

Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites

Zeynep Tufekci

University of Maryland, Baltimore County

The prevailing paradigm in Internet privacy literature, treating privacy within a context merely of rights and violations, is inadequate for studying the Internet as a social realm. Following Goffman on self-presentation and Altman's theorizing of privacy as an optimization between competing pressures for disclosure and withdrawal, the author investigates the mechanisms used by a sample (n = 704) of college students, the vast majority users of Facebook and Myspace, to negotiate boundaries between public and private. Findings show little to no relationship between online privacy concerns and information disclosure on online social network sites. Students manage unwanted audience concerns by adjusting profile visibility and using nicknames but not by restricting the information within the profile. Mechanisms analogous to boundary regulation in physical space, such as walls, locks, and doors, are favored; little adaptation is made to the Internet's key features of persistence, searchability, and cross-indexability. The author also finds significant racial and gender differences.

Keywords: *privacy; disclosure; social network sites; Goffman; Altman; presentation of the self; Facebook; Myspace*

The erosion of privacy because of information technologies has gathered both scholarly and popular attention. Worrisome stories about identity theft and stolen credit card numbers regularly show up in newspapers and television news. Concerns about erosion of civil liberties because of government surveillance are compounded by the fact that so many of our transactions—social, commercial, informational, and governmental—now occur electronically, subjecting

them de facto to storage and later retrieval. The latest twist on this concern is privacy threats that result from *voluntary* disclosures, especially by younger adults and minors. Recently, this issue has garnered (relentless) media coverage in the context of social network sites such as Facebook and Myspace.

Many commentators seemed puzzled by the high levels of personal information revealed online by the younger generation. “Why would anyone put that much information about herself on a Web page” seems to be an implicit question that puzzles parents and educators. Why won't kids increase privacy protections on their profiles? These types of threats to privacy seem to be far more within the locus of personal control than, say, government surveillance or data theft.

In this article, I argue that a better understanding of this conundrum can be achieved by recognizing that in the self-presentation (Goffman, 1959) context provided by these Web sites, privacy should be understood as a process of optimization (Altman, 1975) between disclosure and withdrawal. The kids *want* to be seen. While that is hardly surprising, what is new and threatening is that the process of seeing and being seen has migrated to digital environments which confound the traditional ways in which we control our audiences and negotiate the boundary between the private and the public, the past and the future, disclosure and privacy.

Information Technology and Privacy

Information technology erodes privacy in novel ways, connected to its key distinguishing features of persistence, searchability and cross-indexability. A spoken conversation is ephemeral; unless someone is

AUTHOR'S NOTE: The author would like to thank the editor of this issue, Jacquelyn Burkell, and anonymous reviewers for their insightful and constructive comments on an earlier draft of this article. Portions of this research were supported by the Department of Sociology and Anthropology at the University of Maryland, Baltimore County.

Bulletin of Science, Technology & Society Vol. 28, No. 1, February 2008, 20-36

DOI: 10.1177/0270467607311484

Copyright © 2008 Sage Publications

recording it then and there, it is lost forever. If the police have no wiretap on your phone today, they cannot turn back the clock and recover a conversation if you become a suspect next month. That is not the case with electronic transmissions, which generally are stored by Internet service providers, archived by search engines, and documented in cookies and Web histories *by default*. The point is not that it is not possible to record, wiretap, or otherwise capture these interactions in the physical world but that it is not possible to do so *without specific prior arrangement*.

Increasing portions of our social, communicative, and commercial acts now take place in this digital world of effortless, habitual, involuntary persistence. What was once ephemeral, with evidence of it living only in the memory of the current witnesses—a conversation in a cafe, a cash purchase in a store, a nod toward an acquaintance while walking down the street—is increasingly enacted online, where it leaves a potentially lasting imprint. Furthermore, the format in which the information persists, the digital record, is easily searchable and cross-indexable with other data, other conversations, other purchases, other transactions. This certainly creates a vigorous threat to privacy (Agre & Rotenberg, 1997; Solove, 2004; Whitaker, 1999).

Common activities on the Internet can be categorized under three broad headings: commercial, informational, and communicative (social) (Kraut, Mukhopadhyay, Szczypula, Kiesler, & Scherlis, 1999; Weiser, 2001). In analyses of privacy dynamics, these different types of activities should not be treated as an undifferentiated cluster of similar behavior. The first two mostly correspond to instrumental uses; examples include purchasing airline tickets or looking up the weather. There is a clear desired outcome, and although little to nothing is gained for the user from disclosing of information about the transaction to any other party, it is advantageous for commercial interests, and sometimes the government, to log, collect, and analyze these data, thus setting up a conflict between relatively powerful interests and the relatively powerless user. This individualized collection of personal information has been conceptualized as a “digital dossier,” defined as the collection of our traces online that can be logged, stored, and retrieved (Solove, 2004). Certainly, the existence of these traces is a major concern, with important social implications.

For many people, the Internet is increasingly “a social ecology involving other people, values, norms and social contexts” (Petric, 2006). Through networked

computers, people communicate with their social contacts through multiple mechanisms, some synchronous (instant messaging and chat) and some asynchronous (e-mail). Furthermore, people often create self-presentations, such as personal home pages and profile pages in social network sites. Questions of privacy arising from social representations and interactions, which I refer to as *technologically mediated sociality*, should be analyzed in a framework that takes into account the dynamic boundary between the public and the private in social interactions, with careful cognizance of the disparities and dissimilarities between the social Internet, on one hand, and the commercial and the informational, on the other hand. I refer to the latter as the *instrumental Internet* and the former as the *expressive Internet*.

In technologically mediated sociality, *being seen* by those we wish to be seen by, in ways we wish to be seen, and thereby engaging in identity expression, communication and impression management are central motivations. The question is less one of data security, as it often is with the instrumental Internet, and more one of visibility, boundary setting, and audience management. What do we want to show to whom? Who can see us? Who’s looking at us?

The social ecology framework of Irwin Altman (1975) provides a conceptually rich multidimensional dynamic model for interpreting the interpersonal regulation of privacy. Altman’s model, developed before the advent of the online social realm, sees privacy as a set of “interpersonal boundary-control processes,” by which a person asserts control over how much he or she is open to various others. This regulatory process is dialectic in that contact is both restricted and sought, and it is optimizing in that there is, in any given situation and moment, a desired balance. Privacy also incorporates the management of how much input to accept from others and how much to participate and share of oneself. Altman’s behavioral mechanisms for achieving optimal privacy in any given situation involve verbal and paraverbal behavior, control of personal space, claiming of territory, and cultural mechanisms by which norms and rules about contact are negotiated among people within a group.

The most important difference between Altman’s (1975) model and the more limited conception of privacy as social withdrawal, or, as commonly stated, “the right to be let alone,”¹ is that more privacy is not necessarily the most desired outcome. Altman proposes that there is an “optimal degree of desired access of the self to the others at any moment in time”

(p. 11). A state of perfect privacy would be akin to a state of absolute solitude, which is not only undesirable but also the harshest modern judicial punishment short of the death penalty.

Many of the mechanisms for negotiating the boundary between what is kept private and what is made public depend greatly on use and control of space, architectural boundaries, and signaling (Altman, 1977). Locks and doors, eye contact, gestures, words, physically moving away, and many other mechanisms are unavailable in a simple form in technologically mediated sociality, and there are other specific characteristics of online environments that undermine some of the taken-for-granted means of privacy regulation.

Palen and Dourish (2003) expand Altman's (1975) conceptualization of privacy by taking into account the specific threats (and opportunities) afforded by information technology. They classify the new challenges into three categories: threats to spatial boundaries, threats to temporal boundaries because of persistence of data, and intersections between multiple spaces.

First, we no longer have a sense of the spatial boundaries of our audience. As Goffman (1959) explored, self-presentation is a conscious, interactive act that requires both an awareness of and participation from the audience. However, in technologically mediated sociality, the audience has been obscured. We can no longer see who is looking, nor, sometimes, can we even make an educated guess. If one is in a street corner, a classroom, the beach, or a bar, the audience is limited by walls, doors, and distance. Although it is possible that there may be unexpected members within the audience, the presence of others is much more transparent than it is on the Web.

Second, the "recordability and the subsequent persistence of information" shifts the temporal boundaries such that the audience can now exist *in the future*. Recall Altman's view of optimal privacy as "desired access to self and others at any moment in time." But which point "in time" are we talking about in an environment where persistence and recording are the norm? Not only are we deprived of audience management because of spatial boundaries, we also can no longer depend on simultaneity and temporal limits to manage our audiences.

The third threat to optimal privacy created by information technology is the "intersections of multiple physical and virtual spaces, each with potentially differing behavioral requirements" (Palen & Dourish, 2003, p. 130). This creates the "steady erosion of clearly situated action," as highlighted by Grudin (2001), and

greatly compounds audience management problems (Goffman, 1959). For example, a person may act in a way that is appropriate at a friend's birthday party, but the photograph taken by someone with a cell phone camera and uploaded to Myspace is not appropriate for a job interview, nor is it necessarily representative of that person. Yet that picture and that job interview may now intersect.

Adopting Altman's view of privacy as a "selective control of access to the self," we will explore the boundary negotiations, especially the "disclosure-nondisclosure boundary" in one particular online environment, social network sites. It is important to note here that publicity is not just a concern for celebrities and politicians: People, especially young people, seek to be public, to be seen, and, of course, to look at others. And online social network sites provide a very powerful tool for that purpose.

Online Social Network Sites

While online social network sites come in many flavors, we can identify some core features. They center around the profile, which is "a representation of their [selves] (and, often, of their own social networks)—to others to peruse, with the intention of contacting or being contacted by others" (Gross, Acquisti, & Heinz, 2005). boyd, who has conducted extensive ethnography on these sites and with their users for many years, offers this definition: "A 'social network site' is a category of Web sites with profiles, semi-persistent public commentary on the profile, and a traversable publicly articulated social network displayed in relation to the profile" (boyd, 2006).²

Two of the most prominent online social network sites are Facebook and Myspace. Facebook originally started as a Harvard site and rapidly spread to other colleges. While it has recently opened to the general public, it is still dominated by college users. More importantly, Facebook is divided into "networks," which for college students means their schools. The default setting is that only people in your college (network) can see your full profile, while all others can see only the profile picture, the name of your home network, and the name provided by the owner of the profile. Therefore, at least for college students, Facebook has a close connection between offline and online social environments (Ellison, Steinfield, & Lampe, 2007), especially because to join a college's network, one must have a valid dot-edu e-mail from that school. Facebook is sometimes perceived as a "walled garden" because of this separation into distinct networks.

Furthermore, Facebook is not indexed by Google,³ unlike Myspace, which is globally searchable by all Internet users.

Myspace is not divided into networks or subgroups the way Facebook is. It started as a general social network site, open to all users, and has garnered a lot more negative media attention partly because it always had a portion of younger users (unlike Facebook, which opened up to high school students just last year), prompting fears of sexual predators somehow connecting and exploiting this population.

Almost all social network sites allow various levels of privacy controls, the most important of which is the level of “visibility.” In Facebook, the default visibility level is visibility to everyone in the “network,” that is, everyone in the college for a college student. There is no such walled area in Myspace. However, both in Facebook and in Myspace, one may also restrict the profile to “friends only,” meaning that only other profiles that are explicitly linked as a “friend” can access one’s profile. It is important to note that “friend” in a social network site is not synonymous with “friend” as it is generally understood, but there is some overlap between the concepts. In her research, boyd (2006) has found that people “friend” (verb) for a multitude of reasons, and our individual interviews and focus groups confirm that.

While versions of these sites have been around for many years, it is only in the past few years that they have exploded in popularity. Consequently, there are relatively few academic articles and systematic studies of these sites, although the number has been increasing lately. The existence of such Web sites also expands research methods because it is possible to do quantitative analysis via mass downloading of the profiles, in addition to traditional ethnographic and survey studies. Downloading of profiles has been done more often for Facebook, mostly because of the fact that it is easier to identify boundaries (i.e., to download a particular college).

Jones and Soltren (2005) downloaded the entire campus networks for MIT, Harvard, New York University, and the University of Oklahoma. Most methods of downloading can access only profiles that are set as visible to everyone within the network. Jones and Soltern were able to download 72.3% of all profiles in all three schools. They found that more than 60.0% of the students disclosed information such as favorite book, music, and interests, while 17.1% disclosed their cell phone number. Stutzman (2006) also downloaded the visible network for incoming freshmen at the University of North Carolina, Chapel Hill and found that 88.0% of the students were using Facebook, 96.2%

had disclosed their birthday, 83.2% had disclosed relationship status, 74.7% disclosed political views, and 16.4% shared their cell phone number.

Acquisti and Gross (2006; Gross, Acquisti, & Heinz, 2005) at Carnegie Mellon have also downloaded profiles in addition to surveying students. They found that “CMU users of the Facebook provide an astonishing amount of information.” According to their sweep, 39.9% listed a phone number, and the majority of users disclosed data such as their dating preferences, relationship status, and political views. Acquisti and Gross also found that very few had privacy settings that would restrict the visibility of the profile, and concluded that “it would appear that the population of Facebook users we have studied is, by [and] large, quite oblivious, unconcerned, or just pragmatic about their personal privacy.”

Acquisti and Gross (2006) followed up with a survey examining the privacy beliefs of Facebook users. Their survey included undergraduate students, graduate students, staff, and faculty, so we will report on the undergraduate portion of their survey ($n = 189$). They found that privacy concerns and Facebook usage by undergraduate students were not statistically linked; students seemed to use Facebook regardless of their stated concerns about privacy. They also found that after one has joined Facebook, “there is very little marginal [difference] in information revelation across groups [distinguished by privacy concerns]—which may be the result of perceived peer pressure or herding.” Acquisti and Gross wondered if disclosure was because of lack of awareness of profile visibility and probed this issue. They found that students seemed to be generally aware of the true level of the visibility of their profiles and that the vast majority reported being satisfied with the current level of visibility and searchability of their profiles.

At Michigan State, Lampe, Ellison, and Steinfeld (2006, 2007) also downloaded and surveyed students regarding their Facebook usage. Only 19% of the profiles were set as “friends only.” Not only did they find high levels of disclosure as reported elsewhere, they also discovered that higher levels of disclosure were associated with a greater number of friends. However, it remains unexplored whether users differentiate between different kinds of disclosure and whether privacy concerns in general, or specific audience management issues in particular, mediate disclosure.

Current Research

This research examines undergraduate students’ disclosure behavior on Facebook and Myspace and the

relationship between disclosure and privacy concerns and fear of unwanted audiences. We first look whether general online privacy concerns were related to the decision to start using online social network sites. We then analyze specific disclosure levels in light of privacy concerns. Unlike most previous research, we do not restrict our survey to Facebook but examine behavior on Myspace, where different expectations of audience and disclosure may hold.

We also wanted to separate general and specific audience concerns from general privacy concerns. As Palen and Dourish (2003) point out, loss of control over the audience is one of the main challenges in finding a balance among disclosure, publicity, and privacy. Thus, we also included as a variable in our analysis unwanted gaze on profile, a measurement of students' concern over the possibility that somebody they did not want to would see their profile. That is likely a more pressing concern to students than more abstract notions of privacy or imagined threats such as a random stranger or an unspecified person in the future looking at their profile.

We also wanted to look at specific disclosures. Existing research does establish that students disclose a fair amount. However, all disclosures may not carry the same weight—both Facebook and Myspace include fields ranging from the innocuous favorite book to potentially more sensitive questions such as sexual orientation. We probed whether general privacy concerns and general or specific audience concerns had an impact on types of disclosure.

We also wanted to probe for the use of instruments similar to those identified by Altman and others as privacy-regulation mechanisms in physical spaces, such as walls, locks, and even disguises. First, we examined the identifiers participants used in their profiles, which may be their real name or a nickname; each has different implications with regard to others finding one's profile. We also looked at whether the participants used profile visibility levels as a means of audience management. Recognizing the existence of privacy-regulating cultural norms and technical defaults in online environments, we contrasted the use of these strategies in Myspace and in Facebook.

Finally, we analyzed students' awareness of privacy threats that derive from specific future audiences because of searchability and persistence of online records. We asked them how likely they thought it was that a future employer, a future romantic partner, a government agency, or a corporation would look at their social network site profile and whether that had

Table 1. Demographics of the Combined Sample

	Percentage of the Sample
Gender	
Female	52.6
Male	47.4
Race/ethnicity	
White	45.2
African American	12.7
Hispanic	2.3
Asian American	31.2
Other	8.6
Grade	
Freshman	44.7
Sophomore	28.9
Junior	19.2
Senior	9.2
Social network site	
User	85.4
Nonuser	14.6

Note: $N = 601$.

an effect on their use of real names, profile visibility, and levels of disclosure.

Method

Sample

The research was conducted in a midsized public research university in the mid-Atlantic region of the United States. The data were compiled in three waves: May and December 2006 and spring 2007. The participants were students enrolled in multiple sections of an introductory social science course. Students in four sections of the course were surveyed in the first round, while students in two sections were surveyed in the second and third rounds. In total, we collected 704 usable surveys. Demographic characteristics of the sample are described in Table 1.

While this is a convenience sample and thus has limited generalizability, its characteristics were generally representative of the university as a whole because this introductory class was a popular choice to fulfill a university-wide social science requirement. Women were somewhat overrepresented (52.6%, as opposed to 44.0% in the university as a whole). The sample had a significant portion of first-year students (44.0%), who tend to be heavy users of social network sites. Students, to the degree they had declared majors, ranged from humanities and social sciences to engineering and physical sciences and were not concentrated in any particular major.

Before combining the samples, data from the three waves were compared with regard to key variables. Demographically, there were no statistically significant differences either in the racial or gender composition or in the average age of the participants, reflecting the relatively constant composition of the introductory class. We then analyzed if there were statistically significant differences between the answers in different data collection rounds. We found that the students' self-reported behavior and attitudes vis-à-vis social network sites remained remarkably steady over the rounds in question. There were very few statistically significant differences, and to the degree these differences existed they were mostly reflective of an increase in privacy awareness and concerns—an unsurprising development given the intense media focus during this period on the alleged dangers of social network sites. We have thus combined the three samples and analyze the whole ($N = 704$) sample, except when there were important differences between the three data collection points, which then are noted as relevant.

Measures and Variables

Most of our questions were asked in identical form to participants in all three waves of data collection, except where noted.⁴ Many of our variables were related to students' use of social network sites. Almost all students who had a profile on any social network site had a profile on Facebook, while slightly more than half had a profile on Myspace. About half had a profile on both, and a very small percentage (3.3%) had a profile only on a different site. The social network site usage breakdown is presented in Table 2.

We measured all students' baseline privacy concerns in online environments but delved into more detail for social network site users. To gauge general online privacy concerns, the participants were asked, "How concerned are you with online privacy?" (indicated as "general privacy" in the tables). Response options ranged from 1 (*not concerned at all*) to 4 (*very concerned*). For social network site users, we asked about general unwanted audiences with the question, "How concerned are you that people you do not want to see your profile will see it?" (indicated as "unwanted gaze" in the tables). For the third round, we asked the future *likelihood* of an employer, romantic partner, government, or corporation looking at their social network site profile. Basic descriptive information for these variables is listed on Table 3.

We probed whether students used their real names on Facebook or on Myspace. Profiles can be made visible at different levels, the most common settings being "visible to friends only" or "visible to everyone." We asked

Table 2. Social Network Site (SNS) Choices

	As Percentage of SNS Users
Has profile on	
Facebook (FB)	91.2
Myspace (MS)	55.5
Choice of SNS (% of SNS users)	
Only FB	40.7
Only MS	4.8
Both FB and MS	50.5
Another SNS (neither FB nor MS)	3.3

Note: $N = 601$.

Table 3. Scales, Means, and Standard Deviations of Key Measures

	<i>M</i>	<i>SD</i>
General concern with online privacy ^a	2.76	0.960
General unwanted audiences ^b	2.91	1.048
Likelihood of future audiences ^c		
Employer	2.90	1.143
Romantic partner	3.62	1.344
Government agency	2.63	1.280
Corporation	2.55	1.227

a. Scale of 1 to 4 (1 = *not concerned at all*, 2 = *a little concerned*, 3 = *somewhat concerned*, 4 = *very concerned*).

b. Scale of 1 to 5 (1 = *never thought about it*, 2 = *not concerned at all*, 3 = *a little concerned*, 4 = *somewhat concerned*, 5 = *very concerned*).

c. Scale of 1 to 5 (1 = *never thought about it*, 2 = *not likely at all*, 3 = *a little likely*, 4 = *somewhat likely*, 5 = *very likely*).

about levels of visibility of the profile separately for Facebook and Myspace, except for the first sample, when the two were combined (thus making interpretation ambiguous). Our analysis in the text notes this discrepancy and separates out the results from the first data-collection round. Also, the small (3.3%) group of users who had no profile on Facebook or Myspace are excluded from questions about behavior on these sites.

We asked all social network site users the types of information they chose to disclose on their profile. In this article, we analyze the most common fields: favorite music, favorite book, favorite movie, political view, romantic status, sexual orientation (added on second and third data-collection rounds), religion, phone number, classes, and address. The answers were collected dichotomously, as yes or no.

Findings

In line with previous research, we found that 85.4% of the sample already had a profile on at least one

Table 4. Social Network Site Use and Privacy Concerns (t Test)

	User	Nonuser	<i>t</i>	<i>df</i>	Sig. (Two-Tailed)
<i>N</i>	515	184	2.320	687	.021
<i>M</i>	2.73 ^a	2.98 ^a			
<i>SD</i>	0.954	0.969			

a. Scale of 1 to 4 (1 = *not concerned at all*, 2 = *a little concerned*, 3 = *somewhat concerned*, 4 = *very concerned*).

social network site, a particularly striking fact since these sites have existed in their current format for only a few years. These sites were also adopted more quickly by the younger students: Significantly more 18-year-old students had profiles, compared to those above 18. Of 18-year-olds, 91.4% had a profile on a social network site, compared to 83.2% of those above 18. ($\chi^2 = 7.190$, asymp. two-sided $p = .007$).

The Decision to Step Into the Social Network Site World

Even though there is a great deal of media coverage of online privacy problems, the participants were not overly worried. The mean response to the question about general online privacy concerns was 2.76 (4 = *high concern*, 1 = *no concern*), indicating some, but not extreme, concern.

We tested to see whether those expressing higher degrees of privacy concerns were less likely to use social network sites. Indeed, nonusers of social network site had higher levels of privacy concerns (see Table 4).

Navigating Disclosure Once Within

Once within the social network sites, levels of self-disclosure were relatively high. We asked whether they used a real name or a made-up name for their Facebook or Myspace profiles. An overwhelming 94.9% of Facebook users reported using their real names—indeed, in interviews conducted in conjunction with this research project, students reported that it is expected that one use a real name in Facebook. While students used their real names less often on Myspace, which is open to the World Wide Web and “Googlable,” a sizable majority, 62.8%, still reported using their real names.

While almost all students used their real name in Facebook, in contrast to Myspace, they were more likely to restrict the viewing of their profiles only to

Table 5. Real Name and Profile Visibility

	Percentage Using Real Name	Percentage With Profile Visible to Everyone
Facebook	94.9	42.2
Myspace	62.7	59.0

Table 6. Logistic Regression Results: Odds (e^b) of Having Made Profile Visible to Everyone (Instead of Only to Friends), Differentiated by Social Network Site (Data Collection Rounds 2 and 3)

	Profile Visible to Everyone on Facebook	Profile Visible to Everyone on Myspace
General privacy	0.962	0.940
Unwanted profile gaze	0.640***	0.614**
Male	1.641 [†]	2.504***
White	0.858	1.261
Age	1.210*	1.060
Baseline odds (constant)	0.076	1.790
<i>N</i>	287	187

[†].05 < p < .10; * p < .05; ** p < .01; *** p < .001.

their friends in Facebook compared to Myspace (see Table 5).⁵

Contrary to expectations, there was no association between using a real name and making the profile visible to everyone. In other words, participants were equally likely to make their profiles visible regardless of whether or not they used their real name.

To probe students' choice to use a real name versus a made-up name, we ran a logistic regression with two predictor variables: the students' general level of concern about online privacy and specific audience concerns (“How concerned are you that people you do not want to see your profile will see it?”). We controlled for gender, age, and race (White or not). We report the results in two tables, Table 6 and Table 7. Table 6 shows data from data-collection Rounds 2 and 3, in which we differentiated between Myspace and Facebook, while Table 7 reports results from Round 1, in which we asked only whether the students' profiles were visible to everyone on each site on which the students had a profile.

The results show that students did adjust their profile's visibility based on their fear of their profile

Table 7. Logistic Regression Results: Odds (e^B) of Having Made Profile Visible to Everyone (Instead of Only to Friends), Undifferentiated by Social Network Site (Data Collection Round One)

	Profile Visible to Everyone
General privacy	1.417
Unwanted profile gaze	0.623**
Male	6.423***
White	1.019
Age	1.011
Baseline odds (constant)	0.745
<i>N</i>	223

* $p < .05$; ** $p < .01$; *** $p < .001$.

being found by unwanted audiences both on Myspace and on Facebook, but their general views on online privacy did not have an effect. On both sites, people were about 40% less likely to make their profile visible to everyone for each level of increase in their concern over the profile being found by unwanted others. Also, men were significantly more likely than women to make their profile visible to everyone on Myspace.⁶ On Facebook, the difference between the genders approached statistical significance ($p = .06$).

Concern over audience and disclosure levels. Profiles on social network sites contain many fields that are presented in a relatively standardized format on the Web page. While any user may choose not to fill (and thus not display on his or her profile) any of the fields, we found that such behavior is relatively rare. This is true especially on Facebook and, among the participant population, students in college.⁷

We asked users whether they indicated their favorite music, book, or movie, their political views, their romantic status—which on Facebook can have values such as “single” or “in a relationship with someone” (often named and linked)—their interests, their sexual orientation (often indicated by “looking for” field, which can say men and/or women), their religion, their phone number and address, and the classes in which they were enrolled. The percentage of students disclosing such information is shown in Table 8 categorized by gender and in Table 9 categorized by race.

As can be seen from Table 8, large percentages of students express their music, book, and movie preferences. Almost half indicate their political views and religion. Two thirds indicate their romantic status and their sexual orientation. Almost half note the classes in which they are enrolled, allowing them to easily search for—and be searched by—their classmates.

While fewer students choose to include information such as their phone numbers and addresses, the proportions are still sizable: One third note their phone numbers on their profiles.

Examining for gender and racial differences, we find that, unsurprisingly, there is a sharp gender divergence in phone number disclosure, with many more men than women noting their phone numbers. On the other hand, women are more likely to indicate their favorite music and books and their religion. While Anglo students are more likely to use their real names on Myspace and indicate their romantic status and interests, African American students are more likely than Anglo and Asian students to indicate their religion.

We ran 12 separate logistic regressions looking at how privacy and unwanted audience concerns relate to disclosure and visibility strategies. Our predictor variables were students' general level of concern about online privacy, their concern about unwanted audiences in general, and gender, age, and race (White or not). Our dependent variables were the types of information disclosed (book, music, sexual orientation, romantic status, etc.) and whether or not a real name was used. The results of the logistic regression, showing the odds ratios, are given in Table 10. These analyses show that fear of profile being seen by unwanted audiences (unwanted gaze) has a significant impact on whether students use their real name on Myspace, but not on Facebook (where real name use is nearly universal). The only other impact of the fear of being found by unwanted audiences was apparent in whether the students indicated their religion. The only other privacy concern that was manifested in disclosure behavior was a relationship between general online privacy concerns and the tendency to indicate phone numbers. Disclosure levels in the rest of the fields were not associated at statistically significant levels with either general privacy concerns or concerns about unwanted audiences.

Disclosure behavior on these Web sites was more heavily influenced by demographic characteristics of the participants. The odds of a man indicating his phone number were 3 times that of a woman, and the odds of him indicating his address were 1.5 times that of a woman, even after controlling for privacy and audience concerns. Anglo students were also more likely to indicate their favorite music and books and much more likely to indicate their romantic status than were non-Anglo students but were less likely to indicate their religion. The tendency to indicate political views, romantic status, sexual orientation, phone number, and classes decreased with age.

(text continues on p. 31)

Table 8. Whether Real Name is Used and Information Indicated on Profile by Gender

	Percentage Indicating Information on Profile																								
	Uses Real Name Facebook		Uses Real Name Myspace		Favorite Music*		Favorite Book*		Favorite Movie		Political View		Romantic Status		Sexual Orientation [†]		Religion***		Phone Number***		Classes		Address		
	%	n	%	n	%	n	%	n	%	n	%	n	%	n	%	n	%	n	%	n	%	n	%	n	
Total	94.9	498	62.3	197	80.3	411	66.2	339	77.7	397	46.3	236	75.6	387	72.2	249	44.7	229	21.3	109	47.1	241	12.5	64	
Gender																									
Female	95.3	286	59.0	102	83.3	235	69.9	197	79.9	222	47.7	134	77.7	219	71.7	137	50.4	142	13.1	37	49.3	139	10.6	30	
Male	94.2	212	66.4	95	76.5	76	61.7	142	76.1	175	44.5	102	73.0	168	72.7	112	37.7	87	31.3	72	44.3	102	14.8	64	
N	525		316		512		512		511		510		512		345		512		512		512		512		512

Statistically significant difference between the genders (statistical test is phi).

†.05 < *p* < .10; **p* < .05; ***p* < .01; ****p* < .001.

Table 9. Whether Real Name Is Used and Information Indicated on Profile by Race

Race	Percentage Indicating Information on Profile																							
	Real Name Facebook	Real Name Myspace**	Real Name	Favorite Music	Favorite Book**	Favorite Movie	Political View	Romantic Status***	Sexual Orientation†	Religion*	Phone Number	Classes	Address	%	n	%								
Anglo-American	94.6	212	68.2	101	84.0	178	69.3	147	78.7	166	49.3	104	84.0	178	74.6	100	38.2	81	24.5	52	24.5	52	13.2	28
African American	95.6	65	42.5	17	79.4	50	69.8	44	84.1	53	45.2	28	68.3	43	76.7	33	54.0	34	17.5	11	17.5	11	12.7	8
Asian American	95.3	161	56.5	52	74.6	126	55.0	93	74.0	125	40.2	68	66.3	112	65.0	80	47.9	81	20.7	35	20.7	35	9.5	16
N	461	280		280	444	444	444	444	443	444	442	442	444	444	300	444	444	444	444	444	444	444	444	444

Note: Statistically significant difference between the genders (statistical test is χ^2).
 †.05 < p < .10; *p < .05; **p < .01; ***p < .001.

Table 10. Logistic Regression Results: Odds (e^{β}) of Using Real Name on Profile and Having Indicated Particular Fields on Profile, Modeled With General Privacy Concerns, Concerns About Profile Being Found by Unwanted People, Gender, Race, and Age Information Indicated on Profile

	Real Name Facebook	Real Name Myspace	Favorite Music	Favorite Book	Favorite Movie	Political View	Romantic Status	Sexual Orientation	Religion	Phone Number	Classes	Address
General privacy	1.430	1.041	1.013	0.931	1.064	0.958	0.994	1.180	0.920	0.702***	0.926	1.044
Unwanted profile gaze	0.831	0.714**	1.053	0.994	1.078	1.006	1.025	0.853	1.226*	0.858	1.075	1.108
Male	0.759	1.142	0.695	0.695	0.895	0.995	0.776	1.097	0.766	3.200***	0.849	1.660*
White	0.920	1.459	1.616*	1.491*	1.204	1.373	2.325***	1.105	0.670*	1.324	1.310	1.032
Age	0.838	0.914	0.922	0.973	0.908	0.860*	0.812***	0.771***	0.949	0.829*	0.831**	0.932
Baseline odds (constant)	496.4*	18.877	22.962	3.982	25.187*	15.227	155.04***	164.69***	6.581	6.624	30.115*	0.286
<i>N</i>	490	288	475	475	475	474	475	328	475	475	475	475

† .05 < p < .10; * p < .05; ** p < .01; *** p < .001.

Table 11. Gender Differences in Mean Levels of Perceived Likelihood of Being Found by Future Audiences

	Total	Male	Female	<i>t</i> Test Statistics		
				<i>t</i>	<i>df</i>	<i>p</i>
Employer	2.90	2.90	3.10	-0.018	232	.986
Romantic partner	3.62	3.48	3.73	-1.404	232	.162
Government**	2.63	2.91	2.41	3.007	232	.003
Corporation*	2.55	2.76	2.39	2.264	232	.024

Note: Response options were: 1 = *never thought about it*, 2 = *not likely at all*, 3 = *a little likely*, 4 = *somewhat likely*, and 5 = *very likely*. * $p < .05$, two-tailed. ** $p < .01$, two-tailed. *** $p < .001$, two-tailed.

Concern over persistence and searchability. Finally, to measure the specific awareness of threats because of persistence of information in a digital setting, we asked a subset of the students (the third wave of data collection) how likely they thought it was that a future employer, a future romantic partner, a government agency, or a corporation would look at their social network site profile. Results showing totals and the differences between the genders are shown in Table 11. Students ascribed a higher likelihood that their future mates would look at their profiles than that a future employer, government, or corporation would (repeated measures ANOVA, $df = 3$, $F = 68.739$, $p = .000$). Also, men were more likely than women to think about the government or a corporation looking at their profile at some point in the future.

To assess the significance of perceived likelihood of specific future audiences on disclosure, we ran 12 logistic regressions with dependent variables of disclosure levels and profile visibility on Facebook and Myspace. Perceived likelihoods of different future audiences (employer, romantic partner, government, and corporations) were predictor variables.⁸ Gender, race, and age remained our standard controls. The results are shown in Table 12. Also shown in Table 13 are two other logistic regressions, measuring the association between using real name on Facebook or Myspace and the perceived likelihood of these future audiences.

In line with previous analyses, demographic variables, rather than the concerns about future audiences queried in this survey, seemed to have more of an effect on participants' behavior on these Web sites. The perceived likelihood of future romantic partners looking at the profile seemed to be associated with the greatest differences in disclosure behavior. Students who perceived this as likely were more likely to indicate their favorite music but not their favorite book, possibly indicating the central role music plays in signaling identity within youth culture. They were also more likely to indicate their classes and marginally more likely to

indicate their romantic status (single or not). On the other hand, students who believed that the government might be looking at their profiles were less likely to provide their phone numbers or their classes, while those who thought corporations were likely to look at their profiles were *more* likely to indicate their classes—perhaps signaling their educational experience. Interestingly, the category of employers, though reported in the news as looking at social network site profiles for hiring decisions, had no statistically significant relationship with any type of disclosure. None of the four audiences we queried, government, employer, mate, or corporation, were associated with using a real name on either Facebook or Myspace.

Discussion

This study expands on the results of previous studies by looking at specific audience concerns as well as general privacy worries (Acquisti & Gross, 2006) and also by looking at specific disclosure and audience management techniques. We found that students who were worried about privacy were less likely to start using social network sites. Once the students did make the jump, they managed their concerns about unwanted audiences by adjusting their usage of nicknames on Myspace and through adjusting the visibility of their profiles on Facebook and Myspace but not by regulating their levels of disclosure, except for the case of phone numbers. We also found that the perceived likelihood that future employers, government, corporations, or romantic partners would see their profile did not have an impact on the visibility of their profiles. The students also did not find any of those scenarios very likely, except for future romantic partners. (A possible romantic partner looking at the profile, rather than being a cause for concern, may actually be an *aim* for many of the students.)

As in previous research, we found that general privacy concerns were not of much relevance to students'

Table 12. Logistic Regression Results: Odds (e^b) of Having Made Profile Visible to Everyone Modeled With Gender, Race, Age, and Perceived Likelihood of Employers, Romantic Partners, Government, and Corporations Viewing the Profile

	Profile Visible to Everyone On Facebook	Profile Visible to Everyone on Myspace	Favorite Music	Favorite Book	Favorite Movie	Political View	Romantic Status	Sexual Orientation	Religion	Phone Number	Classes	Address
Male	2.625**	20.166***	0.417*	0.534*	0.555 [†]	0.831	0.601	1.413	0.482*	2.510*	0.815	3.155**
White	0.768	2.887*	1.657	1.803 [†]	1.492	1.101	1.738	1.074	0.448**	1.239	1.032	1.051
Age	1.079	1.572*	1.031	1.004	0.999	0.921	0.815 [†]	0.728**	0.910	0.994	0.880	1.070
Employer	1.257	0.878	0.728	0.931	0.820	1.178	1.148	1.065	0.856	1.492	1.136	1.257
Romantic partner	0.993	1.438	1.493**	1.230	1.214	1.098	1.298 [†]	1.136	1.193	0.947	1.330*	0.979
Government	0.904	0.583	1.112	0.875	0.955	1.008	0.768	0.787	1.206	0.607*	0.635*	1.115
Corporation	1.032	1.880	0.994	1.124	1.340	1.002	1.149	1.192	0.956	1.274	1.631*	0.712
Baseline odds (constant)	0.086	0.000**	1.057	1.027	1.583	1.714	57.830 [†]	704.82**	6.722	0.091	2.569	0.020
N	162	108	195	195	194	195	195	195	195	195	195	195

[†] .05 < p < .10; * p < .05; ** p < .01; *** p < .001.

Table 13. Logistic Regression Results: Odds (e^b) of Using a Real Name on Facebook or Myspace Modeled With Gender, Race, Age, and Perceived Likelihood of Employers, Romantic Partners, Government, and Corporations Viewing the Profile

	Uses Real Name on Facebook	Uses Real Name on Myspace
Male	1.521	1.175
White	0.536	1.258
Age	0.918	0.953
Employer	1.681	1.002
Romantic partner	0.961	0.861
Government	1.421	1.149
Corporation	12.522	1.035
Baseline odds (constant)	1.521	2.683
<i>N</i>	173	104

decisions regarding disclosure. However, starting from a conceptualization of privacy as a boundary negotiation process and “selective access to the self,” we tried to move beyond the dichotomy between “students say they are worried but they don’t care” and “students say they are worried but they don’t know” and offer another possibility: Students *do* try to manage the boundary between publicity and privacy, but they do not do this by total withdrawal because they would then forfeit a chance for publicity. Students attempt to optimize their privacy and restrict who can find them by using monikers that they can share with only those they want to be found by or by restricting the visibility of their profiles to only “friends.”

This is not to suggest that students have taken into account every possible threat or that the current optimization level chosen by students is not without serious unconsidered risks. What we want to emphasize is the complexity of audience management and boundary negotiation in online social environments. It seems that students are better at managing certain boundaries than are others: We found that students are more adept at managing those boundaries that are analogous to “spatial” boundaries in that they try to restrict the visibility of their profile to desired audiences but are less aware of, concerned about, or willing to act on possible “temporal” boundary intrusions posed by future audiences because of persistence of data. This may reflect a tendency among the youth to live in the moment. It may also be a consequence of transporting familiar modes of boundary regulation in physical space onto the Internet without fully internalizing the different fundamental characteristics of the medium, such as persistence and searchability.

Interviews in conjunction with this study suggest that students see a certain level of self-presentation and self-disclosure as a minimum—why have a profile if your profile will not say *enough* about who you are? As other researchers have also noted, profiles have become a means of identity presentation (boyd & Heer, 2006). Just as one could not, in physical space, engage in identity expression without the time and attention devoted to the work that inevitably accompanies the presentation of the self (Goffman, 1959), one cannot present an online persona without manifesting a certain level of self-definition. As the spectacularly high adoption rates of social network sites show, being totally “unlisted” is not a very attractive option for college students.

In understanding the level of “minimum disclosure,” we should consider that online environments have cultural norms (which are different from each other) and certain *expectations* about levels of participation. In interviews, many students expressed explicit awareness of these “norms” of self-expression, including type and amount of information, and also asserted that these norms differ between Facebook and Myspace.

The almost universal prevalence of real name use in Facebook (but not in Myspace) is an example of this. Interviews confirm that students generally do not act as if using a real name is a choice in Facebook. The setup of Facebook makes it appear as if it may be obligatory to use a real name, although there is no such obligation in reality, and a small percentage do not use real names. Having originated as a college site, Facebook acts as a much extended phonebook or directory and plays an important role as college students arrive on campus and start forging new relationships. It is an ideal environment for those motivated by desire for publicity: If “being found” is a primary motivation, then not using a real name does not make sense. This cultural norm of name disclosure is also partly because of the perception of Facebook as a “walled garden,” clustered in “networks” where, by default, one’s profile is not visible outside the network. Of course, the network itself is very large (a large university can have tens of thousands of Facebook users within the network) and quite permeable. (Since the data collection period, Facebook has opened itself to non-college populations, and the situation may drastically change as students face the decision whether to “friend” their mom.)

While students do adopt prevailing norms, they also try to deal with possible fallout. We found that students were more likely to restrict their profiles to only their friends on Facebook, compared to Myspace, where the

use of the nickname might allow them greater invisibility through being unsearchable. In this instance too, students took action on their *current concerns*: The more concerned they were about unwanted audiences in general, the more likely they were to take steps to wall off their profiles. It is interesting to contrast the effect of real concern over unspecified undesirable audiences with the lack of concern about government, corporate, or employer surveillance. It may be that the actual audience of concern for students is peers they would like to avoid and direct authority figures, parents, coaches, and professors *in the present*.

We should also consider that one motivation for creating a profile and disclosing a certain amount of information could be interpreted as similar to a situation proposed by Palen and Dourish (2003), in which “one of the roles of disclosure can ironically be to limit, rather than increase, accessibility” (p. 131). Palen and Dourish note that academics often put their papers and research online to decrease the number of requests they must personally answer. Indeed, if your profile makes it clear that you are in a relationship or that you are politically conservative or that religion is very important to you or that you cannot stand (or you live for) hip hop, this can be considered fair warning to people who may not be compatible with you. In fact, researchers have argued that, in contrast to the idea that the Internet makes for superficial relationships, attraction and friendship formation founded on similarity might be easier via online social environments, where much self-presentation can take place before other steps are taken (Walther, 1996).

So, why do students not increase their privacy settings further? Altman’s framework of privacy optimization suggests that the need to be seen is greater than the fears students have about privacy intrusions. Previous research has shown that students are generally aware of the visibility of their profiles, so it is not unreasonable to suppose that they are making a choice about publicity based on their *current* concerns and may be shortsighted about *future* problems.

There was evidence of gender and racial differences in self-disclosure, and these should be explored further. In a forthcoming article, we find that women are more likely to want to use these sites to keep in touch with existing friends, while men are more often attempting to meet new people (Tufekci, 2007b). It is also interesting to note the decrease in levels of disclosure of political views, romantic status, sexual orientation, phone number, and classes with age. It seems that the younger students are more political, more comfortable with sexual orientation, more motivated for publicity, and more willing to give up their privacy.

Limitations

The data are from a purposive sample, and that limits the generalizability of the results. The data are cross-sectional in nature, so we cannot make causal assertions. Research on this subject is prone to being dated—social network sites rise and fall in popularity quite quickly. We expect that the rash of media reports about the purported dangers of social network sites, and a few highly publicized cases of negative consequences stemming from profiles, will affect students’ behavior on these sites. Also, toward the end of the data collection period, Facebook made a decision to allow general audiences to create profiles on the site. While this does not change college as the default network structure of the site, it does damage the perception that it is a walled garden and may affect student behavior.

Further Research

This study raises many questions. We saw that the likelihood of future exposure of the profile did not affect students’ current choices. Our data do not answer whether this is because students are unconcerned about such events. The one concern with the most effect, unwanted audiences, is a rather general category, and future research could look at that in more detail. Who exactly are the people who students hope do not see their profiles? It will also be interesting to see the impact of relentless media coverage about the threats posed by social network sites.

Conclusion

David Brin (1998) has argued that increased levels of exposure for everyone will bring about a “transparent society” in which we will recognize that many previously stigmatized behaviors are common or not a big deal. For example, the prevalence of profiles that indicate same-sex attraction may help further remove the stigma around minority sexual orientation. On the other hand, there has been a rash of negative consequences stemming from these sites, ranging from a beauty queen being blackmailed because of raunchy pictures on Facebook to a college graduate being denied a teaching certificate because of being pictured with a drink (even though she was not underage at the time) on Myspace. Much of the attention in this context has focused on examples like these: underage drinking or pictures that are considered risqué. However, some of the information such as favorite books, political views, or favorite quotes may have implications that have not been encountered because these sites are so new that their users are neither vying

for public service nor rising through the corporate ranks.

As this article was being written, Hillary Rodham Clinton's letters to a friend written when she was 19 were published in the *New York Times*. Thirty years from now, we might be able to go back and sift through every move made by every political candidate in young adulthood. Every book, every song, every quote, every friend, every comment on their profiles might become political fodder. We can also imagine that some of Brin's predictions might come to play. Already, youthful marijuana use has become a relatively unimportant issue in U.S. politics.

But there is an important point here: Most of the relatively embarrassing revelations about the youthful behavior of politicians came to light only through a massive effort by reporters *after* the person was already established as a national figure. That level of exposure, at earlier rungs in the civic ladder, might have a drastic constricting effect. Many people may be simply "filtered out" very early in their career, before they are important enough to embarrass specifically. Post hoc revelations by investigative reporters certainly do harm to some political and civic leaders, but *contemporaneous* filtering at low levels made possible by these sites may dramatically shrink the pipeline or drastically alter the characteristics of those who make it through.

Firms may refrain from hiring students whose book preferences are outside a band of acceptability. Will a boss assume that a job applicant whose favorite books are *1984* and *Brave New World* is rebellious and not worth the risk of hiring? Will a parent's political preference field in his or her college profile be brought up in school board elections? Will this mean that only those whose expressed preferences are acceptably bland can rise through corporate or civic ranks?

Another important consequence has been an explosion in what I call "grassroots surveillance" or peer monitoring, which has undergone a profound change because of these sites. Young people (and older people for that matter) have always been interested in what each other are doing, wearing, reading, listening to, fighting with, dating, and so on. However, much of that information is now available with the click of a mouse, in a searchable, archived, prominent format. In a forthcoming article, we document the prevalence of quite dramatic consequences for friendships and relationships. Students now find themselves in an environment in which the norm is to publicly articulate one's social networks and some of the interactions therein (Tufekci, 2007a). Such norms of disclosure are having an effect that is the opposite of some of the early predictions

about the impact of the Internet: Instead of being able to experiment with multiple identities, young people often find themselves having to present a constrained, unitary identity to multiple audiences, audiences that might have been separate in the past. As we leave behind the 20th century, it is almost as if we have come full circle back to the village where everyone potentially knows your business.

In the light of all this, it is important to recognize that simply wishing for (or ordering) students to refrain from having profiles, or from putting information in their profiles, is not going to work. Students are seeking to be seen. They are not wading in these waters without any reflection, but they may also not have fully adjusted to the implications of self-presentation in online environments.

The problems engendered by the affordances of information technology are here with us to stay, and there are no simple solutions. Our conversation about this issue should include an understanding of the process of privacy optimization sought by students and a dialogue about how we, as a society, wish to draw the boundaries between public and private, disclosure and withdrawal, and past choices and future possibilities.

Notes

1. This famous expression was formulated by Judge Brandeis in his dissent in the Supreme Court case *Olmstead v. U.S.* (1928). Much popular discourse on privacy is based on legal considerations, framed in terms of rights and violations, and this article is an explicit attempt to place privacy instead within the context of social interaction and boundary regulation.

2. Please note that danah boyd has legally changed her name to lowercase and asks that she be cited that way.

3. Although at the time of this writing there was a rumor that this might change soon.

4. We added questions in the third data collection round to probe specific issues that had been raised by students during the first two waves of data collection.

5. Over the data collection waves, there was a small but statistically significant decrease in the number of students using their real name and students with profiles visible to everyone in Myspace. There was also a small, statistically insignificant, increase in the number of students who used their real name and made their profiles visible to everyone in Facebook. Data on whether or not they restricted their profiles solely to their friends on Facebook and Myspace come only from the second and third data collection rounds because of wording differences with the first round.

6. In a logistic regression, the coefficient reported is the odds ratio, which indicates the relative amount the odds of an outcome, the dependent variable, increase or decrease when the value of the independent variable is increased, controlling for all the other independent variables. In our case, the dependent variable is whether or not a profile is visible to everyone. The odds of a man making his profile visible to everyone on Myspace are two and a

half times greater—2.504 to be exact—than those of a woman, controlling for all the other independent variables such as privacy concerns, race, and age.

7. This may not be true for other sociodemographic groups, especially teenagers, who are using online social network sites more to “hang out” with their close friends (boyd, 2007) and may not necessarily be thinking of (or caring as much about) their profile being seen and understood by others.

8. We did not include the variable about unwanted profile gaze, as we were exploring specific kinds of unwanted future perusing of profile and did not want that variable to cancel out the effects of specific concerns. In either case, there were no differences in the statistical significance of the results if general privacy and specific audience concerns were included.

References

- Acquisti, A., & Gross, R. (2006, June). *Imagined communities: Awareness, information sharing, and privacy on the Facebook*. Paper presented at the 6th Workshop on Privacy Enhancing Technologies, Cambridge, UK.
- Agre, P., & Rotenberg, M. (1997). *Technology and privacy: The new landscape*. Cambridge, MA: MIT Press.
- Altman, I. (1975). *The environment and social behavior*. Monterey, CA: Brooks/Cole.
- Altman, I. (1977). Privacy regulation: Culturally universal or culturally specific. *Journal of Social Issues*, 33(3), 66-84.
- boyd, d. (2006). Friends, Friendsters, and MySpace top 8: Writing community into being on social network sites. *First Monday*, 11(12).
- boyd, d. (2007). Social network sites: Public, private, or what. *Knowledge Tree*, 13.
- boyd, d., & Heer, J. (2006, January). *Profiles as conversation: Networked identity performance on Friendster*. Paper presented at the proceedings of the Hawaii International Conference on System Sciences, Persistent Conversation Track, Kauai, HI.
- Brin, D. (1998). *The transparent society*. New York: Addison-Wesley.
- Ellison, N. B., Steinfield, C., & Lampe, C. (2007). The benefits of Facebook “friends”: Social capital and college students’ use of online social network sites. *Journal of Computer-Mediated Communication*, 12(4).
- Goffman, E. (1959). *The presentation of self in everyday life*. Garden City, NY: Doubleday Anchor.
- Gross, R., Acquisti, A., & Heinz, H. J., III. (2005, November). *Information revelation and privacy in online social networks*. Paper presented at the proceedings of the ACM Workshop on Privacy in the Electronic Society, Alexandria, VA.
- Grudin, J. (2001). Desituating action: Digital representation of context. *Human-Computer Interaction*, 16(2, 3, & 4), 269-286.
- Kraut, R., Mukhopadhyay, T., Szczypula, J., Kiesler, S., & Scherlis, W. (1999). Communication and information: Alternative uses of the Internet in households. *Information Systems Research*, 10(4), 287-303.
- Lampe, C., Ellison, N., & Steinfield, C. (2006). A Face(book) in the crowd: Social searching vs. social browsing. In *Proceedings of the 2006 20th Anniversary Conference on Computer Supported Cooperative Work* (pp. 167-170). New York: ACM Press.
- Lampe, C., Ellison, N., & Steinfield, C. (2007). A familiar Face(book): Profile elements as signals in an online social network. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 435-444). New York: ACM Press.
- Olmstead v. U.S., 277 U.S. 438, 478 (1928).
- Palen, L., & Dourish, P. (2003). Unpacking “privacy” for a networked world. In *Proceedings of the ACM Conference on Human Factors in Computing Systems* (pp. 129-136). New York: Association for Computing Machinery.
- Petric, G. (2006). Conceptualizing and measuring the social uses of the Internet: The case of personal Web sites. *Information Society*, 22, 291-301.
- Solove, D. J. (2004). *The digital person: Technology and privacy in the information age*. New York: New York University Press.
- Stutzman, F. (2006). An evaluation of identity-sharing behavior in social network communities. *iDMA Journal*, 3(1).
- Tufekci, Z. (2007a). *Presentation of the self for everyday surveillance: On the Internet everybody knows you’re a dog*. Unpublished manuscript.
- Tufekci, Z. (2007b). *Social support and online social network sites: Women communicating, men searching?* Unpublished manuscript.
- Walther, J. (1996). Computer-mediated communication: Impersonal, interpersonal, and hyperpersonal interaction. *Communication Research*, 23(1), 3.
- Weiser, E. B. (2001). The functions of Internet use and their social and psychological consequences. *CyberPsychology & Behavior*, 4(6), 723-743.
- Whitaker, R. (1999). *The end of privacy: How total surveillance is becoming a reality*. New York: New Press.

Zeynep Tufekci is a visiting assistant professor in the Department of Sociology and Anthropology at the University of Maryland, Baltimore County. Her research interests include social and cultural impacts of technology, gender, inequality, social networks, and privacy.