Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2009 Proceedings

Americas Conference on Information Systems (AMCIS)

2009

I Didn't Know You Could See That: The Effect of Social Networking Environment Characteristics on Publicness and Self-Disclosure

Jacqueline C. Pike
University of Pittsburgh, jpike@katz.pitt.edu

Patrick J. Bateman
Youngstown State University, pjbateman@ysu.edu

Brian S. Butler
University of Pittsburgh - Bradford, bbutler@katz.pitt.edu

Follow this and additional works at: http://aisel.aisnet.org/amcis2009

I Didn't Know You Could See That:
The Effect of Social Networking Environment Characteristics on Publicness and Self-Disclosure

Jacqueline C. Pike
University of Pittsburgh
jpike@katz.pitt.edu

Patrick J. Bateman
Youngstown State University
pjbateman@ysu.edu

Brian S. Butler
University of Pittsburgh
bbutler@katz.pitt.edu

ABSTRACT

Web 2.0 technologies have changed the way users interact with the Internet. Users play a growing role in the generation of content, and while doing so disclose a piece of themselves. We seek to provide a theoretical link between the boundary characteristics of a social networking website and self-disclosure. Utilizing Communication Privacy Management Theory, we focus on two forms of boundaries: mode of entry boundary and ingroup/outgroup boundary. We propose that these boundaries play a role in the implicit boundary coordination and negotiation between the users of the environment and the website. This negotiation influences users' perceived publicness of the environment, which influences their self-disclosure behaviors due to their risk avoidance. It is believed that by recognizing the public aspect of participation in online social networks, we can provide suggestions on how its perception can be managed to encourage, or discourage, contributions and disclosures of information by users.

Keywords

Social networking, social computing, publicness, disclosure, boundaries, Internet, Web 2.0

INTRODUCTION

At one time most Internet users were simply consumers of information. The Internet provided users with a way to obtain information while maintaining their anonymity and privacy. Although users were often asked to provide personal information, the importance of privacy issues in e-commerce made individuals remain reluctant to do so (Awad and Krishnan 2006; Metzger 2004). However, the emergence of Web 2.0 technologies has changed the way users interact with the Internet. No longer are users only consuming information; they are now generating content as well (Tapscott and Williams 2008). Whether recording daily events in a blog, creating a podcast, or developing a virtual identity on a social networking site, users now play a large part in creating web content which is available to countless others.

Social networking websites, also referred to as social computing websites, are publicly accessible meeting spaces where users present information about themselves and digest information about others. These sites often involve large numbers of users (e.g. MySpace.com surpassed 100 million users in August 2006 and Facebook has over 67 million users, half of which visit every day). Scholars have specified three characteristics that are common across most social networking sites: 1.) users construct profiles, 2.) users specify other users with whom they have a relationship, and 3.) the specification of a relationship allows for viewing of information generated by the other party in the relationship (Boyd and Ellison 2007; Parameswaran and Whinston 2007). Social networking websites and the technology behind them facilitate the flow of streams of text, photos, and videos ranging from the silly (e.g. YouTube videos of pets) to the profound (e.g. raw video of combat and conflict in the Middle East) (Treese 2006). These sites have created a new medium for public self-expression that not only allows people to connect with others who share an area of interest, but also possesses the power to potentially shape public opinion, drive commerce, and change society.

User-generated content is key to the success of social networks (Sullivan and Thaw 2006). While from a viewer's perspective the content of these sites is just another consumable item, the individuals who provide the material these are often

construction significant public self-expressions. Whether they are sharing personal information about themselves (e.g. profile), posting media (e.g. photos and videos), or openly connecting with loved ones, friends, and acquaintances (e.g. friend lists), individuals reveal clues about their offline identity, gender, age, race, and geographic location (Douglas and McGarty 2002). Participation in social networking environment requires users to share a piece of their personal selves, or self-disclose information. Though, it is important to recognize that the disclosed information may not be factual (Carter 2005).

The issue of self-disclosure is of particular interest in the context of social networking environments. First, the user-generated content is typically freely accessible to anyone, which increases the public nature of the contribution (Goffman 1963; Slevin 2000). Second, contributed content is stored, and hence is persistent, allowing it to be read for an indefinite length of time by unknown future audiences. As a result, contributors lose control of their contribution in an environment where the trustworthiness and morality of others who have access to the information cannot be governed (Ware 1984).

While the information systems literature has focused on privacy related issues (for review see Awad et al. 2006), it has not fully considered the public dimension created by new sociotechnical systems. This paper is aimed at better understanding the public nature of these online spaces by examining how the perceived publicness of a social networking website impacts users' disclosure of information. Utilizing Communication Privacy Management Theory (Petronio 2000), we argue that characteristics of a social networking environment, specifically its mode of entry boundary and ingroup/outgroup boundary, create psychological boundaries around the personal information, impact users' perceptions of how public the space is, and ultimately shape individuals' self-disclosure behaviors.

THE PUBLIC ASPECT OF SOCIAL NETWORKING ENVIRONMENTS

Since the first years of the Internet, scholars have examined the potential and realized relationships between the Internet and the public sphere. Some scholars hypothesized that the Internet had the potential to create a new public sphere online, but found that only a lower quality duplication was developed in a given context (Dahlberg 2001). However, this situation may be changing due to the emergence of sociotechnical systems that provide users with a greater ability to create rich online identities and easily detail their daily lives and happenings. These new public spaces, known as a "virtual public," are relatively transparent and open computer-mediated spaces which allow groups of individuals to attend and contribute to online interpersonal interactions (Aarseth 1997; Carter 2005; Jones and Rafaeli 1999, p. 1; Papacharissi 2002).

However, there is some debate over the issue of publicness on the Internet. Goffman analogizes public presentation to a performance on a stage for a given audience. Sociology scholars have found that Goffman's conceptualization of publicness does not apply to mass communication media and web technology (Slevin 2000; Thompson 1996). Instead Slevin suggests that the Internet has created a new kind of publicness and argues that the old definition of publicness requires two people to be in the same space at the same time, while today's publicness involves people "using communication media to make information and their points of view visible and available to others" (2000, p. 182). Slevin's (2000) definition of publicness describes much of the activity which occurs in social networking environments.

The key difference between Goffman's and Slevin's definitions of publicness lies in the performer's awareness of the degree of access possessed by the audience to the information presented. When a group of people occupy a shared physical space, the performer is aware that others have essentially unrestricted access to his or her statements and actions. In contrast, in online spaces performers may, or may not, form this awareness of others. Hence, in addition to differing with respect to their true publicness, that is the degree to which others have unrestricted access to the space or information (Goffman 1963; Slevin 2000), online spaces may also differ in their perceived publicness, or the degree to which users believe that others have unrestricted access to their information.

Self-Disclosure

Self-disclosure is any information about the self that a person communicates to another (Wheeless and Grotz 1976). In the context of social networking, online self-disclosure involves communicating personal information about the self via contributions to a website. Social networking environments (e.g. MySpace.com, Facebook.com, Linkedin.com) provide a combination of tools that help users create various forms of content, many of which involve self-disclosure.

The creation of an online identity or profile is one such tool that is common to most social networking websites (Boyd et al. 2007). Users create accounts on a social networking website which are associated with their virtual identities. When creating accounts, users are asked for their email address, first and last name, gender, date of birth, and preferred language. Other optional information which users can contribute may include relationship status, sexual preferences, specific location (e.g. zip code, city, country), political affiliation, and religious affiliation. In many cases, registered members, or those with accounts, have the ability to create content and publish information about themselves, which is typically provided for others on web

pages that are solely dedicated to the user. This content can include, but is not limited to, photographs, videos, activities, general interests, entertainment interests, favorite books, and personal heroes. Provision of personal and contact information is often encouraged and displayed prominently on the website. Members of the website can record relationships with other members by identifying them as "friends." Oftentimes, the "friend" designation provides the user with special privileges, such as the ability to view additional content created by the user. Finally, members of the website can record comments on other users' profiles. This is analogous to a guestbook since anyone can record a message and everyone who visits the profile can view the messages. All of these tools either directly or indirectly involve the disclosure of personal information about the user.

Individuals desire minimized vulnerability and loss of face (Petronio 2000). As such, a user who perceives the social networking environment to be less public will tend to disclose more personal information because the risk of vulnerability is lower. Conversely, a user who perceives the site to be more public will tend to disclose less personal information as the risk of vulnerability is higher.

> Hypothesis 1: The perceived publicness of a social networking environment is negatively associated with the willingness of users to self-disclose in the environment.

ONLINE DISCLOSURE, PUBLICNESS & BOUNDARIES

To better understand how features of social networking websites affect willingness and tendency to self-disclose, we draw upon Communication Privacy Management Theory[1] (Petronio 1991, 2000, 2004), which posits that individuals balance their need for privacy and their need for disclosure. When deciding to share personal information individuals erect psychological boundaries between what they are willing to disclose to others and what they are not (Petronio 1991, 2000, 2004). These boundaries involve dimensions of: information ownership, individuals believe that they own their information; control, or who has restricted access to information; and permeability, in that they allow certain types of information to flow through. Individuals construct these boundaries because self-disclosure is perceived as risky and may result in vulnerability or loss of face (Petronio 1991). The development of these boundaries is driven by rule-based management systems, involving boundary rule formation, boundary rule usage, boundary rule coordination, and boundary rule turbulence (Petronio 2000).

We focus on one aspect particularly relevant to social networking environment, that of boundary coordination. Prior to communicating, boundary coordination must take place (Petronio 2000). This process involves the potential discloser negotiating with the receiver of the information and determining if the boundary rules provided by the receiver are sufficient. Once the information is shared by the discloser, the information is co-owned by the discloser and the receiver. The receiver, or co-owner, of the information can be an individual, family, group, or organization (Petronio 2000). If boundary coordination is not possible, communication is unlikely (Petronio 2000).

Contributing to an online community represents a form of communication. In social networking environments, the communication takes place between the user and the website, consisting of a technological artifact and a group of unknown others. As the group is not strictly defined, it is not possible for the individual to coordinate boundaries with the others. Since information ownership, control, and permeability rules cannot be worked out with each receiver directly, the negotiation can take place indirectly through the technological artifact of the website (Burnett and Bonnici 2003). In social networking environments, the receivers delegate the boundary rule definition to the system, relying on the processes by which other users select and are selected to implicitly drive a "negotiation," which matches contributing and consuming users who agree on boundary rules. Individuals who agree to accept the environment's boundary rules will be willing to engage in self-disclosure in that environment.

Indirect boundary negotiation places a heightened importance on the individual user's perceptions of the social networking systems' implicit boundary rules. Each social networking environment's technological artifact provides static boundaries put forth during boundary negotiation. Two typical boundaries reflected in social networking technological artifacts are mode of entry boundaries and ingroup/outgroup boundaries (depicted in Figure 1). As the environment's boundaries are static, the user must decide if the environment's boundaries sufficiently to meet the user's boundary requirements.

---

[1] Communication Privacy Management Theory is also known as Communication Boundary Management Theory. Communication Privacy Management Theory is the updated terminology.
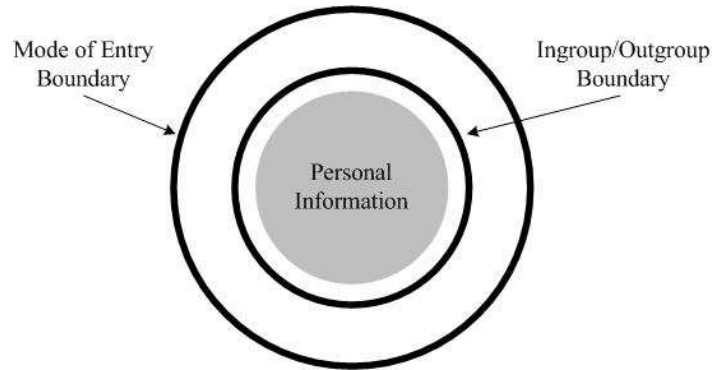
Figure 1. Static Boundaries in the Social Networking Environment

Petronio (2000) suggests that users want to minimize risk and vulnerability when disclosing personal information. However, in a field study of the popular social networking website Facebook.com, Gross and Acquisti (2005) and Stutzman (2006) found that student users demonstrate a lack of concern for privacy risks. However, it may not be that these users are unconcerned with privacy. Instead the users may perceive the site to have low publicness due to its boundary characteristics. Hence they are willing to act as if is a "less – public" space.

Mode of Entry Boundary

The mode of entry boundary creates the first boundary between the personal information in a social networking website and potential receivers. The mode of entry boundary can restrict, to varying degrees, any Internet user from viewing the information in the environment. The mode of entry boundary is instantiated by two aspects of the environment during users' identity creation. First, the mode of entry boundary can be created by requiring an Internet user to create an account or identity before viewing the information in the site which includes the disclosures. Also, the environment may require a referral by someone who has an account in order to create an account. These boundaries are enforced by the website, and the user disclosing information on the website is aware that they exist because he or she had to go through the process when creating an identity. Thus, if a username/password and referral is required, a high mode of entry boundary between the information and potential receivers of the information exists. Users would be less likely to perceive the website as having high publicness, and as a result they may be more willing to self-disclose. If no username/password or referral is required, a low mode of entry boundary exists; users may perceive the site to be more public.

> Hypothesis 2: A social networking environment's mode of entry boundary is negatively associated with perceived publicness. Specifically, a high mode of entry boundary is perceived as less public, and a low mode of entry boundary is perceived as more public.

Ingroup/Outgroup Boundary

The ingroup/outgroup boundary creates a second boundary between personal information in a social networking website and potential receivers. This boundary divides the users of the social networking environment into either "friends" of the user or "non-friends." A "friend" is a user who the discloser has designated as part of his or her social network. If this boundary is high, only users who have been designated as "friends" of the disclosing user will be able to view the disclosed information. If this boundary is low, any user will be able to view the provided information. In other words, there is no distinction between the ingroup and outgroup or the "friends" and "non-friends."

> Hypothesis 3: A social networking environment's ingroup/outgroup boundary is negatively associated with perceived publicness. Specifically, a high ingroup/outgroup boundary is perceived as less public, and a low ingroup/outgroup boundary is perceived as more public.

If users perceive the mode of entry and ingroup/outgroup boundaries in social networking environments as risk mitigating, and perceive the environment as less threatening, they should also then be more willing to disclose more information, assuming their desire for public self-expression is low. This is discussed further below. As shown in Figure 1, the ingroup/outgroup boundary is only triggered if there is a permeable mode of entry boundary. If the mode of entry boundary is sufficiently to meets the discloser's boundary requirements, the need for an in/group outgroup boundary is lessened. As a

result, we expect that there will be a stronger relationship between the mode of entry boundary and perceived publicness than between the ingroup/outgroup boundary and perceived publicness.

> Hypothesis 4: The relationship between a social networking environment's mode of entry boundary and perceived publicness is stronger than the relationship between the ingroup/outgroup boundary and perceived publicness.
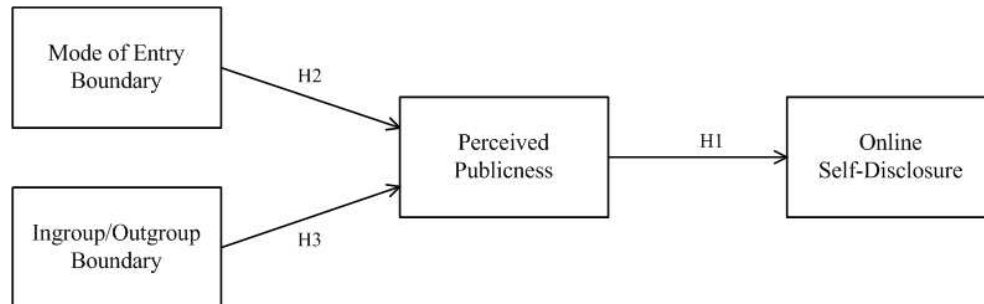

Figure 2. Research Model

RESEARCH METHOD

To examine the proposed research model and hypotheses, an online experiment was conducted with a 2x2 (mode of entry boundary x ingroup/group boundary) between subjects design. Participants were recruited via postings in social networking websites and emails sent to undergraduate and graduate business courses. Following recruitment, the participants were asked to complete a two-part web-based survey which administered the treatment during the second part.

Participants

To recruit participants, an invitation to provide feedback on a social networking website was posted on existing social networking websites (with administrator permission) and emailed to students (with instructor permission). This invitation was viewed 646 times, with 148 individuals selecting to access the new site, leading to 140 starting part one of the study, and 87 completing part one. Of these participants, 54 undertook and completed the second part. Following established procedures for calculating response rates for surveys in online environments (Ridings, Gefen and Arinze 2002) produced a response rate for the first part of 58.7% of individuals who accessed the site completed part one or 13.4% of individuals who read the posted invitation to participate in the study completed part one. For the second part, 62.0% of eligible participants completed the study, or 8.4% of those who read the original invitation to participate completed. Participants were normally distributed with respect to the use of the Internet and social networking website use. Eighty-two percent of participants were male, and fifty-six percent of participants were college graduates.

Treatment and Measures

The experiment was conducted using an online survey and was administered in two parts. Following recruitment, participants were linked to the first part of the study, which asked about participant's offline self-disclosure behaviors (as a control) along with demographic variables. The pool of participants who completed this first part of the survey was then randomly assigned to one of four conditions for the second stage, which occurred approximately ten days after part one. In this stage, participants were first told that user testing for a new social networking environment was being conducted and were asked to read a description of this new environment. This description included a description of the technological features of the website, including the ability to create a profile about oneself, enter information frequently in a log format, upload images or video, and record social connections. The description also indicated whether or not a referral was required to join the site and whether users must have an account and be logged to view the site (manipulation of mode of entry boundary) and whether users can view a profile without a record of a social connection existing on the website (manipulation of ingroup/outgroup boundary). The four conditions are summarized in Table 1.

		In-group / Out-group Boundary	
		High: Only specified people can view profile	**Low:** Anyone can view profile
Mode of Entry Boundary	**High:** Login required and referral required to view profile	Condition 1	Condition 2
	Low: No login required and referral required to view profile	Condition 3	Condition 4

Table 1. Experiment Conditions

After reading the description, participants were asked to answer questions regarding the perceived publicness of the environment and their willingness to self-disclose in the environment, as well as manipulation check questions. Items for self-disclosure items were adapted from Wheeless and Grotz (1976) and the perceived publicness were loosely adapted from Antonsen and Jørgensen (1997).

These data were employed in a simultaneous test of structural and measurement models using Partial Least Squares, Smart PLS 2 (Ringle, Wende and Will 2005). The adequacy of the measurement model was assessed using three common tests of convergent validity (Chin 1998; Hulland 1999). Items loaded on their intended constructs greater than 0.7, indicating that there was more shared variance between a construct and measure than error variance (Carmines and Zeller 1979). Second, the internal consistency of each construct was assessed using composite reliability (Werts, Linn and Jöreskog 1974), and the lowest found was 0.90, well in excess of Nunnally's (1978) 0.7 guideline. Third, the average variance extracted (Fornell and Larcker 1981) was calculated for each scale, which measures the average amount of variance that a construct captures from its indicators relative to the amount due to measurement error. All scales exceeded Chin's (1998) guideline of 0.5, meaning that at least 50% of variance in indicators was accounted for by its respective construct. To assess discriminant validity, the correlations of items with their intended constructs was examined, and found that all items correlated most strongly with their intended construct. The square root of AVE for each construct exceeded all respective inter-construct correlations, providing further evidence of discriminant validity. Table 2 provides a summary of the results of these measurement model analyses. The control variables were offline self-disclosure tendencies, age, gender, and education. To ensure the two treatments produced their intended effects, we conducted paired t-tests using the manipulation check items. The results demonstrated that the treatments held as expected (mode of entry treatment: $t(53)=-6.852$ ($p<.000$), ingroup/outgroup treatment: $t(53)=-9.997$ ($p<.000$)).

		# of Items	Mean	Std. Dev.	Cronbach's Alpha	Internal Consistency	AVE	1	2	3	4	5	6	7	8
1	Mode of Entry	1	5.28	0.80	n.a.	n.a.	n.a.	**1.00**							
2	In/Out Group	1	5.17	0.81	n.a.	n.a.	n.a.	0.15	**1.00**						
3	Perceived Publicness	6	3.95	1.99	.95	0.96	0.81	0.70	0.23	**0.65**					
4	Online Self-Disclosure	5	2.72	1.22	0.89	0.92	0.70	-0.20	-0.21	-0.26	**0.49**				
5	Offline Self-Disclosure	4	2.99	1.32	0.86	0.90	0.70	-0.09	0.07	0.08	0.38	**0.49**			
6	Age	1	2.35	.62	n.a.	n.a.	n.a.	0.09	-0.16	0.02	-0.04	0.05	**1.00**		
7	Gender	1	.18	0.39	n.a.	n.a.	n.a.	-0.10	-0.05	-0.10	0.19	0.19	-0.20	**1.00**	
8	Education	1	2.81	0.91	n.a.	n.a.	n.a.	-0.16	-0.39	-0.12	0.18	0.22	0.35	-0.11	**1.00**

[1] Diagonal elements are the square root of Average Variance Extracted

Table 2. Convergent and Discriminant Validity

ANALYSIS AND RESULTS

The hypotheses were tested by examining the size and significance[2] of structural paths in the PLS analysis and the percentage of variance explained. These results are reported in Figure 3.
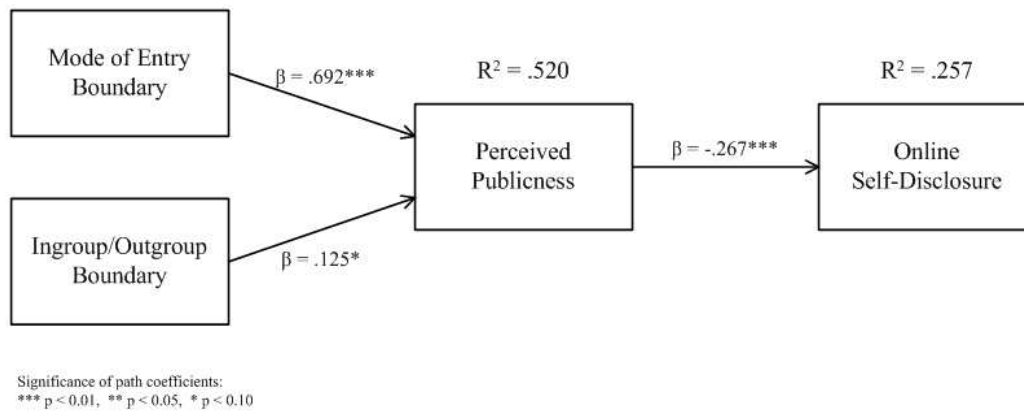

Figure 3. PLS Path Model

First, the model explained 25.7% of the variance in online self-disclosure. Perceived publicness (H1, ß = -0.267, p<.001) significantly influenced online self-disclosure. In other words, the more a user believes that other have unrestricted access to his or her information, the less likely the user will self-disclose in the social networking website. Next, the model explained 52.0% of the variance in perceived publicness. Mode of entry boundary (H2, ß = 0.692, p<.001) and ingroup/outgroup boundary (H3, ß = 0.125, p<.10) were both significantly associated with perceived publicness as hypothesized. Finally, mode of entry had a stronger influence on perceived publicness than ingroup/outgroup boundary, as hypothesized in H4.

The control variable of offline self-disclosure significantly predicted online self-disclosure (ß = 0.28, p<.001). Neither age, education, nor gender significantly influenced the dependent variable.

DISCUSSION

Business models utilizing social networking technologies rely on individuals being willing to engage in self-disclosure because the disclosures attract new and returning users. In order to inform the design and redesign of social networking environments, this research provides a theoretical link between the characteristics of a social networking environment and users' willingness to self-disclosure in the environment. This theoretical link is the perceived publicness construct. Highlighting perceived publicness as an important aspect of an environment could be one way to address tensions that exist between social networking business models focused on expansion and users attempting to manage the boundaries around their personal information. The results of this research run contrary to existing thought on social networking sites that suggests that users disclose information because they want other people to see it (Boyd 2008). This research suggests that while users are self-disclosing in social networking sites, they may not actually want all users to have access to it.

Social networking environments have started to face a variety of issues brought about by the collection and storage of self-disclosed personal information. This information can be misused or used with malicious intent with, or without, an individual's knowledge. In response, some social networking sites have considered stronger measures, such as age verification; however, these are easily circumvented. This highlights the overlooked public nature of these spaces, and that self-disclosure of information can have unintended, or even unwanted, impacts. Rather than directly encourage (or limit) self-disclosure, administrators might try to influence it through the boundary characteristics of the site. This research could also inform designers of environments where self-disclosure is desired but not often performed, such as product review

---

[2] PLS produces standardized regression coefficients for structural paths. Bootstrapping techniques, a nonparametric approach for estimating the precision of paths, were used to test for significance using 500 re-samples.

websites, or where undesired self-disclosure occurs. Social networking environments are also becoming more widely used inside of organizations as a tool for cross-functional collaboration. Thus, designing these environments to encourage disclosure and use is important for managers of organizations as well.

CONCLUSION

This research contributes to our knowledge of why users of social networking environments are willing to disclose personal information in the environments. We suggested that characteristics of the environment's boundaries affect self-disclosure by influencing how public the user perceives the environment to be and presented theoretical and empirical evidence for this claim. Given the large amount of variance in perceived publicness explained and its influence on self-disclosure, we hope to put forth the concept of perceived publicness in social networking environments as worthy of further study.

REFERENCES

1.   Aarseth, E.J. (1997) *Cybertext: Perspectives on ergodic literature* Johns Hopkins University Press, Baltimore, MD.

2.   Antonsen, M., and Jørgensen, T.B. (1997) "The 'publicness' of public organizations," *Public Administration* 75, 337-357.

3.   Awad, N.F., and Krishnan, M.S. (2006) "The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization," *MIS Quarterly* 30, 1, 13-28.

4.   Boyd, D. (2008) "Why youth ♥ social network sites: The role of networked publics in teenage social life," in: *Youth, identity, and the digital media,* D. Buckingham (ed.), MIT Press, Cambridge, MA, 119-142.

5.   Boyd, D.M., and Ellison, N.B. (2007) "Social network sites: Definition, history, and scholarship," *Journal of Computer-Mediated Communication* 13, 1.

6.   Burnett, G., and Bonnici, L. (2003) "Beyond the faq: Explicit and implicit norms in usenet newsgroups," *Library & Information Science Research* 25, 3, 333.

7.   Carmines, E.G., and Zeller, R.A. (1979) *Reliability and validity assessment* Sage, Beverly Hills, CA.

8.   Carter, D. (2005) "Living in virtual communities: An ethnography of human relationships in cyberspace," *Information, Communication & Society* 8, 2, 148-167.

9.   Chin, W.W. (1998) "The partial least squares approach for structural equation modeling," in: *Modern methods for business research,* G.A. Marcoulides (ed.), Lawrence Erlbaum, 295-336.

10.   Dahlberg, L. (2001) "Computer-mediated communication and the public sphere: A critical analysis," *Journal of Computer-Mediated Communication* 7, 1, 5th article.

11.   Douglas, K.M., and Mcgarty, C. (2002) "Internet identifiability and beyond: A model of the effects of identifiability on communicative behavior," *Group Dynamics: Theory, Research, and Practice* 6, 1, 17–26.

12.   Fornell, C., and Larcker, D. (1981) "Evaluating structural equation models with unobservable variables and measurement error," *Journal of Marketing Research* 18, 1, 39-50.

13.   Goffman, E. (1963) *Behavior in public places: Notes on the social organization of gatherings* The Free Press of Glencoe, Collier-MacMillan Ltd., London.

14.   Gross, R., and Acquisti, A. (2005) "Information revelation and privacy in online social networks," WPES, Alexandria, Virginia, 71-80.

15.   Hulland, J. (1999) "Use of partial least squares (pls) in strategic management research: A review of four studies," *Strategic Management Journal* 20, 2, 195-204.

16.   Jones, Q., and Rafaeli, S. (1999) "User population and user contributions to virtual publics: A systems model," *Proceedings of the International ACM SIGGROUP Conference on Supporting Group Work* 239 - 248.

17.   Metzger, M.J. (2004) "Privacy, trust, and disclosure: Exploring barriers to electronic commerce," *Journal of Computer-Mediated Communication* 9, 4.

18.   Nunnally, J.C. (1978) *Psychometric theory*, (2nd ed.) McGraw Hill, New York.

19.   Papacharissi, Z. (2002) "The virtual sphere: The internet as a public sphere," *New Media & Society* 4, 1, 9-27.

20.   Parameswaran, M., and Whinston, A. (2007) "Social computing: An overview," *Communication of the Association for Information Systems* 19, 762-780.

21.   Petronio, S. (1991) "Communication boundary management: A theoretical model of managing disclosure of private information between marital couples," *Communication Theory* 1, 4, 311-335.

22.   Petronio, S. (2000) "The boundaries of privacy: Praxis of everyday life," in: *Balancing the secrets of private disclosures,* S. Petronio (ed.), Lawrence Erlbaum Associates, Mahwah, N. J., 37-50.

23.   Petronio, S. (2004) "Road to developing communication privacy management theory: Narrative in progress, please stand by," *The Journal of Family Communication* 4, 3 & 4, 193-207.

24.   Ridings, C.M., Gefen, D., and Arinze, B. (2002) "Some antecedents and effects of trust in virtual communities," *The Journal of Strategic Information Systems* 11, 3-4, 271-295.

25.   Ringle, C.M., Wende, S., and Will, A. (2005) "Smartpls 2.0 (beta)," University of Hamburg.

26.   Slevin, J. (2000) "Publicness and the internet," in: *The internet and society*, Polity Press, Cambridge, 181-197.

27.   Stutzman, F. (2006) "An evaluation of identity-sharing behavior in social network communities," *International Digital and Media Arts Journal* 3.

28.   Sullivan, B., and Thaw, J. (2006) "Facebook, courted by yahoo, won't sell, director says," in: *Bloomberg*.

29.   Tapscott, D., and Williams, A.D. (2008) *Wikinomics: How mass collaboration changes everything* Portfolio, New York, NY.

30.   Thompson, J.B. (1996) *The media and modernity: A social theory of the media* Stanford University Press, Stanford.

31.   Treese, W. (2006) "Ten years on internet time," 15-17.

32.   Ware, W.H. (1984) "Information systems security and privacy," *Communications of the ACM* 27, 4, 315-321.

33.   Werts, C.E., Linn, R.L., and Jöreskog, K.G. (1974) "Intraclass reliability estimates: Testing structural assumptions," *Educational and Psychological Measurement* 34, 25-33.

34.   Wheeless, L.R., and Grotz, J. (1976) "Conceptualization and measurement of reported self-disclosure," *Human Communication Research* 2, 4, 338-346.