

Tilburg University

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. Poulet, P. de Hert, & R. Leenes (Eds.), *Computers, privacy and data protection: An element of choice* (pp. 211-232). Springer.

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

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 information¹ 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

¹By '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.

At the end of this article we present a privacy-preserving social network site called Clique² 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 information⁷. Moreover, not all social network environments have the same *make-up*. Gross and Acquisti write:

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

³Kirsti 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.

⁵Confusingly, 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.

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

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

10 Keeping Up Appearances

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

98 Sharing personal content and personal information is one of the key elements of
 99 social network sites. Individuals join these networks to present information about
 100 themselves, for instance through text (blogs, descriptions of their current activities
 101 etc.), through pictures, movies and sound clips, and through listing their “favorites”
 102 – a broad category of pre-defined and user-generated labels to help categorize one-
 103 self, ranging from clothing and other commercial brands, to music and movies,
 104 to locations and activities. Thus, an image of each individual user emerges. Most,
 105 though not all, information is added to the profile by users themselves. Other users
 106 can also add information to one's profile, thereby further refining the image created.

107 One of the most fascinating aspects of this emerging field of self-presentation
 108 is the fact that users put so much and such personal information about themselves
 109 in their profiles⁹. It is not surprising, therefore, that much of the research revolving
 110 around social network sites has focused on the *privacy* and *security issues* involved
 111 in individuals' self-presentations and the sharing of personal content and personal
 112 details. Acquisti and Gross write: “. . .one cannot help but marvel at the nature,
 113 amount, and detail of the personal information some users provide, and ponder
 114 how informed this information sharing is”¹⁰. In an article on the privacy risks for
 115 individuals using Facebook Grimmelmann dryly points out:
 116

117 Facebook knows an immense amount about its users. A fully filled-out Facebook profile
 118 contains about 40 pieces of recognizably personal information, including name; birthday;
 119 political and religious views; online and offline contact information; sex, sexual preference
 120 and relationship status; favorite books, movies, and so on; educational and employment
 121 history; and, of course, picture. [. . .] Facebook then offers multiple tools for users to search
 122 out and add potential contacts. [. . .] By the time you're done, Facebook has a reasonably
 123 comprehensive snapshot both of who you are and of who you know.¹¹
 124

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

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

132 ¹⁰Alessandro Acquisti and Ralph Gross, Imagined communities: Awareness, information shar-
 133 ing, and privacy on the Facebook, (paper presented at 6th Workshop on Privacy Enhancing
 Technologies, Cambridge, UK, 2006), 2

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

136 So what makes people behave this way, given that there obviously are security and
 137 privacy issues? Why do they provide such detailed, and true¹², personal informa-
 138 tion on their social network site profile? Many explanations can be given, but we
 139 restrict ourselves to some of the most familiar. Acquisti and Gross say: “*Changing*
 140 *cultural trends, familiarity and confidence in digital technologies, lack of exposure*
 141 *or memory of egregious misuses of personal data by others may all play a role in*
 142 *this unprecedented phenomenon of information revelation*”¹³. Grimmelmann argues
 143 that the reason is actually much more straightforward: people misunderstand the
 144 risks involved in presenting detailed and personal information online. This misun-
 145 derstanding takes a number of forms. For one thing, users are often unaware of who
 146 has access to their personal profile and to the content they place online, because the
 147 architecture and design of social network sites is such that it provides individuals
 148 with a false sense of security and privacy. These sites “*systematically [deliver] them*
 149 *signals suggesting an intimate, confidential, and safe setting*”¹⁴, an environment
 150 that is private, “*closed to unwanted outsiders.*”¹⁵. Second, users falsely believe that
 151 there is safety in numbers, in two senses of the expression. They believe that when
 152 everyone else around them massively starts using social network sites, these sites
 153

154 ¹²There are some interesting differences between the level of truthfulness in self-presentations
 155 across different social network sites. Research has shown, for instance, that while the overwhelm-
 156 ing majority of members use their real name on their Facebook profile (a staggering 94,9%
 157 according to Tufekci (Zeynep Tufekci, Can you see me now? Audience and disclosure regula-
 158 tion in online social network sites, *Bulletin of Science, Technology and Society* 28 (2008)). An
 159 even higher number, 99,35%, was found in a 2009 study by Young and Quan-Haase, Information revelation and internet privacy concerns on social net-
 160 work sites: A case study of Facebook, (paper presented at C&T ’09, University Park, Pennsylvania,
 161 USA, 25-27 June, 2009)). In the above-cited article Tufekci shows that, by contrast, in MySpace a
 162 substantial amount of users (38,2%) provide a nickname on their profiles. There are many explana-
 163 tions for such differences. One of the most straightforward ones is the fact that Facebook actively,
 164 and quite strictly, discourages the use of fake names, as was made clear by a tell-tale example
 165 presented by Grimmelmann: “*Facebook applies [its] policy [regarding the ban on the use of fake*
 166 *names] rigorously almost to the point of absurdity. It refused to let the writer R.U. Sirius sign*
 167 *up under that name, even though he’d written six books and hundreds of articles under it and he*
 168 *uses it in everyday life.*” (James Grimmelmann, “Facebook and the social dynamics of privacy
 169 [draft version],” (2008), http://works.bepress.com/james_grimmelmann/20/, 6). Another explana-
 170 tion could be that users want to avoid the fact that their friends cannot find them online. As boyd
 171 writes: “*While teens are trying to make parental access more difficult, their choice to obfuscate key*
 172 *identifying information also makes them invisible to their peers. This is not ideal because teens are*
 173 *going online in order to see and be seen by those who might be able to provide validation.*” (danah
 174 boyd, Why youth (heart) social network sites: The role of networked publics in teenage social life,
 175 In *MacArthur Foundation Series on Digital Learning – Youth, Identity, and Digital Media Volume*,
 176 edited by David Buckingham. (Cambridge, MA: MIT Press, 2008b), 131-132)

175 ¹³Alessandro Acquisti and Ralph Gross, Imagined communities: Awareness, information shar-
 176 ing, and privacy on the Facebook, (paper presented at 6th Workshop on Privacy Enhancing
 177 Technologies, Cambridge, UK, 2006), 2

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

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

10 Keeping Up Appearances

181 must be safe to use, because otherwise others would avoid them (a line of reasoning
 182 that runs the obvious risk of being flawed if everyone follows it), and they believe
 183 the risks they run are very limited since there are so many members in social net-
 184 work sites that chances are in fact really small that something will befall them as
 185 individuals (Grimmelmann, 2008: 17–18).

186 Or, as boyd argues,

187 [m]ost people believe that security through obscurity will serve as a functional barrier
 188 online. For the most part, this is a reasonable assumption. Unless someone is of particu-
 189 lar note or interest, why would anyone search for them? Unfortunately for teens, there are
 190 two groups who have a great deal of interest in them: those who hold power over them –
 191 parents, teachers, local government officials, etc. – and those who wish to prey on them –
 192 marketers and predators.¹⁶

193 Taking things to a more general level one can argue that there are four fundamental
 194 issues surrounding privacy and (unintended) information disclosure in relation to
 195 online worlds¹⁷. These can be summarised as follows:

196 It is difficult or even impossible for users to know what the composition or the
 197 reach of the *audience* is for whom they are presenting their personal information
 198 and content;

199 Since information on the internet can easily be recorded, copied and stored, it
 200 gets a degree of *persistence* that most information in the real world lacks. This
 201 means that information may (intentionally) reach audiences in the (far) future;

202 Information shared in one internet environment may easily be *transported*
 203 (copied, linked) to other contexts. Thus, information that had one meaning in the
 204 original context may gain a different meaning in another context, possibly reflecting
 205 back on the individual in unintended and unforeseen ways;

206 Our online self-presentations are the result of content and information posted
 207 by both ourselves and others, and made up of an amalgam of images ranging from
 208 deliberate and explicit self-presentations to more implicit “traces of self” of which
 209 users are not especially aware. *Controlling* these self-presentations and the possi-
 210 ble deductions others may make on the basis of them is difficult, if not wholly
 211 impossible, for the individual.

212 These four issues are highly relevant to social network sites as well. For one,
 213 when posting content or personal information in a profile, individuals do not know
 214 (exactly) who will be able to access this information. The audience, to phrase it dif-
 215 ferently, is in-transparent. Now, while some social network sites allow users some
 216 level of control over the visibility of the information placed in profiles (e.g., chang-
 217 ing personal information to “visible to friends only”), the default privacy settings
 218

219
 220 ¹⁶danah boyd, Why youth (heart) social network sites: The role of networked publics in teenage
 221 social life, In *MacArthur Foundation Series on Digital Learning – Youth, Identity, and Digital
 222 Media Volume*, edited by David Buckingham. (Cambridge, MA: MIT Press, 2008b), 133

223 ¹⁷See for example: Leysia Palen and Paul Dourish, “Unpacking ‘privacy’ for a networked world,”
 224 (paper presented at Computer-Human Interaction (CHI) Conference 2003, Ft. Lauderdale, Florida,
 225 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)

226 are usually set to “public”, which means that individuals’ profiles and the informa-
 227 tion contained therein can be viewed by anyone accessing the social network site.
 228 This means, Acquisti and Gross conclude, “*that the network is effectively an open*
 229 *community, and its data effectively public.*”¹⁸

230 Second, since information can be copied, saved and stored easily and infinitely,
 231 information placed online at any particular moment may come back to haunt the
 232 individual years down the line. This means that the audience is unlimited both in
 233 terms of its size and makeup (in contrast to audiences in the physical world), but
 234 also in terms of temporality. In the words of Tufekci, the temporal boundaries shift
 235 in such a way that “*the audience can now exist in the future. [. . .] Not only are we*
 236 *deprived of audience management because of spatial boundaries, we also can no*
 237 *longer depend on simultaneity and temporal limits to manage our audiences.*”¹⁹

238 Third, as we will discuss more extensively below, when presenting disparate
 239 identities in various online domains, there is a risk of information from one of
 240 these domains, for instance a personal or professional home pages, seeping into
 241 another, such as someone’s social network site profile. Since different behavioural
 242 rules guide these various domains mixing and merging information about the person
 243 behind all of these various roles can lead to serious problems. Tufekci gives a very
 244 simple, yet illuminating example:

245
 246 For example, a person may act in a way that is appropriate at a friend’s birthday party, but
 247 the photograph taken by someone with a cell phone camera and uploaded to MySpace is
 248 not appropriate for a job interview, nor is it necessarily representative of that person. Yet
 249 that picture and that job interview may now intersect.²⁰

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

261

262

263

264

265

266

267

268

269

270

¹⁸ Alessandro Acquisti and Ralph Gross, Imagined communities: Awareness, information shar-
 ing, 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

10 Keeping Up Appearances

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

276 10.3 Privacy-Preserving Social Networking: Audience 277 Segregation 278

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

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

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

287 To maximise awareness and usability, these tools ought to be easily recognisable
 288 for users. This is why we have taken a social mechanism that individuals use in
 289 everyday life contexts to control the image others have of them and the information
 290 they disclose about themselves: *audience segregation*. Mirroring or mimicking this
 291 real-life strategy in a virtual environment, we have developed a social network site,
 292 Clique, that implements it.
 293
 294

295 10.3.1 Audience Segregation 296

297 The concept of “*audience segregation*” was coined by Erving Goffman²¹ as part of a
 298 perspective on the ways in which identities are constructed and expressed in interac-
 299 tions between human beings in everyday contexts. According to Goffman, whenever
 300 individuals engage in interactions with others they *perform roles*, the goal of which
 301 is to present an image of themselves which is favourable, not only to the personal
 302 goals they are attempting to achieve within the context in which they find them-
 303 selves (strategic interaction), but at the same time also meets with the approval of
 304 those with which they engage in the interaction (“public validation”²²). To Goffman,
 305 then, *impression management* is key in such self-presentations.
 306

307 Individuals performs a wide variety of roles in their everyday lives, relating to
 308 both the places they visit, and the other people present there²³. For instance, when
 309

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

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

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

316 at work, individuals will display different images of themselves than when they are
 317 at home, or when they buy groceries at a local store, or when they visit a movie
 318 theatre. However, the *location* a person finds himself in is not the only relevant
 319 parameter; so is the *presence* (or absence) of *specific other people* in that location.
 320 Individuals will show different sides of themselves when they are at home with their
 321 family than when they are hosting a party for their colleagues in that same home.
 322 The presentation of selves, then, is *situated* or *contextual* – it relates to *where* one
 323 is, and *who else is there* ²⁴.

324 One of the key elements of Goffman’s perspective on identity its the fact that
 325 individuals attempt to present self-images that are both *consistent* and *coherent*. To
 326 accomplish this, performers engage in what Goffman calls “audience segregation”,
 327 “. . .so that the individuals who witness him in one of his roles will not be the indi-
 328 viduals who witness him in another of his roles”²⁵. With segregated audiences for
 329 the presentation of specific roles, people can “maintain face” before each of these
 330 audiences. Their image will not be contaminated by information from other roles
 331 performed in other situations before other audiences, particularly not by information
 332 that may *discredit* a convincing performance in the current situation²⁶. For example,
 333 a person whose professional role consists of displaying a role of authority, such as
 334 a political leader or a judge, may try to shield aspects of his private life from the
 335 public, such as the fact that in his relationship his partner is the one in charge and he
 336 is not an authoritative person at all when at home. He shields this information from
 337 those he may encounter in his professional life to prevent his professional authority
 338 being undermined by their knowing about this aspect of his personal life.

339 While Goffman’s idea of audience segregation didn’t originally relate directly to
 340 privacy, it is easy to see that audience segregation and privacy are, in fact, closely
 341 linked. Helen Nissenbaum has famously argued that privacy revolves around “*con-*
 342 *textual integrity*”, which means that individuals’ personal integrity ought to be
 343 maintained across and between the various contexts they engage in each day²⁷.
 344 Nissenbaum starts from the following observation:

345 Observing the texture of people’s lives, we find them [. . .] moving about, into, and out of
 346 a plurality of distinct realms. They are at home with families, they go to work, they seek
 347 medical care, visit friends, consult with psychiatrists, talk with lawyers, go to the bank,
 348

349 ²⁴Bibi Van den Berg, “Self, script, and situation: Identity in a world of ICTs,” in *The future of*
 350 *identity in the information society: Proceedings of the third IFIP WG 9.2, 9.6/11.6, 11.7/FIDIS*
 351 *International Summer School on the Future of Identity in the Information Society*, ed. Simone
 352 *Fischer-Hübner, Penny Duquenoy, Albin Zuccato and Leonardo Martucci*. (New York, NY:
 353 *Springer, 2008*), and Bibi Van den Berg. *The situated self: Identity in a world of Ambient*
 354 *Intelligence*. (Nijmegen; Wolf Legal Publishers, 2010)

355 ²⁵Erving Goffman. *The presentation of self in everyday life*. (Garden City, NY: Doubleday,
 356 1959), 137

357 ²⁶Erving Goffman. *The presentation of self in everyday life*. (Garden City, NY: Doubleday,
 358 1959), 137

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

10 Keeping Up Appearances

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 Walzer²⁹, 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,

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

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

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

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

406 breadth, variety and uniqueness of socially constricted, contextual ones. Moreover,
407 with multiple audiences to keep into account, it becomes very difficult to decide
408 what “face” to show. The result, says boyd, is social convergence:

409 Social convergence occurs when disparate social contexts are collapsed into one. Even in
410 public settings, people are accustomed to maintaining discrete social contexts separated by
411 space. How one behaves is typically dependent on the norms in a given social context. How
412 one behaves in a pub differs from how one behaves in a family park, even though both are
413 ostensibly public. Social convergence requires people to handle disparate audiences simul-
414 taneously without a social script. While social convergence allows information to be spread
415 more efficiently, this is not always what people desire. As with other forms of convergence,
control is lost with social convergence.³²

416 Therefore, audience segregation offers users the opportunity to be “round charac-
417 ters” in each role, rather than merely “flat ones”, to borrow some terminology from
418 literature studies.

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

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

442 In these multipurpose social network sites individuals connect with both friends,
443 family members, distant relatives, colleagues, acquaintances, old schoolmates,
444 members of their local community, etc. – some of whom are intimately known to
445 them, while others are distant, loose, or even unknown connections. It is easy to see
446 why individuals using such sites might want to make distinctions between the *types*
447

448
449 ³²danah boyd, “Facebook’s privacy trainwreck,” *Convergence: The International Journal of*
450 *Research into New Media Technologies* 14 (2008a), 18

10 Keeping Up Appearances

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

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

474 10.4 A Note on Terminology

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

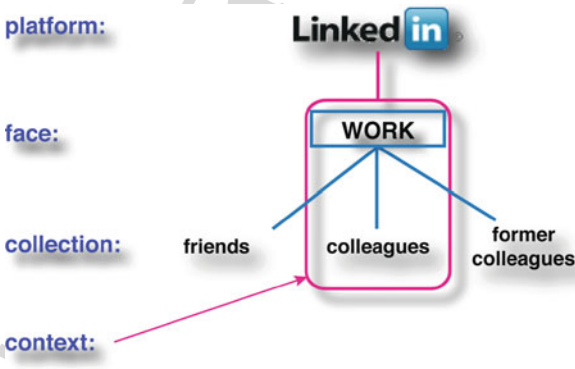
- 482 1. The terms “*platform*” and “social network site” (which we’ve defined in the
 483 introduction to this article) will be used interchangeably;
- 484 2. On the platform a person can create a “*face*”, a profile page on which he displays
 485 particular information about himself. The totality of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

494
 495 ³³This applies, for instance, to one’s e-mail address.

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

523 In the picture below we present a graphic depiction of the structures and concepts

524 we distinguish in relation to social network sites and collaborative workspaces.



AQ2 540 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 connections³⁴. 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

³⁴J. 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

³⁵James 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 there³⁶. 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

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

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

676 Now, one of the most obvious objections to this choice would be the idea that users
677 do not *want* to have this much control over their personal information and personal
678 content in social network sites. In fact, in the past researchers regularly argued that
679 users wouldn't be interested in having possibilities for more fine-grained control
680 over the display of personal data, for instance because making the profile invis-
681 ble makes it harder for other people to find them³⁸, or because they would simply
682 find it too much hassle. However, recent research has shown that, when given the
683 opportunity, many people do in fact want to shield some of their information³⁹,
684 especially since a number of negative examples regarding information spill and pri-
685 vacy issues with respect to social network sites have been published in the press in
686 many Western countries.⁴⁰

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

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

698 When users publish information they are presented with an access control dia-
699 logue as shown in Fig. 10.4 below. In this dialogue window we "nudge"^{41/42} the
700 user to act in a privacy savvy manner without undermining sociality. By default,
701 the user's primary audience (default collection, see Fig. 10.2) is selected as having
702 access to the content to be published. The user can drag collections and individual
703 contacts to the red and green boxes to grow or shrink the audience. Note that in
704 this case, Ronald's colleagues have access to the content to be published, with the
705

706
707 ³⁸See for example: danah boyd, Why youth (heart) social network sites: The role of networked
708 publics in teenage social life, In *MacArthur Foundation Series on Digital Learning – Youth,
709 Identity, and Digital Media Volume*, edited by David Buckingham. (Cambridge, MA: MIT Press,
2008b)

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

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

717 ⁴¹The Nudge 'methodology' consists of: provide incentives, Understand mappings, Defaults, Give
718 feedback, Expect error, Structure complex choices

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

10 Keeping Up Appearances

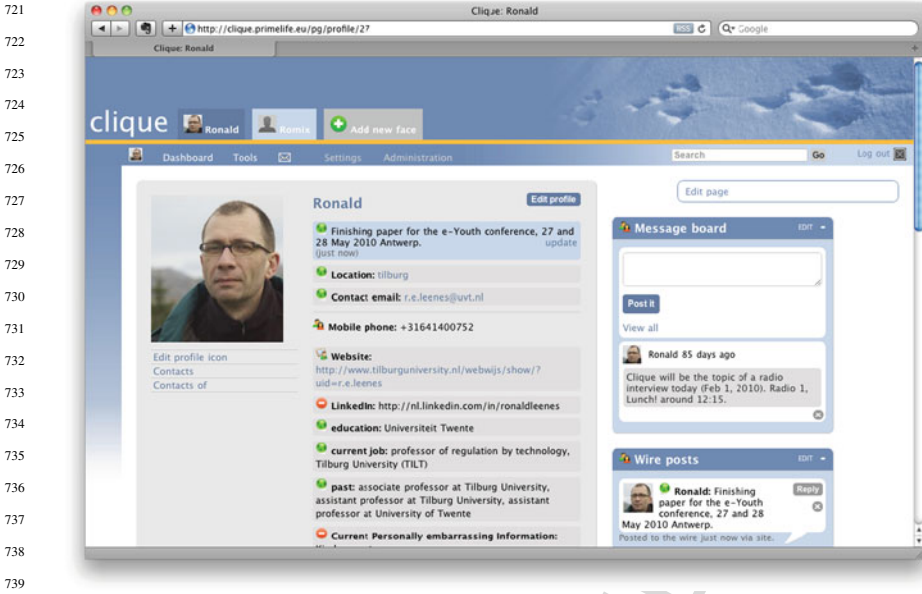


Fig. 10.3 Visibility cues in clique

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.

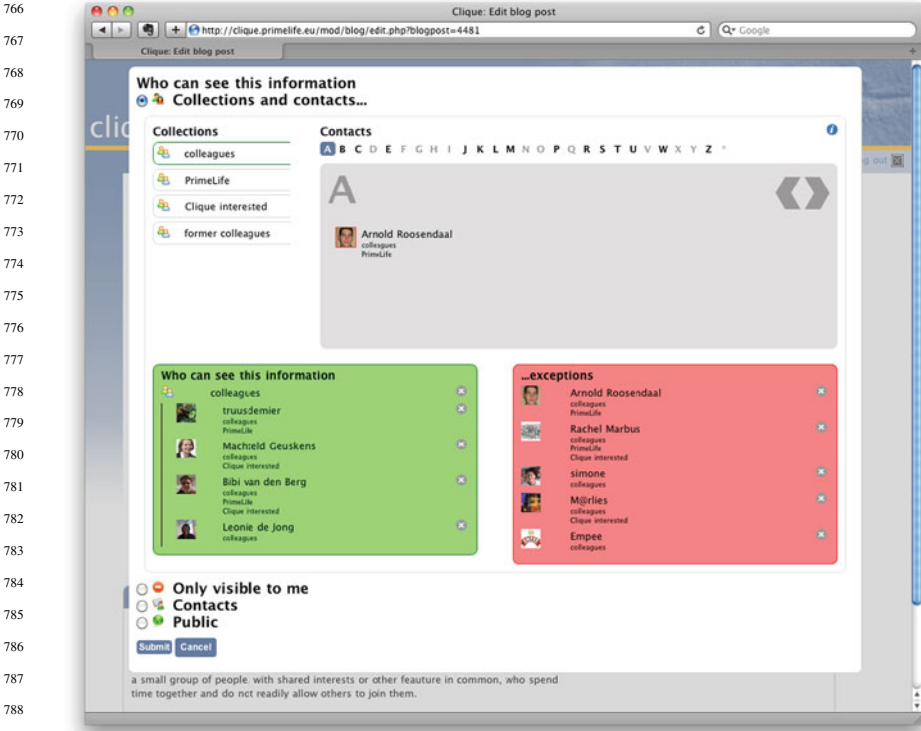


Fig. 10.4 Extended access control dialogue in clique



Fig. 10.5 Audience indicator in clique

10 Keeping Up Appearances



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

856 reduced to an intuitive, easy-to-manage and basic element of the social network
 857 site. This means that the user can engage in interactions with his contacts in a safer
 858 and more “natural” way, without having to manage his information with a high level
 859 of vigilance and privacy-awareness.

860
 861

862 10.6 Conclusion

863

864 Context is a central concept in the disclosure of information. What is appropriate
 865 in one context may not be in another. We have argued that audience segregation is
 866 one of the core mechanisms that people employ in their everyday life to accomplish
 867 contextual integrity and that most current online social network sites have a very
 868 simplistic model of social structures. In our view, technology can be adopted to
 869 help users maintain different partial identities en control who can access their data
 870 even in social networks. We have taken the first steps in developing a prototype that
 871 implements audience segregation.

872

873 Whether or not social network site users can, and will use the mechanisms pro-
 874 vided remains to be seen. To test whether they do, we have set up an experimental
 875 site consisting of the Clique prototype (<http://clique.primelife.eu>). The reader is
 876 invited to participate in this experiment.

877

878 Part of the research leading to these results has received funding from the
 879 European Community’s Seventh Framework Programme (FP7/2007-2013) under
 880 grant agreement No. 216483. The authors want to thank Joeri de Ruiter who did a
 881 tremendous job of implementing the ideas of the authors into the Clique application.

882

883

884

885

886

887

888

889

890

891

892

893

894

895

896

897

898

899

900

References

- 885 Acquisti, A., and R. Gross, Imagined communities: Awareness, information sharing, and pri-
 886 vacy on the Facebook, (paper presented at 6th Workshop on Privacy Enhancing Technologies,
 887 Cambridge, UK, 2006): 36–58.
- 888 Ala-Mutka, K., D. Broster, R. Cachia, C. Centeno, C. Feijóo, A. Haché, S. Kluzer, S. Lindmark,
 889 W. Lusoli, G. Misuraca, Y. Punie, and J.A. Valverde, *The impact of social computing on the EU*
 890 *information society and economy*. Seville: IPTS/JRC, 2009.
- 891 boyd, d., Facebook’s privacy trainwreck, *Convergence: The International Journal of Research into*
 892 *New Media Technologies* 14 (2008a): 13–20.
- 893 boyd, d., Why youth (heart) social network sites: The role of networked publics in teenage social
 894 life, In *MacArthur Foundation Series on Digital Learning – Youth, Identity, and Digital Media*
 895 *Volume*, edited by D. Buckingham, 119–142. Cambridge, MA: MIT Press, 2008b.
- 896 boyd, d., and N.B. Ellison, Social network sites: Definition, history, and scholarship, *Journal of*
 897 *Computer-Mediated Communication* 13 (2007): 210–230.
- 898 Branaman, A., Goffman’s social theory, In *The Goffman reader*, edited by C.C. Lemert and A.
 899 Branaman, xlv–lxxxii. Cambridge, MA: Blackwell Publishers, 1997.
- 900 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).

10 Keeping Up Appearances

- 901 Gross, R., and A. Acquisti, Information revelation and privacy in online social networks (paper
902 presented at WPES'05, Alexandria, Virginia, USA, 2005): 71–81.
- 903 Meyrowitz, J. *No sense of place: The impact of electronic media on social behavior*. New York,
904 NY: Oxford University Press, 1985.
- 905 Nissenbaum, H. Privacy as contextual integrity. *Washington Law Review* 79 (2004): 119–159.
- 906 O'Hara, K., and N. Shadbolt. *The spy in the coffee machine*. Oxford: Oneworld Publications, 2008.
- 907 Palen, L., and P. Dourish. Unpacking 'privacy' for a networked world (paper presented at
908 Computer-Human Interaction (CHI) Conference 2003, Ft. Lauderdale, Florida, USA, 5–10
909 April, 2003): 129–137.
- 910 Solove, D.J. *The future of reputation: Gossip, rumor, and privacy on the Internet*. New Haven, CT:
911 Yale University Press, 2007.
- 912 Thaler, R.H., and C.R. Sunstein. *Nudge: Improving decisions about health, wealth, and happiness*.
913 New Haven, CT: Yale University Press, 2008.
- 914 Tufekci, Z. Can you see me now? Audience and disclosure regulation in online social network
915 sites. *Bulletin of Science, Technology and Society* 28 (2008): 20–36.
- 916 Van den Berg, B. Self, script, and situation: Identity in a world of ICTs. In *The future of iden-*
917 *tity in the information society: Proceedings of the third IFIP WG 9.2, 9.6/11.6, 11.7/FIDIS*
918 *International Summer School on the Future of Identity in the Information Society*, edited by S.
919 Fischer-Hübner, P. Duquenoy, A. Zuccato and L. Martucci, 63–77. New York, NY: Springer,
920 2008.
- 921 Van den Berg, B. *The situated self: Identity in a world of Ambient Intelligence*. Nijmegen: Wolf
922 Legal Publishers, 2010.
- 923 Walzer, M. *Spheres of justice: A defense of pluralism and equality*. New York, NY: Basic Books,
924 1983.
- 925 Young, A.L., and A. Quan-Haase, Information revelation and internet privacy concerns on social
926 network sites: A case study of Facebook (paper presented at C&T '09, University Park,
927 Pennsylvania, USA, 25–27 June, 2009): 265–274.
- 928
- 929
- 930
- 931
- 932
- 933
- 934
- 935
- 936
- 937
- 938
- 939
- 940
- 941
- 942
- 943
- 944
- 945

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”

UNCORRECTED PROOF

946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990