6

College students are increasingly sharing their lives online through social networking sites with little concern for who may be viewing their information. Understanding student use of social networking sites along with privacy rights online will help professionals in the development of appropriate online activity and policies.

Privacy and Social Networking Sites

Dianne M. Timm, Carolyn J. Duven

College students are relying on the Internet to make connections with other people every day (Lukianoff and Creeley, 2007; Verga, 2007; Hodge, 2006). As the Internet has developed and grown, so have the capabilities for interaction. Social networking sites are a part of college students' regular daily lives (Bugeja, 2006; Jones and Madden, 2002). With this new technology, questions about ethical use and the lines of what is private and what is not have become so blurry and misunderstood that students can find themselves involved in situations that are less than desirable.

Social networking sites are a group of Web sites that provide people with the opportunity to create an online profile and to share that profile with others (Barnes, 2006). There are sites to meet almost any topic of interest. The two most commonly used are MySpace, with over 80 million unique users, and Facebook, with over 60 million unique users, about half of whom are college students. MySpace and Facebook have a variety of options and applications that make them attractive to a broad audience. Because these are the most commonly used social networking sites, we focus our discussion on them.

Little empirical research has been related to technology and privacy issues, although numerous anecdotal and opinion articles explain social networking sites and the negative actions taken by individuals on these sites. Several articles address issues related to higher education, but few examine the issues related to privacy. The topic of social networking sites has gathered increasing amounts of attention from student affairs professionals. Indeed, many formal and informal conversations at national conferences as

well as personal interactions between colleagues have considered how best to deal with them. This chapter provides a beginner's guide to help professionals understand privacy rights related to the use of social networking sites and the ethical dilemmas related to their use in work in student affairs.

Understanding Privacy

Privacy is defined here as personal information that an individual deems important and unattainable by the general population (Richards, 2007; Hodge, 2006; Etzioni, 1997; Kaplin and Lee, 1997). Personal information includes a person's name, physical address, e-mail address, online user name, telephone number, social security number, and any other information with which that person could be identified (Blakely, 2007; Richards). Privacy also involves the individual's right to control the dissemination of personal information (Berman and Bruening, 2001). Having the autonomy to control the sharing of information and how it will be used and manipulated is paramount to an individual's right to privacy (Barnes, 2006). Berman and Bruening stated, "When we talk about privacy, we are often talking about personal autonomy as it relates to information about an individual" (p. 2).

When contemplating issues of privacy, there are two important considerations to keep in mind: the intent of the information shared and the expectation that it will remain private (Hodge, 2006). A person who willingly posts information on a social networking site for others to view cannot assume it is private because the intent is to share that information (Meredith, 2006). When an individual uses privacy settings to prevent most users from viewing his or her information, the user has an expectation that this information will remain private (Hodge, 2006). This differs from e-mail, where the sender intends the information to be sent to a specific individual, although this information too can be accessed by others. Lindsay (2007) warns students that anything they post online is public and cannot be assumed private.

Understanding privacy as it relates to social networking sites requires understanding how personal information may be shared and the intent of sharing it. Reszmierski and Ferencz (1997) spoke of privacy as an individual's right to control personal information. Much of the information posted in a profile is in fact personal information that the individual willingly posts to the site. Meredith (2006) stated that when an individual shares information on a social networking site, he or she is sharing that information with the rest of the world even if the intent was to share with only a select group of people. It appears that people become sensitive about their privacy when they feel that they are being exposed.

Individuals feel that it is within their rights under the First Amendment to post information on a social networking site (Hodge, 2006). The First Amendment does protect an individual's right to speak, write, and gather freely so far as it does not cause harm or incite violence (Verga, 2007). An interesting dichotomy exists when students believe what they have written

is private and protected when in reality it is neither (Hodge, 2006). An example is a student who posts negative comments about a faculty member, including threats of a violent nature, on his or her social networking site profile accessible to other members of the institution. The student does have the right to post this information under the First Amendment; however, if the faculty member or others in the community are threatened, the speech is not protected. In this situation, privacy rights are not violated because the student chose to share information in an open public forum.

Another gray area in regard to information posted on social networking sites relates to how the information is accessed and used against an individual. For example, underage students post pictures of themselves consuming alcohol in a residence hall, which is used in a judicial hearing. Under the Fourth Amendment, individuals are protected from illegal search and seizure and guaranteed due process unless information is found in plain view (Lindsay, 2005).When information is posted online by an individual, such as pictures of underage drinking, it is no longer considered private (Barnes, 2006). Information obtained from a social networking site is not considered an illegal search of a person's private information because it is found in plain view in a public forum (Lane, 2006).

Many professionals may also question the impact of the Family Educational Rights and Privacy Act (FERPA) on the student's right to privacy related to social networking sites. FERPA was designed with respect to student records on campus (Kaplin and Lee, 1997). It was created to protect academic records, and the determining factor was that if the information could identify a specific student, it was considered an educational record and protected (Lindsay, 2007). Lindsay explained that this could include class schedules, financial aid records, e-mails, and electronic records but does not have to include directory information. Thus, FERPA has no control over social networking sites because they are not connected to the institution and are created and maintained by individual students.

Both Facebook and MySpace provide a clear privacy statement to inform users about the limits of protection that the site maintains for the information shared, as well as how the site will use the personal information provided. These privacy policies do not delineate who can access the information posted on the site but outline the actions that are taken by the site's administrators. The focus of these privacy statements is on what information will be shared with a third party but does not speak to who else may access the information posted. Little is known about whether individual users read and are aware of privacy settings. However, when Facebook created the news feed feature users were outraged that "friends" would be informed of their actions on the site. Facebook states that it will do everything possible to protect the information posted on the site but "cannot and do not guarantee that User Content you post on the Site will not be viewed by unauthorized persons" (Facebook, 2008). In addition to privacy policies that outline how Web sites will protect personal information provided to

the company, the sites also outline who is responsible for the information posted in a profile. Facebook (2008) states, "You may not want everyone in the world to have the information you share on Facebook; that is why we give you control of your information." Both MySpace and Facebook provide advice to parents and users about how to keep the information shared in the profile protected. MySpace cautions users, "Don't forget that your profile and MySpace forums are public spaces" (MySpace, 2008). Chris Hughes, cofounder of Facebook, stated in a personal conversation with us that Facebook has provided ways for students to continue to connect online and that it is up to the user to protect his or her own information by using the tools provided on the site (Hughes, 2007). The tools provided to social networking site users include a set of privacy controls that users can alter to prevent others from viewing all information shared in a profile. On most sites, the default or automatic setting allows the profile to be seen by the maximum number of people. On Facebook, the default setting for a profile is that all members of the person's network can view the entire profile. On MySpace, the default setting for a profile is that all users on MySpace can view a user's profile. On Facebook, if a user leaves the privacy setting at the default, his or her profile will be visible to less than 0.5 percent of the entire Facebook community (Wischnowsky, 2007). The privacy options that are available for users on other sites vary. On most sites, a user can restrict who can see the profile and is given options to create a limited profile that makes parts of his or her information unavailable to all friends. On Facebook, students can select who can search for their profile, which means they can restrict faculty and staff from viewing it. Although these options are available, many students do not use the privacy settings (Barnes, 2006).

Understanding Social Networking Sites

Social networking sites are set up to provide individuals with a means for communicating and interacting with one another. To join a site, individuals sign up as a member; this process may include providing personal information such as an e-mail address, permanent address, or a zip code. Users then create a sign-in name and password for their personal profile, a requirement that creates a false sense of security and the impression that their information is private, similar to entering a gated community (Hodge, 2006). It is easy to understand why students may be disillusioned about what is considered private.

A profile contains information that an individual chooses to share within the site. Most profiles provide users with the option to share home town, address, e-mail addresses, and phone numbers. There are also opportunities for users to post information regarding where they attend or attended school, where they are employed, personal interests, and more trivial information, such as favorite movies and music. College students share personal information about themselves, including their residence hall room

number, class schedule, and campus involvement (Lenhart and Madden, 2007). Many users share their gender and whether they are in a relationship. In an unpublished paper about online privacy, Jones and Soltren (2005), students at MIT, stated that students are not required to provide information in all sections, although many take the time to complete all portions of the profile.

The individual creating the profile determines the types of information shared in it. Although a profile may seem, on the surface, as a way to share real-world personal information, students may be using it to market their ideal identities (Rosen, 2007). Students may want to portray their ideal self as popular, athletic, and attractive. When individuals create blogs about their life and post pictures of themselves in provocative attire, consuming alcohol and partying, the lines between reality and fantasy may become blurred (Barnes, 2006).

The identity users post on the site is what they personally deem important. The Pew Internet and American Life Project that looked at teen online activity reported that over 50 percent of teens post some false information in their online profiles (Lenhart and Madden, 2007). Junco (2007) reported 10 percent of students lie about their age, 7 percent lie about their behaviors, 5 percent report lying about their picture, 3 percent lie about their gender, and 5 percent lie about their occupation. Mitrano (2006) noted that this technology "can also be a vehicle for traditional adolescent expression" (p. 20). While many students are using social networking sites as a way to connect, some may also be using these sites as a vehicle for personal expression—reality or fantasy.

Understanding the Ethical Implications

The numerous ways that students can use this technology to share pictures, ideas, and thoughts and, most important, connect with one another has been demonstrated throughout this chapter and in other chapters of this volume. As this technology has become more pervasive on college campuses, it has also brought to the forefront ethical issues that student affairs professionals are facing when interacting with students. This topic provokes numerous questions that need to be answered in order for student affairs professionals to understand the impact that this technology is having on student culture and professional practice. Professionals who have a thorough understanding of this technology and privacy rights are better equipped to face the ethical issues present and identify strategies for appropriate use.

As student affairs professionals are gaining insight into how students use social networking sites, the national professional organizations can play a key role in establishing ethical standards that help define the behaviors and actions of professionals working in higher education. In order to better understand this topic, we reviewed the ethical standards of several professional organizations: American College Personnel Association (ACPA,

2007), National Association of Student Personnel Administrators (NASPA, 1990, 2007), Association of Student Judicial Affairs (ASJA, 2007), Association of College and University Housing Officers–International (ACUHO-I, 2007), and National Orientation Directors Association (NODA, 2007). ASJA states that ethical standards are established "to maintain and strengthen the ethical climate and to promote the academic integrity of our institutions." ACPA shares that its statement of ethical principles and standards is designed to "assist student affairs professionals in regulating their own behavior by sensitizing them to potential ethical problems and by providing standards useful in daily practice."

At the time this chapter was being developed, only NODA, ACUHO-I, and ACPA had established standards that specifically address technology. NODA states that technology should be used appropriately and as a tool for furthering the student experience. ACUHO-I states that each professional and institution be "committed to incorporating technology into the residential environment for the benefit of residents and staff and identify strategies to promote appropriate use of technological resources." ACPA states that professionals need to know their institution's guidelines for electronic submission of information. ACPA was the only organization that addressed the professional's ethical responsibility related to privacy rights, calling on professionals to be knowledgeable about current laws and regulations and how student information and records are shared. They state that professionals should stay up-to-date about legislation related to the privacy rights of students, including online activity.

The ethical standards set by the various professional organizations present similar information and have common applications and online impact. Two common themes relate to the issue of privacy and social networking sites: the pursuit of knowledge and providing strong educational communities for students. Staying abreast of current issues, research, and student culture is a key to success in the field(ACPA,2007; ACUHO-I, 2007; ASJA, 2007; NASPA, 1990, 2007; NODA, 2007). Professionals have "an obligation to continue personal professional growth and to contribute to the development of the profession by enhancing personal knowledge and skills" (NASPA, 1990, 2007). In order for professionals to support student learning and education effectively and create intellectual communities for students, they need an understanding of the student culture and the means for communicating (ACPA, 2007; ACUHO-I, 2007; ASJA, 2007; NODA, 2007).

Professionals in student affairs are also called on to serve as role models and create relationships with students that promote learning and development (ACPA, NASPA, 1990). This must be done without confusing students about the role student affairs professionals play and by modeling ethical behavior (ACPA, NODA). Student affairs professionals using social networking sites can role-model how to set up an appropriate profile. In addition, professionals who are knowledgeable about and understand social

networking sites are less likely to use this technology inappropriately or set policies that infringe on student rights (Mitrano, 2006).

Most students have not experienced college without social networking sites. Computers have been accessible to most of them in the home since elementary school (Pierre-Louis, 2007). In 2005, Dare wrote about the top ten technologies that would affect student affairs practice and said that Facebook "is probably the most important item to really learn about on the list, from a student affairs perspective." Recently the Higher Education Research Institute (2007) added a new item in its "time diary" entry on the Cooperative Institutional Research Program (CIRP) survey that is given to entering college freshmen. On this survey, 94 percent of the respondents reported that they had used a social networking Web site at least one time during a typical week.

Examples of Ethical Dilemmas

Student behavior has not changed dramatically over the past twenty to thirty years. Students are still drinking, hanging out with friends, playing pranks, and experimenting with their identities in a variety of ways. What has changed is the way in which administrators are able to view this behavior (O'Toole, 2006). Administrators can view students' pictures and read about their adventures online. You might be thinking, "Why do students share so much of themselves online?" Mitrano (2006) stated, "It is the open display to a million potential eyes that is shocking and alarming to many adults" (p. 22). The challenge for professionals in higher education is in engaging in this technology without overstepping their authority. To understand the ethical dilemmas present, it is important to look at some recent examples of college administration and student use of social networking sites.

There are countless stories about residence life and judicial officials accusing students of underage drinking on campus because they have seen pictures of the students drinking in residence halls posted on social networking sites (Lane, 2006). The pictures were posted by the student, often "tagging," or identifying, all individuals in the photo and providing an explanation of what they were doing and where they were doing it. The students may even write in a blog about their adventures. On Facebook, if individuals have not used privacy settings, this information is available to anyone in the network, including student affairs professionals, faculty, and police at the institution who have Facebook accounts. Does this mean that administrators need to spend Monday mornings reviewing the weekend activities of their students to charge them with disciplinary violations? Hughes (2007) stated that it was unfortunate that professionals and the police are monitoring social networking sites and that students may use the privacy settings to prevent this from occurring. Do we share with students how we access such information? Do we tell them that we are on these sites and can peer into their lives like never before?

Officials at Pennsylvania State University used Facebook to identify students who broke through a police barricade after a football game against Ohio State University (Duboff, 2007). A Facebook group was created shortly after the football game, and the students posted tagged pictures of themselves behind the barricade. According to Duboff, the police used these pictures to identify, question, and fine the students who were involved. Students became upset that the police were looking at their Facebook pages, although the pages were available in plain sight (Hodge, 2006). In the past, these pictures would have been taken, and students would have shared them with friends and family and possibly even an administrator; however, the consequences would not have been as severe. What could student affairs professionals have done in this situation? How might this situation been different if students knew their photos would be viewed and that they would be held accountable? How would this have been different if students fully thought through the consequences of posting pictures like this?

Students believe that information they share on social networking sites is not going to be monitored by administrators; however, they are beginning to understand that there are administrators online. Consider an incident that occurred at George Washington University. Duboff (2007) explains that students at George Washington University believed campus police were monitoring their activity through Facebook, so they created a plan to advertise on the site that they were having a keg party. The police confronted what they assumed would be a large party and instead ended up walking in on a group of students eating cupcakes with the word *beer* written on them. To these students, the party was a way to justify what they already knew: administrators are on Facebook and monitoring what is happening. How might this scenario have been different if the institution stated up front that college officials were on social networking sites and monitoring them on a regular basis? Could professionals engage students in conversations about their online activities more openly if both parties are aware of each other's presence? What is the professionals' responsibility in educating students about posting appropriate information?

The most public situations have included student athletes and hazing at several institutions. Wolverton (2006) wrote about colleges that were facing investigations of alleged hazing incidents after Badjocks.com exposed pictures of inappropriate behavior by athletes. The photos were originally posted on Facebook and MySpace and then removed, but not before Badjocks.com and various student newspapers found the pictures and exposed the students' behavior. The institutions facing this public exposure found on Facebook and MySpace included Elon University, Northwestern University, Wake Forrest University, Catholic University of America, and Quinnipiac University (O'Toole, 2006). Some of the athletic departments responded by banning student athletes from having Facebook profiles (Read, 2006). Read stated that institutions banned the use to protect students from themselves, other students, and agents, but, most important, to protect the image

of the school and the athletic department. However, one must ask what right an institution has to set such limitations for its students and how this may infringe on the rights of the student (Lukianoff and Creeley, 2007). Could professionals at these institutions have better served students by setting clear guidelines for information posted and shared that they too were on these sites and would be looking at student profiles?

Read and Young (2006) claimed that prospective student athletes are looking at current athlete profiles before making a decision to be on the team. Admissions staff at Wake Forest University stated in the *Old Gold and Black*, Wake Forest's newspaper, that they review prospective students' profiles for further information about students and potential fit at the institution (Mirshak, 2007). More recently, residence life professionals have been faced with roommate change requests before students even set foot on campus because incoming students have reviewed their roommate's social networking site profile and arrive at the premature conclusion that they are incompatible. How should professionals talk about online information with students? Professionals must make decisions about whether the information gained through these sites is used to determine institution, team, and roommate compatibility.

This section poses many questions that can serve as conversation starters for professionals because the time has come to understand how this technology affects daily lives. As this technology evolves, professionals will continue to face many more questions than answers and will need to turn to their professional organizations and ethical standards for guidance.

Lukianoff and Creeley (2007) stated that "it is a bad idea to police humor, it is a terrible idea to enforce taste or politeness." In addition, administrators should not punish students for expressing themselves unless this expression would substantially disrupt school operations or interfere with the rights of others (Verga, 2007). Verga (2007) warns public K–12 institutions with policies regarding social networking sites to be aware that if the policies violate a person's constitutional rights, they may not have support in the courts. How this would be interpreted by institutions of higher education is yet to be determined.

Mitrano (2006) recommends that administrators learn all they can about social networking sites before they set policies, educate students, or determine expectations for student use. Administrators need to educate students on how their posted information could potentially be viewed or used (Mitrano, 2006). The guiding professional organizations state that professionals should continue to learn all they can in order to better serve the students with whom they work. Administrators who have avoided this technology need to understand it so they are prepared to help students navigate through these issues.

Social networking sites are public forums and not "a formal official extension of the campus environment" (Hodge, 2006). Lane (2006) explains that institutions have no control over the content posted on social networking sites and whether this information reflects positively or negatively on the institution. It is the responsibility of staff and faculty to

educate students; this should be extended to include social networking sites and online activities.

When students post information that shows them clearly violating a campus policy, the agents of the institution must decide whether to respond as an educator or disciplinarian or a combination of both.

Implications for the Profession

The marriage of privacy and social networking sites is complicated, and this chapter has touched on just some of the ethical issues related to the topic. There are issues related to how students interact with one another, how students are held accountable for behavior depicted on these sites, as well as the expectations for professionals who choose to use this technology (Lukianoff and Creeley, 2007; Verga, 2007; Mitrano, 2006). Most students use social networking site technology. In order for student affairs professionals to provide the highest level of support and service, they must understand the implications of this technology on institutions of higher education and their own practice. Understanding their limits as agents of the institution, applications of current policy, monitoring students' behavior, and interactions with students in regard to this technology will increase their ability to provide cutting-edge services and support to students regardless of personal interest in using this technology.

Student affairs professionals are using social networking site technology, and institutions need to set expectations for appropriate use (Berg, Berquam, and Christoph, 2007; Barnes, 2006; Read and Young, 2006). It is important for institutions to define when a professional is acting as an agent of the institution and when he or she is acting as an individual using a site. There are four things to consider related to identifying the role of an agent of the college and social networking sites:

• What an agent of the institution can examine
• When an agent of the institution formally reports information discovered on a site
• The type of information that needs to be formally reported
• What liability an agent of the institution assumes in knowing about but doing nothing with information discovered online

Setting clear parameters for when a professional is considered an agent of the institution will enable the professional to better use this technology and inform students about their use of this medium.

As a professional using this technology, it is also important to examine personal use of this medium. Why is this medium being used? When and how are the social networking sites accessed? By answering these questions, professionals will be able to better understand how they are using these technologies and will be better equipped to assist students in understand-

ing how student affairs professionals are using this technology. Professionals who have not examined their personal use and the ethical implications of that use will not be as able to educate students. Transparent use of this technology is important to ensure that students' rights are being respected.

At most institutions, current policies do not include standards of conduct specifically related to activity on social networking sites. Mitrano (2006) stated that campus policies are not going to change to allow prohibited behavior; the policies need to be examined to determine if they are applicable to these sites. Discussions about how evidence found on a social networking site profile will be used judicially is warranted. Members of the campus community need to understand how to react to a campus policy violation that may be visible on a site (Lane, 2006). To ensure that students' rights are respected, education related to current policies needs to occur to avoid hindering students' ability to express themselves online (Lukianoff and Creeley, 2007). In addition, the mission of the institution needs to be considered when performing the policy review (Mitrano, 2006). Social networking sites are going to continue to challenge how campus policies are enforced, and student behavior will continue to be monitored (Mitrano, 2006; Lane, 2006).

The examination of policies needs to be followed by conversations regarding how and when this technology will be used to monitor campus activity. Students have the right to know if their profiles are going to be monitored by agents of the institution. It is up to the professionals to serve as role models in using this technology and use it to enhance interactions and communications with students (Berg, Berquam, & Christoph, 2007). Professionals should consider what they post in their own profiles and identify how they will respond and react to student information posted on a profile or in a group.

The opportunities for teachable moments with students will be increased, not eliminated, by the use of this technology. What professionals once were left to assume about student behavior is now verified through picture and story. A professional who sees students engaged in presumably illegal or questionable activity can engage the students in conversations about their actions and decision making. The professional can use information posted to understand the culture and issues students face to provide programming and interventions that will better support students. Students will benefit from knowing that administrators can see what they are doing if professionals are honest about what is viewed and eliminate the feeling of big brother watching.

Professionals should also communicate standards of conduct on social networking sites for the students with whom they interact. It is an opportunity to educate these students in social and judicial contexts about appropriate use of this technology. It is important to talk with the students about what the use of this technology means in the student-to-professional relationship. Student affairs professionals need to outline clear expectations for supervisees about the uses of this technology. Advisers, judicial officers, and professionals with less formal discussions with students need to be clear about what their role is when they are looking at a student profile. Do

student affairs professionals need to put a disclaimer on their profile to state that they may have to act on inappropriate behavior in a photo posted? No, but they need to engage their students in the possible impact of the information shared and the connections created through a social networking site on their relationship.

Further research and conversation are needed on the topic of privacy related to social networking sites in addition to the ethical implications these sites have on student affairs professionals. As more legal issues come to the fore, it will be critical for professionals to stay abreast of precedents set. Graduate programs in student affairs and higher education need to identify ways to incorporate this topic into the curriculum because students have already been exposed to and are using the technology. Campuses are beginning to implement policies, so assessing the effectiveness of such policies would be beneficial. Most important, we need to understand students' perception of privacy as it relates to their online activity in order to provide them the best support and education. Finally, the national professional organizations need to engage in conversations about social networking site technology and develop ethical statements to guide practice.

Social networking online is the way students stay in touch with one another today, where just a decade ago, the emphasis was on person-to-person contact. Students now communicate with others using social networking sites and assume that student affairs professionals are familiar with these sites. It is the professionals' responsibility to understand the uses of this technology and the issues surrounding privacy as it relates to student rights. This can be done by learning about the rights and responsibilities of involvement on social networking sites and setting standards for behavior for professional staff. It is not the time to be skeptical about this type of technology or believe it is just a fad. Issues related to student privacy and vulnerability with social networking sites are growing concerns that need to be addressed by institutions as a whole. Recognizing the need for this discussion to happen is the first step in understanding the implications of this issue on our continued practice.

References

American College Personnel Association. "Statement of Ethical Principles," March 2006. Retrieved Oct. 24, 2007, from http://www.myacpa.org/ethics.

Association of College and University Housing Officers—International. "Ethical Principles and Standards for College and University Housing Professionals." June 2007. Retrieved Oct. 24, 2007, from http://www.acuho-i.org/Portals/0/pdf/2007_EB_Approved_Standards_Revisions.pdf.

Association for Student Judicial Affairs. "Ethical Principles." January 1993. Retrieved Oct. 24, 2007, from http://www.asjaonline.org/en/cms/?60.

Barnes, S. "A Privacy Paradox: Social Networking in the United States." *First Monday: Peer-Reviewed Journal on the Net,* Aug. 15, 2006. Retrieved July 10, 2007, from http://firstmonday.org/issues/issue11_9/barnes/index.html.

Berg, J., Berquam, L., and Christoph, K. "Social Networking Technologies: A 'Poke' for Campus Services." *EDUCAUSE Review,* Mar.–Apr. 2007, 32–44.

Berman, J., and Bruening, P. "Is Privacy Still Possible in the Twenty-First Century?" *Social Research,* 2001. Retrieved Aug. 8, 2007, from http://www.cdt.org/publications/privacystill.shtml.

Blakely, R. "Privacy Fears as Facebook Puts Users' Details on Search Engines." *Times Online,* Sept. 6, 2007. Retrieved Oct. 9, 2007, from http://technology.timesonline.co.uk/tol/news/tech_and_web/the-Web/article2395582.ece?

Bugeja, M. J. "Facing the Facebook." *Chronicle of Higher Education,* January 24, 2006.

Dare, L. "Ten Technologies to Watch and Learn." *Student Affairs Online,* Fall 2005. Retrieved Sept. 5, 2007, from http://studentaffairs.com/ejournal/Fall_2005/TenTechnologies.htm.

Duboff, J. "The Latest Crime-Busting Tool: Facebook.com." *Newsweek,* 2007. Retrieved Aug. 3, 2007, from http://www.msnbc.msn.com/id/12209620/site/ newsweek/print/1/displaymode/1098/.

Etzioni, A. *The Limits of Privacy*. New York: Basic Books. 1999.

Facebook. About Facebook, 2008. Retrieved February 10, 2008, from http://lhup.facebook.com/about.php.

Higher Education Research Institute. "How Many First-Year Students Are Using Social Networking Websites Such as Facebook and MySpace?" March 2008. Retrieved Oct. 28, 2008, from http://www.gseis.ucla.edu/heri/snippet.php?id=2.

Hodge, M. J. "Comment: The Fourth Amendment and Privacy Issues on the 'New' Internet. Facebook.com and Myspace.com." *Southern Illinois University Law School Journal,* 2006, *31,* 95–122.

Hughes, C. "Using the Internet for Political Purposes." Personal conversation, Oct. 18, 2007.

Jones, S., and Madden, M. "The Internet Goes to College: How Students Are Living in the Future with Today's Technology." Pew Internet and American Life Project. Washington, D.C. Sept. 15, 2002. Pew Research Center, Washington, D.C.

Jones, H., and Soltren, J. H. "Facebook: Threats to Privacy." Unpublished Paper. 2005.

Junco, R. "Connecting to the Net.Generation." Paper presented at Securing the eCampus 2.0: Building a Culture of Information Security in an Academic Institution Conference, Dartmouth Institute for Security Technology Studies, Hanover, N.H., 2007.

Kaplin, W. A., and Lee, B. A. *A Legal Guide for Student Affairs Professionals.* San Francisco: Jossey-Bass, 1997.

Lane, J. E. "Facebook and Freedom: Student Speech on the Internet." *ACPA Developments,* Winter 2006. Retrieved Sept. 10, 2007, from http://www.myacpa.org/pub/developments/archives/2006/Winter/article.php?content=legal.

Lenhart, A., and Madden, M. "Teens, Privacy, and Online Social Networks." Pew Internet and American Life Project. Washington, D.C., Apr. 18, 2007.Pew Research Center, Washington, D.C.

Lindsay III, C. L. *The College Student's Guide to the Law*. Lanham, Md.: Taylor Trade Publishing, 2005.

Lukianoff, G., and Creeley, W. "Facing Off over the Facebook: Who's Looking at You, Kid?" *Boston Phoenix,* Feb. 21, 2007. Retrieved Aug. 4, 2007, from http://www.thefire.org/index/php/article/7768.html.

Meredith, P. "Facebook and the Politics of Privacy." *Chronicle of Higher Education,* Sept. 14, 2006. Retrieved Mar. 23, 2007, from http://chronicle.com/.

Mirshak, M. "Facebook the Facts: The Public Is Watching." *Old Gold and Black,* Retrieved June 19, 2007, from U-Wire.

Mitrano, T. "A Wider World: Youth Privacy, and Social Networking Technologies." *EDUCAUSE Review,* Nov./Dec. 2006, pp. 16–28.

MySpace. About Us, 2008. Retrieved February 10, 2008, from http://www.myspace.com/index.cfm?fuseaction=misc.aboutus.

National Association of Student Personnel Administrators. "Standards for Professional Practice." December 1990. Retrieved Oct. 24, 2007, from http://www.naspa.org/about/ standards.cfm.

National Orientation Directors Association. "Statement of Professional Ethics." 2007. Retrieved Oct. 24, 2007, from http://www.nodaweb.org/about/ethics.html.

O'Toole, T. "Public Posting of Illicit Photos Revives Hazing Issue." *USA Today,* May 19, 2006. Retrieved Aug. 18, 2007, from http://usatoday. printthis.clickability.com/pt/cpt? action=cpt&title=USATODAY.com.

Pierre-Louis, E. "Beyond Social Networking." *PC Magazine,* July 17, 2007. Retrieved July 25, 2007, from www://web.lexis-nexis.com/universe/document?=c6378983bf821d 79fc76e24a1729ab13.

Read, B. "Forcing Athletes off Facebook." *Chronicle of Higher Education,* June 23, 2006. Retrieved July 14, 2007, from http://chronicle.com/.

Read, B., and Young, J. R. "Facebook and Other Social-Networking Sites Raise Questions for Administrators." *Chronicle of Higher Education,* August 4, 2006, 52(48), 37.

Reszmierski, V. E., and Ferencz, S. K. "Privacy and the Handling of Student Information in the Electronic Networked Environments of Colleges and Universities." *Cause White Paper.* CAUSE Association, Boulder, Colorado, 1997.

Richards, D. V. "Posting Personal Information on the Internet: A Case for Changing the Legal Regime Created by S 230 of the Communications Decency Act." *Texas Law Review,* 2007, *85,* 1321–1322.

Rosen, C. "What Are Facebook Friends for?" *Christian Science Monitor, 99,* no. 220: 9–9, October 10, 2007. Retrieved Oct. 12, 2007, from http://www.csmonitor.com/2007/ 1010/p09s01-coop.html.

Verga, J. "Policing Their Space: The First Amendment Parameters of School Discipline of Student Cyberspeech." *Santa Clara Computer and High Technology Law Journal,* 2007, *23,* 727–748.

Wischnowsky, D. "Online Social Site Defends Security: Facebook.com Used in Sex Scam, Cops Say." *Chicago Tribune,* Feb. 7, 2007.

Wolverton, B. "Hazing Photos Spur Debates on Complicity of Coaches." *Chronicle of Higher Education,* June 6, 2006, 52(39), pp. A1, A33–34.

DIANNE M. TIMM is the assistant dean of students and director of student life at Cornell College.

CAROLYN J. DUVEN is the assistant director of residence life at Cornell College in Mount Vernon, Iowa.