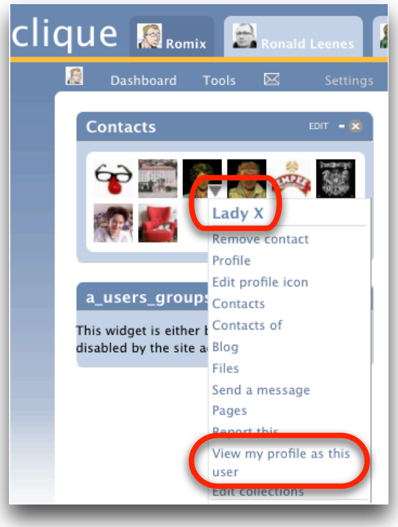
**About me**
Prof.dr. Ronald Leenes is professor in Regulation by Technology at TILT, the Tilburg Institute for Law, Technology, and Society (Tilburg University). His primary research interests are privacy and identity management, regulation of, and by, technology. He is also involved in research in ID fraud, biometrics and Online Dispute Resolution.

Figure 5. Profile with access control policies on each attribute.

One can also view one’s own profile from the perspective of another user (figure 6). Contact icons feature a contextual menu (activated by mousing over the bottom-right corner of the icon) which, apart from options such as remove from my contact list, contains an option ‘view my profile as this user’). These visual indicators should help the user to determine whether the image of themselves they think they project conforms to what others within the SNS actually see of them. This helps them maintain control over their audiences.

## 7. Conclusion

Context is a central concept in the disclosure of information. What is appropriate in one context is not in another. We have argued that most current online social network sites have a very simplistic model of social structures which creates many privacy issues. In our view, technology can be adopted to help users maintain different partial identities en control who can access their data even in social networks. We have developed a prototype that implements the core ideas. At the time of writing large online social network sites, such as Facebook and Hyves are clearly migrating to similar ideas, albeit currently less developed.



This widget is either b
disabled by the site a

Figure 6. Contextual menu for contacts.

Whether or not SNS users can and will use the mechanisms provided remains to be seen. To test whether they do, we have set up an experimental site consisting of the Clique prototype (http://clique.primelife.eu). During 2010 we will try to attract real SNS users to use the platform in order to test the concepts and further improve the notions.

Part of the research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement No. 216483. The author wants to thank Joeri de Ruiter who did a tremendous job of implementing the ideas of the author and Bibi van den Berg into the Clique application.

## 8. References

1. Grimmelmann, J.T.: Saving Facebook. NYLS Legal Studies Research Paper No. 08/09-7 (2008)
2. boyd, d.m., Ellison, N.: Social Network Sites: Definition, History, and Scholarship. J. Computer-Mediated Comm. **13** (2007) art. 11
3. Berg, B.v.d., Beato, F.: H1.2.6 – Audience segregation in social network sites [SNSs]. PrimeLife Consortium (2009)
4. boyd, d.: Social Network Sites: Public, Private, or What? Knowledge Tree **13** (2007)

5. boyd, d.: Reflections on Friendster, Trust and Intimacy.: Ubicomp 2003, Workshop application for the Intimate Ubiquitous Computing Workshop, Seattle, WA (2003)
6. Acquisti, A., Gross, R.: Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. Privacy Enhancing Technologies Workshop (PET) (2006)
7. Hogben, G.e.: Security Issues and Recommendations for Online Social Networks. ENISA, Heraklion, Greece (2007)
8. Liz, P.r.: Draft opinion of the Section for Transport, Energy, Infrastructure and the Information Society on The impact of social networking sites on citizens/consumers. Brussels (2009)
9. 29WP, A.: Opinion 5/2009 on online social networking. Article 29 Data Protection Working Party  Brussels (2009)
10. Pekárek, M., Pötzsch, S.: H1.2.5 – Requirements and concepts for privacy-enhancing access control in social networks and collaborative workspaces. PrimeLife Consortium (2009)
11. boyd, d.: Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life. In: Buckingham, D. (ed.): MacArthur Foundation Series on Digital Learning – Youth, Identity, and Digital Media Volume MIT Press, Cambridge, MA (2007)
12. Acquisti, A., Gross, R.: Information Revelation and Privacy in Online Social Networks (The Facebook case). ACM Workshop on Privacy in the Electronic Society (WPES) 2005. ACM, Alexandria, VA (2005)
13. Tufekci, Z.: Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites. Bulletin of Science, Technology & Society **28** (2008) 20-36
14. Donath, J., boyd, d.: Public displays of connection. BT Technology Journal **22** (2004) 71-82
15. Joinson, A.N.: 'Looking at', 'Looking up', or 'Keeping up with' People? Motives and Uses of Facebook. CHI 2008, Florence, Italy (2008)
16. Lampe, C., Ellison, N., Steinfield, C.A.: A Face(book) in the Crowd: Social Searching vs. Social Browsing. ACM Special Interest Group on Computer-Supported Cooperative Work. ACM Press (2006) 167-170
17. boyd, d.: Taken Out of Context  American Teen Sociality in Networked Publics (PhD thesis), Berkeley (2008)
18. boyd, d.: None of this is Real. In: Karaganis, J. (ed.): Structures of Participation (2007)
19. Goffman, E.: The presentation of self in everyday life. University of Edinburgh, Edinburgh (1956)
20. Sundén, J.: Material Virtualities. Peter Lang Publishing, New York (2003)
21. Turkle, S.: Life on Screen. Phoenix, London (1997)
22. Rachels, J.: Why privacy is important. Philosophy and Public Affairs (1975) 323-333
23. Barriger, J.: Social Network Sites: A comparative analysis of six sites. The Office of the Privacy Commissioner of Canada Ottawa (2009)
24. Thaler, R., Sunstein, C.: nudge – Improving decisions about health, wealth and happiness. Yale University Press, Boston (2008)

[i] The Onion is a satirical weekly published on the net. The Facebook episode can be found here: http://www.theonion.com/content/video/facebook_twitter_revolutionizing

[ii] See for instance, http://www.theregister.co.uk/2009/02/26/facebook_comment

[iii] See for instance http://news.bbc.co.uk/2/hi/uk_news/wales/8232250.stm

[iv] As reported in [11]. The study itself is: Lenhart, Amanda. 2007. "Social Networking Websites and Teens: An Overview." PEW Internet and the American Life Project, January 7.

[v] See Negroponte, Nicholas. 1996. Being Digital. New York: Vintage.

[vi] For instance, the Canadian Privacy Commissioner in a study on 6 popular SNS's in Canada observed that 'Facebook, LinkedIn and MySpace all require more than a click of a button to delete an account – Facebook and LinkedIn require the user to email the site requesting deletion (LinkedIn guarantees a response within 5 days) while MySpace allows the user to click to request cancellation, but then sends information on how to delete the account via the email address provided at registration." [23]

[vii] See for instance, http://www.nytimes.com/2009/01/29/fashion/29facebook.html

[viii] Popular culture types, such as Madonna and Prince are famous exceptions. They reinvent themselves every couple of years, with success.

[ix] For instance, Facebook holds US patent 7,117,254 'Method of inducing content uploads in a social network'.

[x] Posting dated 18 Feb 2008 12:41 AM by "Night of Fungi" on Facebook.

[xi] See for instance: http://www.nytimes.com/2009/01/29/fashion/29facebook.html

[xii] Post by "The Trickster" on someone's wall in Facebook dated Dec 13 2007 6:45 AM.

[xiii] This is how the wall is depicted on the satirical sketch by the Idiots of Ants for the BBC, where someone sprays graffiti on the outside wall of the victim in the sketches' house. See http://laughingsquid.com/facebook-in-real-life-by-idiots-of-ants/

[xiv] http://www.zephoria.org/thoughts/archives/2009/11/30/sociality_is_le.html

[xv] In fact there is. Even under the US notion of reasonable expectations of privacy as developed in Katz v. United States, 389 US 347, 348 (1967), constitutionally protected may be what a man seeks to preserve as private, even in an area accessible to the public.

[xvi] See http://elgg.org/. The Clique prototype can be found here: http://clique.primelife.eu/