Keeping up appearances

van den Berg, B.; Leenes, R.E.

Published in:
Computers, privacy and data protection

Publication date:
2011

Document Version
Peer reviewed version

Link to publication in Tilburg University Research Portal

Citation for published version (APA):
van den Berg, B., & Leenes, R. E. (2011). Keeping up appearances: Audience segregation in social network sites. In S. Gutwirth, Y. Poullet, P. de Hert, & R. Leenes (Eds.), *Computers, privacy and data protection: An element of choice* (pp. 211-232). Springer.

AQ1

Chapter 10
Keeping Up Appearances: Audience Segregation in Social Network Sites

Bibi van den Berg and Ronald Leenes

10.1 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 channels. These include, among others, personal and professional home pages, forums, online communities, blogs, dating sites, and social network sites such as Facebook, LinkedIn and MySpace. In this article we discuss some of the privacy-issues surrounding the presentation of personal content and personal information[1] in social network sites (SNSs). Particularly, we examine users' abilities to control who has access to the personal information and content they post in such communities. We conclude that social network sites lack a common mechanism used by individuals in their everyday interactions to manage the impressions they leave on others and protect their privacy: *audience segregation*. The lack of this mechanism significantly affects the level of users' control over their self-presentation in social network sites. In this article we argue that adding a virtual version of this real-world mechanism would contribute to enhancing privacy-friendliness in social network sites. We show that audience segregation is not only important in real life, but vital, yet currently undervalued and overlooked for the protection of one's self-images and privacy in social network sites.

B. van den Berg (✉)
Tilburg Institute for Law, Technology and Society (TILT), Tilburg University, Tilburg, The Netherlands
e-mail: bibi.vandenberg@uvt.nl

[1] By 'personal content' we mean any content (i.e. text, pictures, sounds, movies etc.) that can be attributed to and/or is experienced as 'personal' by the person posting it. By 'personal information' we mean any attribute (i.e. name, address, work or leisure affiliation, etc.) that can be attributed to and/or is experienced as 'personal' by the person posting it. This definition is broader than the definition of 'personal data' within Directive 95/46/EC and that of 'Personally Identifiable Information' as used in the US.

S. Gutwirth et al. (eds.), *Computers, Privacy and Data Protection: An Element of Choice*, DOI 10.1007/978-94-007-0641-5_10, © Springer Science+Business Media B.V. 2011

At the end of this article we present a privacy-preserving social network site called Clique [2] that we have built to demonstrate the mechanism. We discuss Clique and the three tools we have developed for it: contact-management, setting visibility rights, and managing multiple faces in a single social network environment.

10.2 Privacy Issues in Social Network Sites: Overview and Discussion

One of the fastest growing online fora for self-presentation and social interaction in recent years are "*social network sites"* (SNSs). In June 2008 these sites attracted "*an average of 165 million unique visitors a month*"[3]. Currently, Facebook claims to have over 400 million users.[4] In these online domains, users can present themselves using a so-called "profile", and they can engage in interactions with a network of "contacts"[5] also active in the same environment. One of the most oft-quoted definitions of social network sites was developed by boyd and Ellison, who write that these are

> web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system. The nature and nomenclature of these connections may vary from site to site.[6]

Despite the fact that social network sites are a recent phenomenon, there is quite a bit of variation in the intended goals of individual social network sites – ranging from dating and meeting friends, to connecting with work relations and finding new jobs, to providing recommendations for products, services and information[7]. Moreover, not all social network environments have the same *make-up*. Gross and Acquisti write:

[2] See http://clique.primelife.eu. Clique was built using Elgg [see http://elgg.com], an open source social networking engine.

[3] Kirsti Ala-Mutka, et al., The impact of social computing on the EU information society and economy. (Seville: IPTS/JRC, 2009), 16

[4] http://www.facebook.com/press/info.php?statistics, last accessed on 23 April 2010.

[5] 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. This issue will be discussed in more detail below. 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'* [. . .] *. . .'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.'*" James Grimmelmann, "Facebook and the social dynamics of privacy [draft version]," (2008), http://works.bepress.com/james_grimmelmann/20/, 5 and 28.

[6] danah boyd and Nicole B. Ellison, Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication* 13 (2007): 211.

[7] Ralph Gross and Alessandro Acquisti, Information revelation and privacy in online social networks, (paper presented at WPES'05, Alexandria, Virginia, USA, 2005), 71

> The most common model is based on the presentation of the participant's profile and the visualization of her network of relations to others – such is the case of Friendster. This model can stretch towards different directions. In matchmaking sites, like Match.com or Nerve and Salon Personals, the profile is critical and the network of relations is absent. In diary/online journal sites like LiveJournal, profiles become secondary, networks may or may not be visible, while participants' online journal entries take a central role. Online social networking thus can morph into online classified in one direction and blogging in another.[8]

Sharing personal content and personal information is one of the key elements of social network sites. Individuals join these networks to present information about themselves, for instance through text (blogs, descriptions of their current activities etc.), through pictures, movies and sound clips, and through listing their "favorites" – a broad category of pre-defined and user-generated labels to help categorize oneself, ranging from clothing and other commercial brands, to music and movies, to locations and activities. Thus, an image of each individual user emerges. Most, though not all, information is added to the profile by users themselves. Other users can also add information to one'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[9]. It is not surprising, therefore, that much of the research revolving around social network sites has focused on the *privacy* and *security issues* involved in individuals' self-presentations and the sharing of personal content and personal details. 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*"[10]. 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.[11]

[8] Ralph Gross and Alessandro Acquisti, Information revelation and privacy in online social networks, (paper presented at WPES'05, Alexandria, Virginia, USA, 2005), 72

[9] See for example: Zeynep Tufekci, Can you see me now? Audience and disclosure regulation in online social network sites, *Bulletin of Science, Technology and Society* 28 (2008), and Alyson L. Young and Anabel Quan-Haase, Information revelation and internet privacy concerns on social network sites: A case study of Facebook, (paper presented at C&T '09, University Park, Pennsylvania, USA, 25–27 June, 2009)

[10] Alessandro Acquisti and Ralph Gross, Imagined communities: Awareness, information sharing, and privacy on the Facebook, (paper presented at 6th Workshop on Privacy Enhancing Technologies, Cambridge, UK, 2006), 2

[11] James Grimmelmann, Facebook and the social dynamics of privacy [draft version], (2008), http://works.bepress.com/james_grimmelmann/20/, 9

So what makes people behave this way, given that there obviously are security and privacy issues? Why do they provide such detailed, and true[12], personal information on their social network site profile? Many explanations can be given, but we restrict ourselves to some of the most familiar. Acquisti and Gross say: "*Changing cultural trends, familiarity and confidence in digital technologies, lack of exposure or memory of egregious misuses of personal data by others may all play a role in this unprecedented phenomenon of information revelation*"[13]. 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 thing, users are often unaware of who has access to their personal profile and to the content they place online, because the architecture and design of social network sites is such that it provides individuals with a false sense of security and privacy. These sites "*systematically* [deliver] *them signals suggesting an intimate, confidential, and safe setting*"[14], an environment that is private, "*closed to unwanted outsiders.*"[15]. 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

[12] There are some interesting differences between the level of truthfulness in self-presentations across different social network sites. Research has shown, for instance, that while the overwhelming majority of members use their real name on their Facebook profile (a staggering 94,9% according to Tufekci (Zeynep Tufekci, Can you see me now? Audience and disclosure regulation in online social network sites, *Bulletin of Science, Technology and Society* 28 (2008)). An even higher number, 99,35%, was found in a 2009 study by Young and Quan-Haase (Alyson L. Young and Anabel Quan-Haase, Information revelation and internet privacy concerns on social network sites: A case study of Facebook, (paper presented at C&T '09, University Park, Pennsylvania, USA, 25-27 June, 2009)). In the above-cited article Tufekci shows that, by contrast, in MySpace a substantial amount of users (38,2%) provide a nickname on their profiles. There are many explanations for such differences. One of the most straightforward ones is the fact that Facebook actively, and quite strictly, discourages the use of fake names, as was made clear by a tell-tale example presented by Grimmelmann: "*Facebook applies* [its] *policy* [regarding the ban on the use of fake names] *rigorously almost to the point of absurdity. It refused to let the writer R.U. Sirius sign up under that name, even though he'd written six books and hundreds of articles under it and he uses it in everyday life*." (James Grimmelmann, "Facebook and the social dynamics of privacy [draft version]," (2008), http://works.bepress.com/james_grimmelmann/20/, 6). 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*." (danah boyd, 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*, edited by David Buckingham. (Cambridge, MA: MIT Press, 2008b), 131-132)

[13] Alessandro Acquisti and Ralph Gross, Imagined communities: Awareness, information sharing, and privacy on the Facebook, (paper presented at 6th Workshop on Privacy Enhancing Technologies, Cambridge, UK, 2006), 2

[14] James Grimmelmann, "Facebook and the social dynamics of privacy [draft version]," (2008), http://works.bepress.com/james_grimmelmann/20/, 17

[15] James Grimmelmann, "Facebook and the social dynamics of privacy [draft version]," (2008), http://works.bepress.com/james_grimmelmann/20/, 18

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 something will befall them as individuals (Grimmelmann, 2008: 17–18).

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.[16]

Taking things to a more general level one can argue that there are four fundamental issues surrounding privacy and (unintended) information disclosure in relation to online worlds[17]. These can be summarised as follows:

It is difficult or even impossible for users to know what the composition or the reach 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 degree of *persistence* that most information in the real world lacks. This means that information may (intentionally) reach audiences in the (far) future;

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 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 the individual.

These four issues are highly relevant to social network sites as well. 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 in-transparent. Now, while some social network sites allow users some level 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

[16] danah boyd, 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*, edited by David Buckingham. (Cambridge, MA: MIT Press, 2008b), 133

[17] See for example: Leysia Palen and Paul Dourish, "Unpacking 'privacy' for a networked world," (paper presented at Computer-Human Interaction (CHI) Conference 2003, Ft. Lauderdale, Florida, USA, 5-10 April, 2003), and Daniel J. Solove. *The future of reputation: Gossip, rumor, and privacy on the Internet*. (New Haven, CT: Yale University Press, 2007)

are usually set to "public", which means that individuals' profiles and the information contained therein can be viewed by anyone accessing the social network site. This means, Acquisti and Gross conclude, "*that the network is effectively an open community, and its data effectively public*."[18]

Second, since information can be copied, saved and stored easily and infinitely, information placed online at any particular moment may come back to haunt the individual years down the line. 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*."[19]

Third, as we will discuss more extensively below, 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 pages, 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:

> 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.[20]

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, for instance, of a profile with personal details, stories and pictures. Now, 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.

[18] Alessandro Acquisti and Ralph Gross, Imagined communities: Awareness, information sharing, and privacy on the Facebook, (paper presented at 6th Workshop on Privacy Enhancing Technologies, Cambridge, UK, 2006), 3

[19] Zeynep Tufekci, Can you see me now? Audience and disclosure regulation in online social network sites, *Bulletin of Science, Technology and Society* 28 (2008), 22, emphasis in the original

[20] Zeynep Tufekci, Can you see me now? Audience and disclosure regulation in online social network sites, *Bulletin of Science, Technology and Society* 28 (2008), 22

The central question we posed ourselves in our own research on privacy issues in social network sites was how we could contribute to solving some of the issues outlined in this section. We will turn to a description of some of our ideas now.

10.3 Privacy-Preserving Social Networking: Audience Segregation

In our view, there are two central issues to be addressed in providing users with more privacy-respecting or -preserving social network environments:

User *awareness* of the privacy issues discussed in the previous section should be raised, i.e., users ought to become more aware of the fact that, and the ways in which, personal information and personal content may "leak" to unintended audiences and places on the internet;

Users should be provided with *tools* to help them manage their personal information and content in a more privacy-friendly manner.

To maximise awareness and usability, these tools ought to be easily recognisable for users. This is why we have taken a social mechanism that individuals use in everyday life contexts to control the image others have of them and the information they disclose about themselves: *audience segregation*. Mirroring or mimicking this real-life strategy in a virtual environment, we have developed a social network site, Clique, that implements it.

10.3.1 Audience Segregation

The concept of "*audience segregation"* was coined by Erving Goffman[21] as part of a perspective on the ways in which identities are constructed and expressed in interactions between human beings in everyday contexts. 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 which they engage in the interaction ("public validation"[22]). To Goffman, then, *impression management* is key in such self-presentations.

Individuals performs a wide variety of roles in their everyday lives, relating to both the places they visit, and the other people present there[23]. For instance, when

[21] Erving Goffman. *The presentation of self in everyday life*. (Garden City, NY: Doubleday, 1959)

[22] Ann Branaman, Goffman's social theory, In *The Goffman reader*, edited by Charles C. Lemert and Ann Branaman. (Cambridge, MA: Blackwell Publishers, 1997), xlvi

[23] See for example: Joshua Meyrowitz. No sense of place: The impact of electronic media on social behavior. (New York, NY: Oxford University Press, 1985), and Bibi Van den Berg. The situated self: Identity in a world of Ambient Intelligence. (Nijmegen: Wolf Legal Publishers, 2010)

at work, individuals will display different images of themselves than when they are at home, or when they buy groceries at a local store, or when they visit a movie theatre. 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. The presentation of selves, then, is *situated* or *contextual* – it relates to *where* one is, and *who else is there* [24].

One of the key elements of Goffman's perspective on identity its the fact that individuals attempt to present self-images that are both *consistent* and *coherent*. To accomplish this, performers engage in what Goffman calls "audience segregation", "*. . .so that the individuals who witness him in one of his roles will not be the individuals who witness him in another of his roles*"[25]. With segregated audiences for the presentation of specific roles, people 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[26]. For example, 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 by their knowing about this aspect of his personal life.

While Goffman's idea of audience segregation didn't originally relate directly to privacy, it is easy to see that audience segregation and privacy are, in fact, closely linked. Helen Nissenbaum has famously 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[27]. 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,

[24] Bibi Van den Berg, "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, ed. Simone Fischer-Hübner, Penny Duquenoy, Albin Zuccato and Leonardo Martucci. (New York, NY: Springer, 2008), and Bibi Van den Berg. The situated self: Identity in a world of Ambient Intelligence. (Nijmegen: Wolf Legal Publishers, 2010)

[25] Erving Goffman. *The presentation of self in everyday life*. (Garden City, NY: Doubleday, 1959), 137

[26] Erving Goffman. *The presentation of self in everyday life*. (Garden City, NY: Doubleday, 1959), 137

[27] Helen Nissenbaum, Privacy as contextual integrity, *Washington Law Review* 79 (2004), also see Kieron O'Hara and Nigel Shadbolt. *The spy in the coffee machine*. (Oxford: Oneworld Publications, 2008), 77 ff.

> 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.[28]

Following Michael Walzer[29], 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.

10.3.2 Audience Segregation in Social Network Sites: Why?

Above we have argued that in current social network sites users lack mechanisms to *separate and manage the various audiences for whom they perform*. Many social network sites only provide their users the option to collect one list of contacts, called "friends". Given the fact that Facebook users, for instance, on average have 130 "friends"[30], this necessarily conflates different contexts. Providing users with mechanisms to control access over the information they present in such online communities would improve the quality of interactions and self-presentations for three reasons. First of all, it would mimic real life interaction patterns to a larger degree, and align more closely with the ways in which individuals tend to engage with others in everyday settings. As we have seen, audience segregation is a common feature of self-presentations in everyday life, and even a necessary *requirement* for optimal impression management and role performance. Second, enabling access control and audience segregation in social network sites could be a first step in countering some of the privacy and security risks we have discussed above and, therefore, make social network sites more privacy-friendly. Considering the numbers of people active on social network sites today it seems that this is a worthwhile goal to strive for indeed. Third, enabling users to compartmentalise the audiences for whom they perform in social network sites provides them with an opportunity to present different sides of themselves to different audiences, thereby allowing each (partial!) self-presentation to be textured and full of depth. Audience segregation enables users to avoid what danah boyd calls "*social convergence*"[31]. If individuals do not have enough facilities to properly manage impressions in front of various separate audiences, they need to present one single "face" that works for all of these audiences. While these conflated self-presentations might be acceptable for a wide range of audiences and a wide assortment of social contexts, they will at the same time lack the depth,

[28] Helen Nissenbaum, Privacy as contextual integrity, *Washington Law Review* 79 (2004): 137.

[29] Michael Walzer. *Spheres of justice: A defense of pluralism and equality*. (New York, NY: Basic Books, 1983)

[30] See http://www.facebook.com/press/info.php?statistics, last visited April 23, 2010.

[31] danah boyd, "Facebook's privacy trainwreck," Convergence: The International Journal of Research into New Media Technologies 14 (2008a)

breadth, variety and uniqueness of socially constricted, contextual ones. Moreover, with multiple audiences to keep into account, it becomes very difficult to decide what "face" to show. The result, says boyd, is 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.[32]

Therefore, audience segregation offers users the opportunity to be "round characters" in each role, rather than merely "flat ones", to borrow some terminology from literature studies.

Now, not all social network sites have the same intended *goals*. Some cater specific needs, such as providing opportunities for finding a date or meeting new friends, while others cater to specific groups, such as professionals, or provide opportunities for finding specific products, services and information. When social network sites cater individuals' specific needs or revolve around particular groups, it is easy to see that audience segregation is both relevant and desirable. A person presenting himself in a profile on a dating network may feel uncomfortable if the information displayed there "spills over" into other domains and networks, for instance into their work-related network. Alternatively, a person presenting himself in a network providing professional connections will want to avoid information regarding his (all too) personal sphere or background from seeping in.

However, audience segregation does not merely apply to the spill-over of information from one online environment into another, but is also an issue *within* one and the same environment. We envision that users would find it convenient and worthwhile to be able to control their various kinds of online profiles using a single dashboard. This would entail that, for instance, a person's work profile, his personal profile and the profile for his avatar in an online role-playing game such as Second Life would be combined within a single social network site. Moreover, a person's profile information from collaborative workspaces such as wikis and forums could be stored in the same place as well. Facebook and Friendster already cater to the more "general" goal of connecting individuals without a particular shared interest or aspect of self, and hence it seems likely that social network sites such as these will most easily grow into the "central identity management platforms" that we envisage.

In these multipurpose social network sites individuals connect with both friends, family members, distant relatives, colleagues, acquaintances, old schoolmates, members of their local community, etc. – some of whom are intimately known to them, while others are distant, loose, or even unknown connections. It is easy to see why individuals using such sites might want to make distinctions between the *types*

[32] danah boyd, "Facebook's privacy trainwreck," Convergence: The International Journal of Research into New Media Technologies 14 (2008a), 18

of information they want to make available to each of these different categories of connections, and give different connections access to different *content*. For instance, an individual might want to share his holiday pictures with close friends, family members and other relatives, but not with his colleagues or old schoolmates. Or, more specifically, he might want to share his holiday pictures with his close friends and family members – but *not* with Mom and Aunt So-and-so. Alternatively, an individual might want to share work-related documents or postings with his colleagues, but not with his friends, *except* for Friend So-and-so, and so on and so forth.

Currently, most social network sites provide limited options for making one's profile or its content (in)visible for specific others or specific collections of others. Generally, users can choose from: "visible to everyone" (i.e. all members of the social network site), "visible only to friends" (i.e. all of a user's contacts!), "visible only to friends and friends of friends", and in some cases "invisible to everyone"[33]. In some social network sites, the user can specify the (in)visibility settings of specific *types* of information, e.g. they can make their basic information (name, home town etc.) available to all members of the platform, while keeping their pictures only for their contacts. Assigning different "collections" within one's own network of contacts has recently been added as an option to Facebook, but at the moment none of the other major social network sites (e.g. Friendster, LinkedIn, MySpace) have it, let alone assigning different access rights to different individuals and for different kinds of content within one's own network of contacts.

10.4 A Note on Terminology

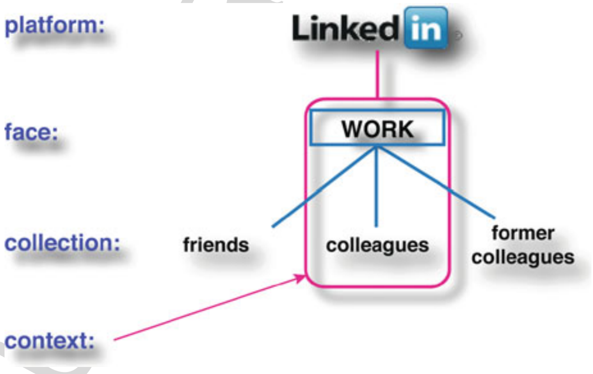
Before turning to a presentation of the way in which we've translated the conceptual ideas of audience segregation into a working demonstrator, we address an issue concerning terminology. The language used to discuss online communities, the users participating in them, and the connections between these users is often quite fuzzy and imprecise. This is why we pause to define each of these concepts.

1. The terms "*platform*" and "social network site" (which we've defined in the introduction to this article) will be used interchangeably;
2. On the platform a person can create a "*face*", a profile page on which he displays particular information about himself. The totality of all the faces a person manages within a platform makes up his identity. While users currently tend to have only one face in social network sites catering specific needs (e.g. dating or professional self-presentation), those catering to several needs, or those catering no specific need at all, might invoke users to create *multiple* faces within the same domain. In such social network sites, then, the personal information making up various identities may be brought together for each individual user;

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

3. "*Contacts*" are all the individuals with whom a users is connected within the platform;
4. "*Collections*" are sets of contacts selected and assigned by the individual from the totality of his network. Collections can consist of anywhere between zero and an unlimited amount of contacts. The individual can assign a name to each collection to identify them as a collection (e.g., "colleagues" or "old schoolmates" or "boring people"). Collections have labels that have meaning for their creator. The labels are not visible to the members of a particular collection. They need not know that they are grouped into a cluster "distant friends". The distant friends may know or realise that they don't belong to someone's inner circle, but usually this is not made explicit in real life interactions.
   Each time content is added to the profile, it can be made available for specific collections, or even for specific members of each collection, based on the user's own preferences (more on this below). The management of collections and the content available to them should be dynamic, transparent and open to change at all times.
5. A "*context*" is each instance in which a *particular face* and a *particular collection* come together. For instance, a "work context" is one in which a user presents his "work identity" (face) to his "collea-gues" (collection). Similarly, a "reminiscence context" arises when a user presents information (pictures, documents, text in chat relays) (face) regarding his younger years to his "old school friends" (collection). A third example is that of a person making his holiday pictures available, i.e. information that is often regarded as quite personal (face) to all of his family members (collection) and some individuals from his friends (collection).

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



AQ2 **Fig. 10.1** Terminology

10.5 Transforming the Conceptual Framework into Practical Tools

In the remainder of this article we will present our proposals for realising audience segregation within a social network site. We have implemented this mechanism into three tools: a tool for contact-management, one for setting access control policies, and one for managing multiple faces.

10.5.1 Contact-Management: Collections

Our starting point for realising audience segregation in social network sites is the introduction of *nuance* in connections[34]. By this we mean: enabling users to create their own labels for "collections" in which they may cluster one or more of their contacts. As we have seen above, in most current-day social network sites all contacts in a user's network are lumped together in one category. No distinction is made between the different social networks a person may participate in, as all of us do in our everyday lives. This means that a) it is impossible for users to hide parts of their network of contacts from other contacts (e.g., a person does not want his colleagues to see his friends, or he does not want his mother to see his colleagues); and b) that it is impossible to show particular information to one portion of one's network, while hiding it from others. All information displayed on one's profile is there for all to see, at least for one's entire network of contacts.

By allowing users to create collections within their list of contacts, they can cluster social relations according to their own preferences, and thereby mimic the actual practice of building and maintaining separate social spheres in real life in the process. It is important that users are free in labelling their own set of collections, since they themselves know best what the fabric of their own social lives consists of and how it could be divided into relevant and meaningful categories.

James Grimmelmann has argued that offering what he calls "technical controls" to manage the (in)visibility of a person's profile in social network sites is not a workable solution. He claims that if the provider of the social network site offers the possibility to place contacts in clusters (such as "family" or friends') then these clusters are never going to be an adequate representation of the complexity of social relationships in real life. He writes:

> Consider the RELATIONSHIP project, which aims to provide a "vocabulary for describing relationships between people" using thirty-three terms such as "apprenticeTo," "antagonistOf," "knowsByReputation," "lostContactWith," and "wouldLikeToKnow."[. . .] Clay Shirky shows what's wrong with the entire enterprise by pointing out that RELATIONSHIP's authors left out "closePersonalFriendOf," "usedToSleepWith," "friendYouDontLike," and every other phrase we could use to describe our real, lived

[34] J. Donath and danah boyd, Public displays of connection, *BT Technology Journal* 22 (2004): 72.

> relationships.[. . .] We shouldn't expect Facebook's formal descriptors to be precise approximations to the social phenomena they represent.[35]

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

In Clique, the creation and management of collections was one of the first functionalities introduced. Users in Clique can cluster contacts into self-assigned and self-labelled sets. After inviting contacts, they can assign them to one or more collections, and change or delete these ascriptions at any time. Figure 10.2 shows what collection management in Clique looks like. Notice that the collection "colleagues" is marked as Ronald's primary audience (marked as default).

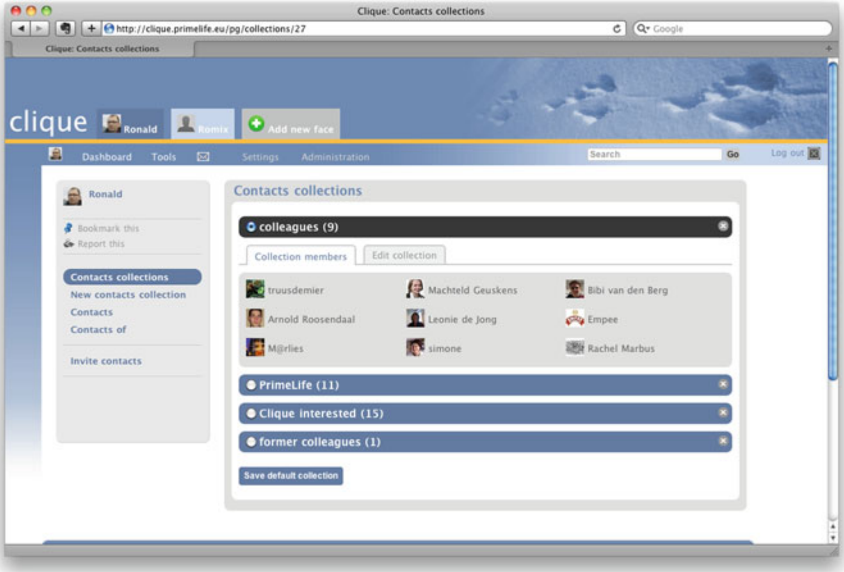


Fig. 10.2 Managing collections in clique

[35] James Grimmelmann, "Facebook and the social dynamics of privacy [draft version]," (2008), http://works.bepress.com/james_grimmelmann/20/, 27

10.5.2 Setting Visibility Rights

The second principle in realising audience segregation in social network sites is *contextualising* the user's profile and all the information gathered there[36]. This means that a person's specific "face" is combined with information made public for a specific collection. Such contextualisation mimics the maintenance of different social spheres as we have them in real life. In most social network sites the user builds one single profile, in which all of his information is stored. All of his contacts see the same information. However, as we have argued in this article it is important to allow users to diversify the information and content they present to various audiences. Moreover, many people now maintain different profiles in different social network sites, which is cumbersome and time-intensive. As we have argued above it seems reasonable to suspect that users would prefer gathering all of the various profile pages in one single social network site. Obviously this development makes it all the more important that users can contextualise the content and information they share in each face.

We have developed two tools for contextualising content and information in Clique. The first is the use of *visibility rights,* which enables users to assign access rights to different collections and individuals. Each time users post items of information (personal information in a profile, pictures, text, documents, etc.) within a context, they can choose for which contacts (both collections and individuals) this item will be visible. For example, a user may decide to make his holiday pictures invisible to his colleagues but visible to his relatives and some members of his collection of friends, or he may decide to prevent acquaintances from reading his diary entries, but leave them visible to everyone else in his contacts list.

In Clique we provide individual users as much control over the visibility settings of each individual item of information as possible for two reasons. First, individuals use social network sites to present personal information and personal content with different goals and purposes in mind. Some may use them, for instance, only to stay in touch with people they know intimately in the real world, whereas others may want to use them especially to present (aspects of) themselves before an audience of strangers. Obviously, the needs of these people, in terms of the visibility of their information, varies. Therefore, it would be patronising and limiting if the social network provider or the software designer would decide for users which information to share and for which (limited or unlimited) audience.

Second, users' ideas of which kinds of information are deemed "private" vary. As O'Hara and Shadbolt write:

> Different people have different views of what should be private. [. . .] People must be able to reach their own decisions about what should be private, and what gains they would hope to make by releasing information about themselves.[37]

[36] J. Donath and danah boyd, Public displays of connection, *BT Technology Journal* 22 (2004): 72.

[37] Kieron O'Hara and Nigel Shadbolt. *The spy in the coffee machine*. (Oxford: Oneworld Publications, 2008), 74

Now, one of the most obvious objections to this choice would be the idea that users do not *want* to have this much control over their personal information and personal content in social network sites. In fact, in the past researchers regularly argued that users wouldn't be interested in having possibilities for more fine-grained control over the display of personal data, for instance because making the profile invisible makes it harder for other people to find them[38], or because they would simply find it too much hassle. However, recent research has shown that, when given the opportunity, many people do in fact want to shield some of their information[39], especially since a number of negative examples regarding information spill and privacy issues with respect to social network sites have been published in the press in many Western countries.[40]

We have built a fine-grained architecture for setting access control policies, in which each consecutive element of the profile can be made visible for either collections, or individuals, or a mixture of both. This means, for instance, that a user can make his name and date of birth visible to everyone while keeping his address invisible for anyone, and allowing only some of his contacts, of his own choosing, to see his mobile phone number. The picture below shows the user profile page in Clique. With each entry there is an icon, which displays who can access that particular datum.

Users can choose between the following access control options for the content published on their profile: "only visible to me", "contacts/collections", "all contacts", and "public".

When users publish information they are presented with an access control dialogue as shown in Fig. 10.4 below. In this dialogue window we "nudge"[41]/[42] the user to act in a privacy savvy manner without undermining sociality. By default, the user's primary audience (default collection, see Fig. 10.2) is selected as having access to the content to be published. The user can drag collections and individual contacts to the red and green boxes to grow or shrink the audience. Note that in this case, Ronald's colleagues have access to the content to be published, with the

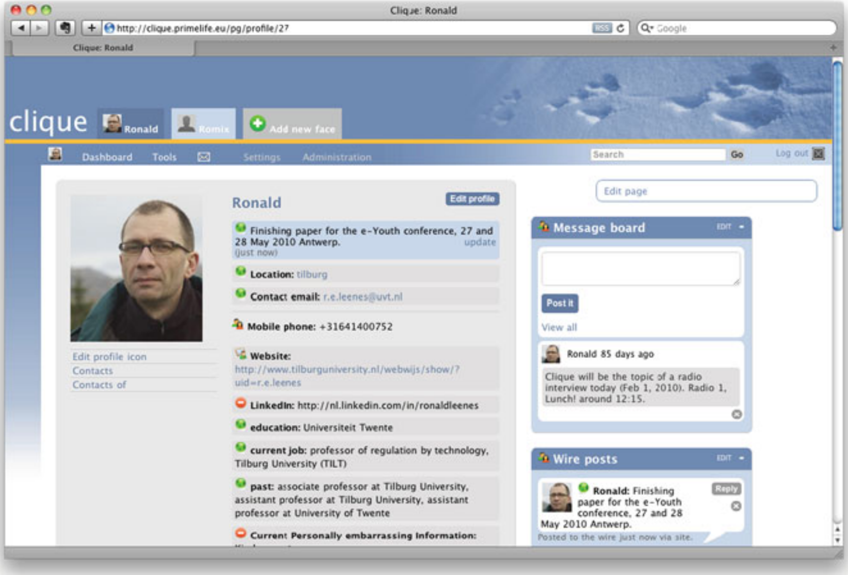
[38] See for example: danah boyd, Why youth (heart) social network sites: The role of networked publics in teenage social life, In *MacArthur Foundation Series on Digital Learning – Youth, Identity, and Digital Media Volume*, edited by David Buckingham. (Cambridge, MA: MIT Press, 2008b)

[39] See for example: Zeynep Tufekci, Can you see me now? Audience and disclosure regulation in online social network sites, *Bulletin of Science, Technology and Society* 28 (2008)

[40] On 21 November 2009, for instance, the Canadian Broadcasting Corporation presented a story of a Canadian woman who was on long-term sick leave due to depression. This woman's health benefits were allegedly terminated after the health insurance company discovered pictures of the woman tanning on a beach and having a good time at a party with strippers on her Facebook page. See http://www.cbc.ca/canada/montreal/story/2009/11/19/quebec-facebook-sick-leave-benefits.html [last accessed 25 November 2009].

[41] The Nudge 'methodology' consists of: provide iNcentives, Understand mappings, Defaults, Give feedback, Expect error, Structure complex choices

[42] Richard H. Thaler and Cass R. Sunstein. *Nudge: Improving decisions about health, wealth, and happiness*. (New Haven, CT: Yale University Press, 2008)



Ronald

Finishing paper for the e-Youth conference, 27 and 28 May 2010 Antwerp. update
(just now)

Location: tilburg

Contact email: r.e.leenes@uvt.nl

Mobile phone: +31641400752

Website: http://www.tilburguniversity.nl/webwijs/show/?uid=r.e.leenes

LinkedIn: http://nl.linkedin.com/in/ronaldleenes

education: Universiteit Twente

current job: professor of regulation by technology, Tilburg University (TILT)

past: associate professor at Tilburg University, assistant professor at Tilburg University, assistant professor at University of Twente

Current Personally embarrassing Information:

Ronald 85 days ago

Clique will be the topic of a radio interview today (Feb 1, 2010). Radio 1, Lunch! around 12:15.

Ronald: Finishing paper for the e-Youth conference, 27 and 28 May 2010 Antwerp.

Posted to the wire just now via site.

AQ3

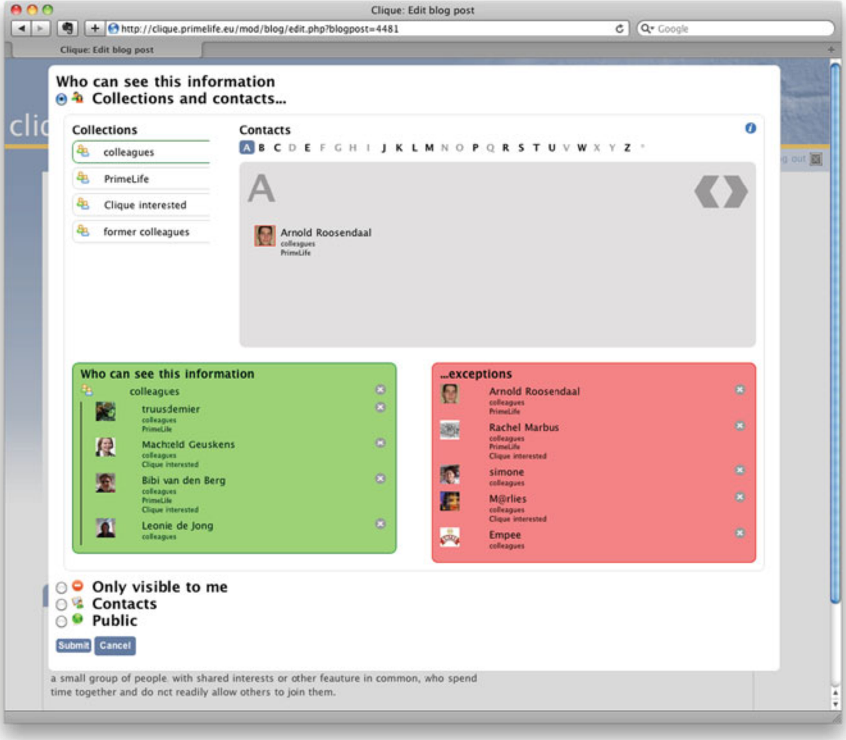
Fig. 10.3 Visibility cues in clique

exception of Arnold Roosendaal, and four other individuals. While enabling access to a collection, thus, the user can still choose to make information unavailable for particular individuals.

The icon associated to the published content reveals the audience when hovering over (see Fig. 10.5).

10.5.3 Managing Multiple Faces in One Social Network Site: Tabs

The second tool we have developed to contextualise information is the introduction of *tabs* to represent the different faces a user may want to combine within the same social network environment. Each tab functions as a separate social sphere, representing one aspect of the user's identity. For instance, users may create a tab for their private face and for their professional face. Each of these faces contains a network of contacts, who can be assigned to the various collections within each tab. Access rights can be defined for collections and contacts with regard to all personal information and content presented in a context (i.e. using a specific face in front of a specific collection). Contacts only get access to the information that is made visible for them. This means that a) contacts who only know the individual professionally, for instance, are prevented from acquainting themselves with his digital representation from a leisurely profile; and b) within each face, contacts can only access the information that is made available for them through the use of visibility rights.



Who can see this information
● Collections and contacts...

Collections
- colleagues
- PrimeLife
- Clique interested
- former colleagues

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

Arnold Roosendaal
colleagues
PrimeLife

Who can see this information
colleagues
truusdemier
colleagues
PrimeLife
Machteld Geuskens
colleagues
Clique interested
Bibi van den Berg
colleagues
PrimeLife
Clique interested
Leonie de Jong
colleagues

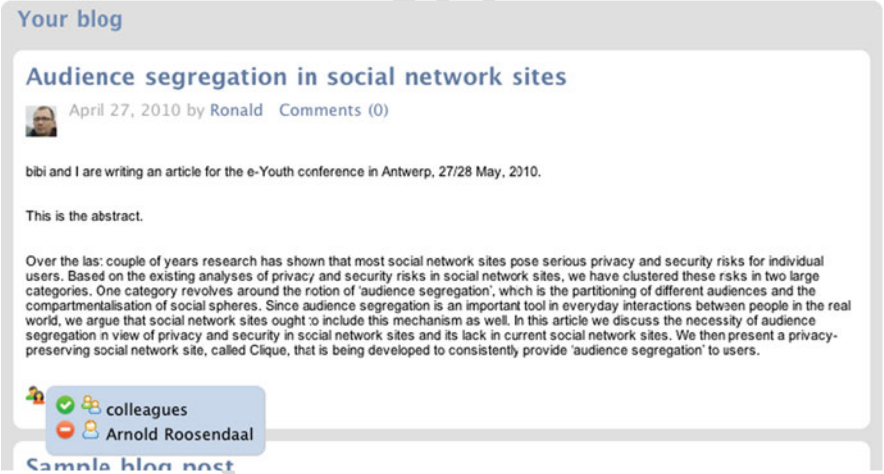
...exceptions
Arnold Roosendaal
colleagues
PrimeLife
Rachel Marbus
colleagues
PrimeLife
Clique interested
simone
colleagues
M@rlies
colleagues
Clique interested
Empee
colleagues

○ Only visible to me
○ Contacts
○ Public

Submit Cancel

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.

Fig. 10.4 Extended access control dialogue in clique



Your blog

Audience segregation in social network sites

April 27, 2010 by Ronald Comments (0)

bibi and I are writing an article for the e-Youth conference in Antwerp, 27/28 May, 2010.

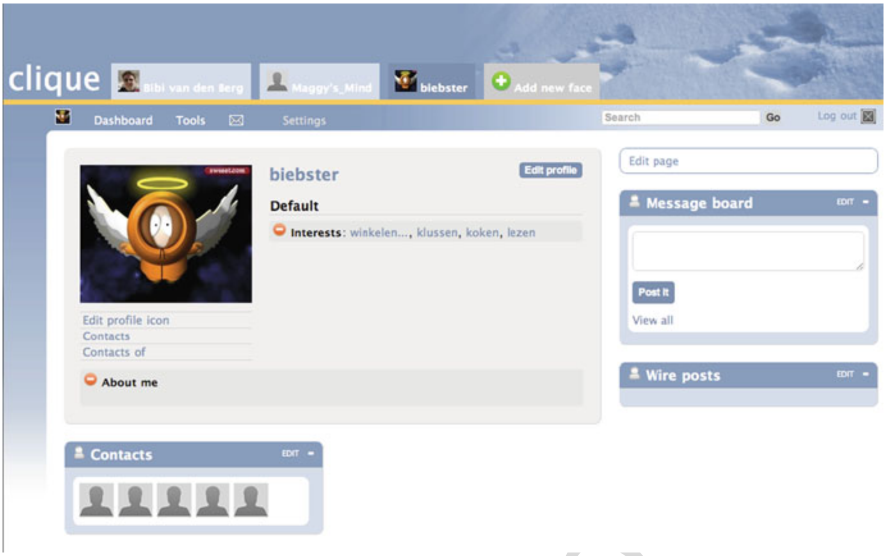
This is the abstract.

Over the last couple of years research has shown that most social network sites pose serious privacy and security risks for individual users. Based on the existing analyses of privacy and security risks in social network sites, we have clustered these risks in two large categories. One category revolves around the notion of 'audience segregation', which is the partitioning of different audiences and the compartmentalisation of social spheres. Since audience segregation is an important tool in everyday interactions between people in the real world, we argue that social network sites ought to include this mechanism as well. In this article we discuss the necessity of audience segregation in view of privacy and security in social network sites and its lack in current social network sites. We then present a privacy-preserving social network site, called Clique, that is being developed to consistently provide 'audience segregation' to users.

colleagues
Arnold Roosendaal

Sample blog post

Fig. 10.5 Audience indicator in clique



Interests: winkelen..., klussen, koken, lezen

Fig. 10.6 Managing multiple faces in clique

Using tabs to distinguish between different contexts is a visually appealing and easy way for the individual to manage his or her own profile and the various faces contained therein. Information added to one of the faces (e.g. the "Biebster" tab in Fig. 10.6 below) is invisible in all other tabs, and hence it is easy for the user to manage who sees what. Clique can therefore be seen as a dashboard for multiple social contexts. By simply clicking through the different tabs a user can see what information is accessible there, and by hovering over the icons attached to each item of information, he or she can easily keep track of what information is made available to whom. Figure 10.6 displays multiple tabs, each representing a different face, for a single user.

Creating new faces is a bit cumbersome, since it means that users need to build a new profile, set the security and privacy settings, and add contacts and content for each individual face. This means users need to invest energy and time in setting up a new profile. Particularly when users create multiple faces for which the contact list shows a significant overlap we may wonder whether users are willing to make this investment, and whether they may see (enough of) the benefits and advantages of creating separate faces. However, this objection can be remedied by allowing users to import existing profile pages and contact lists, for instance from LinkedIn or Facebook, into separate tabs in Clique. Moreover, once the face has been created it is instantly clear what the advantages of this system are, and that they outweigh the initial energy to be invested. The visual separation of different social spheres and the division of content between these spheres, entails that users can effortlessly see which contact sees which information, both in terms of the profile and the content he or she has posted on his page. Managing audience segregation has thus been reduced to an intuitive, easy-to-manage and basic element of the social network site. This means that the user can engage in interactions with his contacts in a safer and more "natural" way, without having to manage his information with a high level of vigilance and privacy-awareness.

10.6 Conclusion

Context is a central concept in the disclosure of information. What is appropriate in one context may not be in another. We have argued that audience segregation is one of the core mechanisms that people employ in their everyday life to accomplish contextual integrity and that most current online social network sites have a very simplistic model of social structures. 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 taken the first steps in developing a prototype that implements audience segregation.

Whether or not social network site 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). The reader is invited to participate in this experiment.

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 authors want to thank Joeri de Ruiter who did a tremendous job of implementing the ideas of the authors into the Clique application.

References

Acquisti, A., and R. Gross, Imagined communities: Awareness, information sharing, and privacy on the Facebook, (paper presented at 6th Workshop on Privacy Enhancing Technologies, Cambridge, UK, 2006): 36–58.

Ala-Mutka, K., D. Broster, R. Cachia, C. Centeno, C. Feijóo, A. Haché, S. Kluzer, S. Lindmark, W. Lusoli, G. Misuraca, Y. Punie, and J.A. Valverde, *The impact of social computing on the EU information society and economy*. Seville: IPTS/JRC, 2009.

boyd, d., Facebook's privacy trainwreck, *Convergence: The International Journal of Research into New Media Technologies* 14 (2008a): 13–20.

boyd, d., 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*, edited by D. Buckingham, 119–142. Cambridge, MA: MIT Press, 2008b.

boyd, d., and N.B. Ellison, Social network sites: Definition, history, and scholarship, *Journal of Computer-Mediated Communication* 13 (2007): 210–230.

Branaman, A., Goffman's social theory, In *The Goffman reader*, edited by C.C. Lemert and A. Branaman, xlv-lxxxii. Cambridge, MA: Blackwell Publishers, 1997.

Donath, J., and d. boyd, Public displays of connection. *BT Technology Journal* 22 (2004): 71–83.

Goffman, E., *The presentation of self in everyday life*. Garden City, NY: Doubleday, 1959.

Grimmelmann, J., Facebook and the social dynamics of privacy [draft version], (2008), http://works.bepress.com/james_grimmelmann/20/ (last accessed on July 6, 2009).

Gross, R., and A. Acquisti, Information revelation and privacy in online social networks (paper presented at WPES'05, Alexandria, Virginia, USA, 2005): 71–81.

Meyrowitz, J. *No sense of place: The impact of electronic media on social behavior*. New York, NY: Oxford University Press, 1985.

Nissenbaum, H. Privacy as contextual integrity. *Washington Law Review* 79 (2004): 119–159.

O'Hara, K., and N. Shadbolt. *The spy in the coffee machine*. Oxford: Oneworld Publications, 2008.

Palen, L., and P. Dourish. Unpacking ′privacy′ for a networked world (paper presented at Computer-Human Interaction (CHI) Conference 2003, Ft. Lauderdale, Florida, USA, 5–10 April, 2003): 129–137.

Solove, D.J. *The future of reputation: Gossip, rumor, and privacy on the Internet*. New Haven, CT: Yale University Press, 2007.

Thaler, R.H., and C.R. Sunstein. *Nudge: Improving decisions about health, wealth, and happiness*. New Haven, CT: Yale University Press, 2008.

Tufekci, Z. Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology and Society* 28 (2008): 20–36.

Van den Berg, B. Self, script, and situation: Identity in a world of ICTs. In *The future of identity in the information society: Proceedings of the third IFIP WG 9.2, 9.6/11.6, 11.7/FIDIS International Summer School on the Future of Identity in the Information Society*, edited by S. Fischer-Hübner, P. Duquenoy, A. Zuccato and L. Martucci, 63–77. New York, NY: Springer, 2008.

Van den Berg, B. *The situated self: Identity in a world of Ambient Intelligence*. Nijmegen: Wolf Legal Publishers, 2010.

Walzer, M. *Spheres of justice: A defense of pluralism and equality*. New York, NY: Basic Books, 1983.

Young, A.L., and A. Quan-Haase, Information revelation and internet privacy concerns on social network sites: A case study of Facebook (paper presented at C&T ′09, University Park, Pennsylvania, USA, 25–27 June, 2009): 265–274.

Chapter 10

Q. No.	Query
AQ1	All references are repeated in the footnotes. We retain as such. Please confirm.
AQ2	Please provide text citation for “Fig. 1”
AQ3	Please provide text citation for “Fig. 3”