

## Sharing Ephemeral Information in Online Social Networks: Privacy Perceptions and Behaviours

Bernardo Reynolds, Jayant Venkatanathan, Jorge Gonçalves, Vassilis Kostakos

► **To cite this version:**

Bernardo Reynolds, Jayant Venkatanathan, Jorge Gonçalves, Vassilis Kostakos. Sharing Ephemeral Information in Online Social Networks: Privacy Perceptions and Behaviours. 13th International Conference on Human-Computer Interaction (INTERACT), Sep 2011, Lisbon, Portugal. pp.204-215, 10.1007/978-3-642-23765-2\_14 . hal-01591807

**HAL Id: hal-01591807**

**<https://hal.inria.fr/hal-01591807>**

Submitted on 22 Sep 2017

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



# Sharing Ephemeral Information in Online Social Networks: privacy perceptions and behaviours

Bernardo Reynolds, Jayant Venkatanathan, Jorge Gonçalves, Vassilis Kostakos  
Madeira Interactive Technologies Institute  
University of Madeira  
{bernardo.reynolds, vjayant, jorge.goncalves, vk}@m-iti.org

**Abstract.** This paper presents a study where the online Facebook practices of a sample of users (n=103) was analysed over a period of two years, via the scraping of data in Facebook and the collection of questionnaire data. The data allows for a contrast between implicit and explicit attitudes regarding Facebook and online sharing. Our analysis reveals that while overall privacy concerns are not reflected in posting behaviour, awareness and familiarity with privacy controls is. This is supported by contrasting users' attitudes regarding day-to-day sharing against actual behaviour on Facebook. We theorise that there exists a failure in translating users' privacy needs into a social-technical environment such as social networking sites. This work demonstrates how aspects such as demographics and usage influence and shape users' behaviour and practices towards privacy. We therefore argue that the factorization of these aspects may augment the translation of users' privacy needs and improve the design of privacy sensitive mechanisms for day-to-day information sharing.

**Keywords:** Social media, sharing, privacy

## 1 Introduction

Information sharing in the form of hyperlinks, videos, status updates or photographs, has gained increasing popularity with the advent of online social networking sites. With a wide variety of content and objectives, publishing comes in the form of small posts answering to questions such as “What’s happening?” or “What’s on your mind?” These mechanisms enable users to satisfy a natural tendency to explicitly disclose or publicise information about themselves, their opinions and activities [21].

The study presented here contrasts users' attitudes regarding day-to-day sharing against their actual behaviour on Facebook. While previous studies have examined this dichotomy in terms of “static” information such as email address, telephone number, or spouse names, relatively little work has considered this dichotomy in the context of everyday information sharing, i.e. sharing newly generated information, thoughts and ideas. This work is important in understanding how to design privacy mechanisms more appropriate for day-to-day sharing of information.

## 2 Related Work

Emerging communication technologies are fundamentally changing the way we behave, interact, and socialise [16]. As Boyd describes, information shared online becomes persistent, searchable, replicable and subject to invisible audiences [5], giving rise to significant privacy concerns. Because online social networks are denser and more diverse than those offline [17,18], thousands of users may be classified as friends of friends of an individual and be able to access shared personal information [9]. Another detail crucial to privacy is the fact that posts are typically displayed in forward or reverse chronological order. This allows others to infer contextual information about the author, especially when other contextual information like time of creation, platform used (web or mobile) or eventual responses to said posts are aggregated and grouped together, which is the convention in social networking sites. The diversity and richness of online social networks makes it challenging for users to group or categorize the individuals composing their social network, and adds complexity to the process of rule development. At the same time, emergent network effects may further affect group behaviour in terms of attitudes and usage of social systems [15].

Substantial work has considered rule development and privacy regulation, suggesting that these can be understood as a presentation of self [9][10], a formulation of dialectic and dynamic behavioural mechanisms depending on circumstantial context [2] or the conjugation of disclosure, identity and temporal boundaries [21]. What was once achieved with walls, doors and other physical or architectural constraints is still to be adapted to today's communication means [14,24]. Privacy management is an intricate process and is further augmented in a computer-mediated environment. On social networking sites, privacy regulation is a socio-technical activity involving interaction with the technological system and the group context. Individuals' privacy behaviour in such systems involves a mixture of technical and mental strategies. For instance, a technical strategy may involve the use of privacy settings to regulate content distribution to select audiences [23], while research has also shown that considering tie strength is another strategy for developing rules for disclosure [25].

Despite the evidence suggesting that users adopt objective strategies for controlling their privacy online, previous work has identified a discrepancy between people's privacy attitudes towards sharing information and their actual sharing patterns, albeit in the context of static information such as contact details and preferences [1,20]. This behaviour has been termed the "privacy paradox". For instance, studies on the sharing of information by students on Facebook suggests that the number of users who actually change their privacy settings is remarkably scarce [8,11], while a follow-up study further revealed a high discrepancy between stated concerns and actual behaviour towards sharing static profile information on Facebook [1]. Other studies have further established the privacy paradox on social networking sites [24]. A tentative explanation for this dichotomous behaviour is that the perceived benefits of Facebook usage outweigh the risks of disclosing personal information [6]. In addition technical issues may also contribute: Facebook has received considerable criticism due to their technical shortcomings in the subject of privacy, possibly due to the fact that the norms developing around this technology are subject to continuous

evolution [4]. Despite these changing norms, however, previous studies have consistently identified a dichotomy between users' proclaimed privacy concerns and their actual behaviour [1,20].

While previous studies have highlighted the privacy paradox in the context of online social networking, most studies have focused on the sharing of static profile information. Arguably, this information is qualitatively different from the information that users share on a day-to-day basis. Research shows posting about current activity and implying location is a common practice on social networking site users [22]. Such information is more likely to be of an ephemeral nature, and users can always decide on the spot about how and with whom to share this information. The study described next aims to address this issue and to uncover users' posting practices in dealing with ephemeral information.

### **3 Study**

#### **3.1 Theoretical approach**

A study was designed to test whether users' perceptions of privacy towards the sharing of ephemeral information matches their actual behaviour. Given that significant evidence suggests the existence of the privacy paradox, it was hypothesised the same applies to disclosure of ephemeral information:

- H1: Users' privacy attitudes towards sharing ephemeral information do not match their actual behaviour.

Previous research also shows an influence of gender on privacy attitudes [13,23]. Furthermore, while not all teens are members of social network sites, these sites developed significant cultural resonance amongst American teens in a short period of time, as well as Europe. Given that age has a significant influence on social networking site adoption, it is hypothesised that this also shapes privacy concerns in relation to sharing.

- H2: Different demographics have contrasting privacy concerns towards sharing of ephemeral information

#### **3.2 Method**

This study adopted a multi-pronged approach to collect data. Two complementary datasets were collected: a quantitative data set gathered using a Facebook scraping application, and a qualitative dataset gathered through an extensive online questionnaire.

Participants were recruited by advertisements in Facebook, via email, and via notice boards. Participants were promised a chance to enter a draw that would award 40 Euros to 10 participants. Interested participants were invited to add to their profile a Facebook application and notified about the crawler application upon installation. Contacts to address any concerns regarding the data collected were provided at various stages of the studies but never solicited.

The application collected information about participants' past behaviour, including wall posts, status updates, friends, privacy settings for posts and basic user information. Status updates were explicit posts written by participants and wall posts were any other items in participants' wall. The software then has to complete a follow-up questionnaire. Apart from gathering data the application also provided the link to the online questionnaire.

The questionnaire study consisted of 40 questions capturing data for demographics, Facebook usage, privacy attitudes, posting practices, and community. In addition the questionnaire had 10 scenario exercises that asked participants to imagine themselves disclosing various types of information and deciding how to share that information with different people in their network. In example, "last night was so much fun but I have a huge hangover" or "I'm late for a class/meeting". The questionnaire, partially inspired by a previous study on the subject of privacy on Facebook [23], was designed as a between subjects study. The manipulated variable was the optimism of the questions collecting disclosure attitude data: in the optimistic condition participants were asked about what information they wished to share, in the pessimistic condition they were asked about which information they wished to hide. In both conditions the scenarios themselves were identical and the information to be shared was related to participants' activity, location or even personal pictures.

Although Facebook started in a college-oriented context and grew mostly through student networks it has now expanded and diversified to reach all sorts of demographics. The participants mainly came from the university environment. Faculty staff and students, under the premise of being able to win gift certificates, participated in the study. These factors may have introduced some response bias.

## 4 Results

The study was conducted between April and May 2010 with 103 participants (61 male) completing both parts of the study. The age ranges used in the questionnaire were: 1. less than 18 years old (no participants), 2. 18-24 years old, 3. 25-34 years old, 4. 35-44 years old 5. more than 44 years old (no participants). The logging application collected data from August 2007 onwards; earlier data was not accessible due to technical restrictions. The data included 4942 wall posts and 2769 status updates. As a baseline level of relationship between participant's questionnaire and log data, the correlation between stated and actual number of friends was 0.783, with participants on average underestimating their true number of friends by about 16.

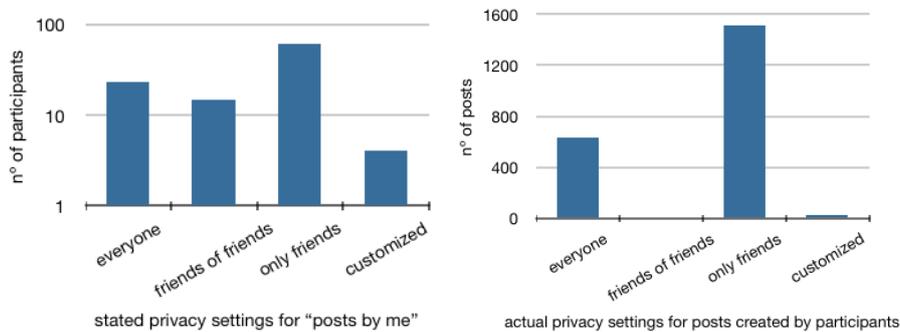
### **H1: Users' privacy attitudes towards sharing ephemeral information do not match their actual behaviour.**

Hypothesis 1 was partially confirmed. Data from the questionnaire showed that most respondents claimed to be Facebook users for 1-2 years, to visit their account daily (38.8%) for 15 minutes (30.1%) and use it mostly to read the newsfeed (76.7%) and posting content (66.9%). With respect to posting practices, the participants asserted that they did not post frequently on Facebook (avg. 2.4 on a 5-point Likert

scale), but the majority claimed to post more often compared to 6 months ago (42.7%). The log data showed an overall average of 8.95 posts per person per month.

This average was 26.4 for the three months leading up to the study, while it was 2.04 over the 3-month period 6 months earlier. Similarly, the average number of explicit status updates was 5.8 per person per month for the whole log, while this average was 5.25 for the three months leading up to the study, and 5.28 for the 3-month period six months earlier.

Regarding privacy attitudes, the questionnaire data shows that participants showed little intent to hide the information they shared from a friend or group of friends (avg. 1.9 on a 5-point Likert scale) and most (54.4%) admitted never having used Facebook’s feature that would allow them to do so. The logged data confirms this claim as only 4 different participants chose to hide a total of 68 posts and only one did so for more than 1 friend. Figure 1 shows a both the stated and actual privacy settings that participants attributed to their own posts.



**Fig. 1.** Stated vs. actual distribution of privacy settings for individual posts.

In their last privacy settings review, participants claimed to have opted for a more private setting (avg. 2.1 on a Likert scale ranging from private to public). Regarding privacy concerns, respondents acknowledged to be worried if all their Facebook friends knew where they had been last night (avg. 3.3 on a 5-point Likert scale), what they were doing at the moment (avg. 3.4). Participants were more worried about non-friends (i.e. strangers) knowing their location at the moment (avg. 4.1), and what they were doing at the moment (avg. 4.1).

Table 1 shows the relationship between participants’ subjective concern about privacy with the number of posts that are shared with big audiences (everyone or all friends) and the frequency of posting. Similarly, Table 2 shows the relationship between participants’ self-perceived frequency of changing their privacy settings on the number of posts that are shared with big audiences (everyone or all friends) and the frequency of posting.

Finally the results revealed no significant impact of the phrasing of the questionnaire (optimistic vs. pessimistic) on participants’ responses, and hence all questionnaires were considered in further analysis.

**Table 1.** Mean ratio of user’s posts visible to “everyone” or “all friends”, and mean posts per month (ppm) broken down by users’ concerns towards privacy.

	(low)				(high)
How concerned are you with privacy?	1	2	3	4	5
Ratio of respondents’ posts with privacy set to “everyone” or “all friends”	27%	32%	26%	27%	31%
ppm:	43	85	51	56	62

**Table 2.** Mean ratio of user’s posts visible to “everyone” or “all friends”, and mean posts per month (ppm) broken down by users’ attitudes towards privacy.

	Rarely				Very Often
How often do you change your privacy settings?	1	2	3	4	5
Ratio of respondents’ posts with privacy set to “everyone” or “all friends”	50%	28%	23%	16%	20%
ppm:	65	59	57	72	23

**H2: Different demographics have contrasting privacy concerns towards sharing of ephemeral information**

Hypothesis 2 was also confirmed. In assessing the effect of gender, a one-way ANOVA shows a significant effect of gender on posts per month ( $F(1,101)=46.404$ ,  $p<0.0001$ ), showing that females post more than males. Furthermore, a chi-square test shows a significant relationship between gender and current privacy setting for “posts by me” ( $\chi^2=9.721$ ,  $df=3$ ,  $p<0.05$ ), showing that females have more “open” privacy settings than males.

In terms of the effect of age, a chi-square test shows a significant relationship between users’ age group and the frequency with which they change their privacy settings ( $\chi^2=15.58$ ,  $df=8$ ,  $p<0.05$ ), showing that older users change their settings more frequently. Additionally, a chi-square test shows a significant relationship between users’ age group and their current privacy setting for “posts by me” ( $\chi^2=34.48$ ,  $df=6$ ,  $p<0.0001$ ), showing that older users have stricter settings.

On average males had 8.04 posts per month on their wall, while females had 9.58. Additionally, 35% of posts by females were visible to “everyone” or “all friends”, while 25% of posts by males had these privacy settings. Privacy attitudes based on gender are shown in Table 3.

**Table 3.** Gender effects on privacy attitudes.

	Gender	
	Female Mean (SD)	Male Mean (SD)
How concerned are you with privacy?	3.88 (1.06)	3.49 (1.09)
How often do you change your privacy settings?	2.55 (0.94)	2.43 (0.97)

Furthermore, a chi-square showed a significant relationship between participants’ age and their reported frequency of changing privacy settings ( $\chi^2 = 240.1$ ,  $df = 15$ ,  $p < 0.0001$ ), with older participants claiming to change their settings more frequently. In addition, the youngest age group posted 7.73 posts per month, gradually increasing to 11.35 posts per month for the oldest age group. The average ratio of posts visible to “everyone” and “all friends” gradually decreased from 33% for the youngest age group to 26% for the oldest group, while their response to “how concerned are you with privacy” increased from 3.5 to 4.0 on a 5-point likert scale respectively.

## 5 Discussion

### Subjective perceptions vs. actual behaviour

The baseline level of correlation between perceived and true number of Facebook friends shows that participants don’t accurately account for their entire network, which may result in poor boundary regulation as users occasionally, and by accident, may give out too much information and experience unwanted approaches [3].

Users were accurate in their assessment that they now post more than in the past. While this is true on average, it does not apply to explicit status updates, but rather to wall-sharing posts. The relative frequency of each activity provides further evidence that on-the-fly ephemeral sharing is more popular than sharing explicit ideas and thoughts, and certainly more popular than the sharing of static profile information.

In terms of participants’ perceptions on privacy, the findings contradict previous results pointing in the direction of an opt-out dynamic for sharing, suggesting that users should have to choose what they wish to hide [5]. Participants responding to the questionnaire had limited intention of explicitly hiding the content they create, and in fact very few actually use of the available means to do so.

However, participants did claim concern about potential privacy threats on Facebook, even though most ephemeral information shared by participants did not reflect these concerns by means of explicit privacy settings. In fact, there was little correlation between participants' broader concern about privacy on Facebook and their actual posting practices: both the number of postings and the portion of those posts visible to a large audience appear to be independent of general privacy attitudes (Table 1).

On the other hand, participants' self-assessment of their frequency of change of privacy settings are in line with their actual posting behaviour: the number of posts and the ratio of posts visible to large audiences decrease as user's self-perceived frequency of changing privacy settings goes up (Table 2).

### **Gender**

In terms of gender differences, females were more concerned about privacy, as also shown in previous studies [13,23]. However, in their actual behaviour females post more often and with fewer privacy restrictions than males. We further analysed the effect of gender in the questionnaire data. In the disclosure scenarios, females were more open across all scenarios except for one. Aside from the first scenario, the optimistic approach was more popular among females than among males. The same was verified on the section where optimistic vs. pessimistic approach was the manipulated variable on a between subjects design. Females were less prone to want to hide their posts when compared to males. Moreover, females made less use of the on-the-fly privacy settings present in the publisher interface.

The results do not imply that females are not worried about privacy, but rather they suggest that females are less pro-active on this issue. These findings demonstrate an incongruity. Although females demonstrate higher concerns in privacy matters, that is not reflected in the strategy they prefer to manage the information they share, nor in the use of available means to better manage the privacy of that information.

### **Age**

Older users claimed to be more concerned with privacy, and their attitude was actually reflected in their posting practices: even though they posted more frequently, their privacy settings were more restrictive than those of younger users. When considering their choice for a pessimistic approach on the information disclosure scenarios, there was no significant difference between younger and older adults. On the other hand, the pessimistic approach resonated more among older participants than among younger ones in the between subjects section of the questionnaire.

Furthermore, older users were less satisfied with the control Facebook provided over their privacy and stated to change their privacy settings more often. Despite this fact, the number of older participants actually using on-the-fly privacy settings to manage the information they share was significantly lower than of younger ones. However, although less elders use this features, the ones who do, do it more frequently than youngsters. These findings contradict recent research demonstrating that young-adult Americans have an aspiration for increased privacy [12] and that the majority of young adult Facebook users are far from being nonchalant and

unconcerned about privacy matters [7]. Our findings contradict these claims to the extent that when compared with elders, young-adults exhibit less concern on the subject of privacy. We find that these findings hold for satisfaction with Facebook's privacy controls, frequency of adjusting privacy settings and last privacy controls review.

In addition, we observed that older users claimed to be more concerned with privacy and their attitude was actually reflected in their posting practices: even though they posted more frequently, their privacy settings were more restrictive than those of younger users. Stated preferences in privacy settings for sharing ephemeral information are consistent with this finding. Older participants stated to use more restrictive settings and also to use less permissive settings when compared to younger participants. Previous research [6] also found that teenagers' rhetoric about online safety with regard to social media mirrored the narratives presented by the news media. This is in agreement with our results in reference to the importance of privacy in the public debate, which was not affected by age. Both young-adults and older ones equally valued the issue.

### **Behaviour over time**

Boyd and Hargittai [7] give prominence to an escalation of engagement with privacy settings from 2009 to 2010. This is congruous with participants' declared adoption of a more private profile in their latest privacy settings review. The proposed justifications for this behaviour are: the increase in public attention to privacy matters, the increased changes in Facebook's default settings and the site prompts to review privacy settings. While we concur with these assumptions we also propose the upsurge in sharing information as a cause for the rise in engagement with privacy settings. Even though our findings reveal an inverse relationship between posting frequency and adjustment of privacy settings, users often rely on the privacy settings to regulate content distribution to select audiences [23].

### **Privacy by design**

Overall, our findings on the influence that gender and age have in privacy attitudes are inline with previous research [7,13,19,23]. Women, in general, are more worried about their privacy when compared to men. Taking into account different criteria such as stated privacy concerns, choice of approach for managing disclosures, preferences in privacy settings to control posts, and other, we can infer that males state to be more open when it comes to sharing information. Lewis et al [19] propose safety concerns as the central cause for this phenomenon. Such safety issues revolve around fear of abuse of social networking sites (SNSs) by sexual predators and other information disclosures risks associated with SNSs. However, such concern is not reflected on their actual behaviour nor on the strategy females chose to manage disclosure.

As for age, younger participants were more permissive and adopted looser controls when sharing information. There is a number of factors that can serve as justification for this circumstance. One is youngsters being born amidst the digital world of today, therefore having more familiarity and trust in services like Facebook. Another is ingenuity as conscience and accountability of actions is something humans grow through life. And as with many other matters, youngsters are typically careless

of the consequences that rise from their actions. Assuming this applies to the act of sharing ephemeral information, it is also safe to assume youngsters are less concerned with the consequences of not managing their privacy.

Significant privacy implications can arise from over-sharing, and the results presented here provide some guidance on how to limit the extent of this phenomenon. First, the results show that users underestimate the size of their audience; therefore it is important to highlight and remind users of its extent.

In addition, users' general privacy concerns are not necessarily manifested in their posting behaviour, with both young and female user groups sharing with larger audiences, thus making them good target groups for redesigned privacy controls. The potential benefit of such a design strategy is underlined by the fact that users are aware that in fact they now share more than in the past, and those who claim awareness and frequent use of privacy controls do in fact share less often and to less people.

### **Design guidelines**

Summarising the results and findings from the study, we present here the following set of principles and respective guidelines.

#### **Principle:** *Demographics shape behaviour towards privacy*

We found divergent privacy concerns and practices across gender and age. These two demographic factors had an influence on privacy concerns, choice of approach to disclosure and others.

**Guideline:** Consider the demographic factors we presented and accommodate those in the design.

**Example:** allowing both experienced and inexperienced users to translate their privacy intentions into privacy settings.

#### **Principle:** *Usage patterns shape behaviour towards privacy*

We demonstrated usage patterns such as time since joining Facebook, frequency of logins to Facebook, time spent on each login and others have a massive influence on privacy practices and concerns like privacy concerns, latest privacy controls review choice and frequency of changing privacy settings.

**Guideline:** Consider all the usage factors we presented and accommodate those in the design.

**Example:** Build usage based privacy settings, e.g. frequently suggest new users of the system to protect their content.

## **6 Conclusion**

This paper presents a study that contrasts users' privacy perceptions about sharing ephemeral information against their actual behaviour. Previous work suggests a dichotomy between these. The findings reveal that while overall privacy concerns are not reflected in posting behaviour, awareness and familiarity with privacy controls is.

We theorise that there exists a failure in translating users' privacy needs into a socio-technical environment such as social networking sites. This study suggests that such a translation relies on successfully factorizing aspects such as, but not limited to, gender and age.

There are a number of ways that the work presented here can be extended. First, one could implement a narrowcasting solution grounded in this work to perform usability tests. In addition, quantitative analysis on user adoption for the Facebook Groups feature could be conducted because it supports narrowcasting shared information. More specifically, user impressions and attitudes towards Groups could be captured. Finally, this kind of work could be extended to a network like Twitter, which is 100% based on status updates, thus rendering further insights.

**Acknowledgments.** We thank Tasos Spiliotopoulos for his valuable comments and everyone who took part in the study. This work is funded by the Portuguese Foundation for Science and Technology (FCT) grant CMU-PT/SE/0028/2008 (Web Security and Privacy).

## References

1. Acquisti, A. and Gross, R.: Imagined communities: awareness, information sharing, and privacy on Facebook. Proc. PET 2006, Springer, 36-56 (2006 )
2. Altman, I.: Privacy Regulation: Culturally Universal or Culturally Specific? *Journal of Social Issues*, 33 (3), 66-84 (1977)
3. Baarkhus, L. and Tashiro, J.: Student Socialization in the Age of Facebook. Proc. of the Conference on Human Factors and Computing Systems: CHI 2010, ACM Press 133-142 (2010)
4. Bellotti, V. and Sellen, A.: Design for Privacy in Ubiquitous Computing Environments. Proc. Third European Conf. Computer-Supported Cooperative Work ECSCW'93 (Milano, Italy), 77-92 (1993)
5. Boyd, D.: Facebook's Privacy Trainwreck: Exposure, Invasion, and Social Convergence. *Convergence* 14, (1) (2008)
6. Boyd, D.: Taken out of context: American teen sociality in networked publics, Ph.D. dissertation, University of California at Berkeley (2008)
7. Boyd, D. and Hargittai, E.: Facebook Privacy Settings: Who Cares? *First Monday* 15 (8) (2010)
8. Debatin, B., Lovejoy, J., Horn, A., Hughes, B.: Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences, *Journal of Computer-Mediated Communication* 15, 83-108 (2009)
9. DiMicco, J.M. and Millen, D.R.: Identity management: multiple presentations of self in Facebook. In *Conference on Supporting Group Work*, ACM Press, 383-386 (2009)
10. Goffman, E.: *The presentation of self in everyday life*. Garden City, NY: Doubleday Anchor (1959)
11. Gross, R. and Acquisti, A.: Information Revelation and Privacy in Online Social Networks. In *Workshop on Privacy in the Electronic Society*, ACM Press (2005)
12. Hoofnagle, C., King, J., Li, S., Turow, J.: How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies? (2010)

13. Joinson, A.N.: Looking at, looking up or keeping up with people?: Motives and use of Facebook. In Conference on Human Factors in Computing Systems (CHI), Florence, Italy, ACM Press, 1027-1036 (2008)
14. Kostakos, V.: A design framework for pervasive computing systems. PhD Thesis, University of Bath, UK. Technical Report CSBU2005-02, ISSN 40-9497 (2005)
15. Kostakos, V.: Is the crowd's wisdom biased? A quantitative analysis of three online communities. In proceedings of Computational Science and Engineering, August 29-31, Vancouver, Canada, 251-255 (2009)
16. Kostakos, V., O'Neill, E., Little, L., & Sillence, E.: The Social Implications of Emerging Technologies. *Interacting with Computers*, 17, 475-483 (2005)
17. Kostakos, V. and Venkatanathan, J.: Making friends in life and online: Equivalence, micro-correlation and value in spatial and transpatial social networks. In proceedings IEEE SocialCom, Minneapolis, USA, pp. 587-594 (2010)
18. Lenhart, A.: Adults and Social Network Websites. Pew Internet and American Life Project. Retrieved January 14, 2009 from [http://www.pewinternet.org/PPF/r/272/report\\_display.asp](http://www.pewinternet.org/PPF/r/272/report_display.asp) (2009)
19. Lewis, K., Kaufman, J., Christakis, N.: The taste for privacy: An analysis of college student privacy settings in an online social network, *Journal of Computer-Mediated Communication*, volume 14, number 1, pp. 79-100, Knowledge Tree 13, May (2008)
20. Norberg, P., Horne, D., Horne, A.D.: The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors, *Journal of Consumer Affairs*, 41 (1), 100-126 (2007)
21. Palen, L., Dourish, P.: Unpacking Privacy for a Networked World. In Proc. of the Conference on Human Factors and Computing Systems: CHI 2003, ACM Press 129-136 (2003)
22. Patterson, D.J., Baker, C., Ding, X., Kaufman, S.J., Liu, K., Zaldivar, A.: Online everywhere: evolving mobile instant messaging practices. In Proceedings of UbiComp '08, vol. 344 ACM, New York, NY, 64-73
23. Stuntzman, F., Kramer-Duffield, J.: Friending only: examining a privacy-enhancing behaviour in Facebook. In Proc. of the Conference on Human Factors and Computing Systems: CHI 2010, ACM Press 1553-1562 (2010)
24. Tufekci, Z.: Can You See Me Now? Audience and Disclosure Management in Online Social Networking Sites. *Bulletin of Science and Technology Studies*. Volume 11, Number 4, June, pp. 544-564(21) (2008)
25. Wellman, B. and Wortley, S.: Different Strokes from Different Folks: Community Ties and Social Support. *American Journal of Sociology* 96, 3, 558-588 (1990)