

Libraries at University of Nebraska-Lincoln
Library Philosophy and Practice (e-journal)

University of Nebraska - Lincoln

Year 2009

Online Social Networking Sites and
Privacy: Revisiting Ethical
Considerations for a New Generation of
Technology

Peter Fernandez
University of Tennessee - Knoxville, pfernand@utk.edu

Online Social Networking Sites and Privacy: Revisiting Ethical Considerations for a New Generation of Technology

Peter Fernandez

Agricultural Sciences & Natural Resources Librarian

University of Tennessee

Knoxville, Tennessee USA

Introduction

Before libraries can act ethically with regard to social networking sites, they must first have a nuanced understanding of the potential consequences of these sites. Social networking sites such as MySpace and Facebook are ultimately motivated by profit, a goal that can undermine user privacy, and that actively relies on the sharing of personal information. In contrast, most libraries in the US have an ethical commitment to patron privacy. Yet libraries are also committed to outreach and social networking sites provide a forum where libraries can create an online presence and spread awareness about their services. These diverse motivations provide a recipe for conflict that is too often ignored. Libraries may be able to appropriate the outreach opportunities of social networking sites while simultaneously maintaining ethical standards; however, responsible appropriation of technology requires that librarians reevaluate their commitment to privacy in the context of social networking sites that have a different conceptual understanding of privacy.

Such an evaluation falls beyond the scope of a single paper and ultimately must be assessed on an individual level, according to each librarian's unique circumstances which can vary depending on the type of library and its cultural context. This paper outlines a model for thinking about these two seemingly contradictory perspectives on privacy, in the context of librarians working in the US in public or academic libraries. Despite legitimate concerns about privacy, social networking sites are not entirely incompatible with the mission of most libraries. Yet neither are they neutral spaces where libraries can develop an online presence without regard for the consequences. This paper calls attention to the potential ethical conflicts between library and social networking sites, and provides a foundation for further debate on the subject.

The benefits of maintaining a presence on these websites is clear, because they allow libraries to reach out to patrons in the world of Web 2.0, a virtual world that many patrons already inhabit with ease. Unfortunately, both of the major social networking websites in the United States today, Facebook and MySpace, are motivated by profit. This can be a problem, because their profits are dependent on the free flow of personal information about their customers. In this context, a deep understanding of libraries' ethical stance is particularly important because social networking websites represent a moving target. Social networking sites can, and do, rapidly change their specific features and privacy policies. Librarians cannot exert direct control over the social networking sites they interact with, but they can prepare themselves for potential conflicts with a firm understanding of their own ethical priorities. Combined with up-to-date knowledge about the motivations and practical consequences of social networking sites, this will ensure that libraries are prepared to deal with the consequences of using these sites.

Libraries represent a trusted resource, and they should avoid lending their credibility to institutions that fail to uphold similar ethical values. This should not serve as an excuse for libraries to ignore this technology. For many libraries, the potential outreach benefits will outweigh the concerns outlined in this article. Nevertheless, it remains vital to understand the nature of this space in order to make the best decisions for a particular library.

Libraries' Role in Social Networking Sites

Time is rapidly running out for librarians to confront the privacy issues inherent to Web 2.0 websites. A recent Pew study found that more than 50 percent of teenagers in the US maintain a presence, typically called a "profile," on at least one social networking website (Lenhart & Madden, 2007). According to a senior analyst for Forrester Research one in four Americans has a MySpace profile (Owyang, 2008). Facebook estimates that it has over 100 million users and is the fourth most trafficked website in the world (Facebook Statistics, 2008). These sites allow users to create profiles that maintain a record of personal information submitted by the user. This profile can contain things like the user's favorite music, birthday, contact information, and favorite hangouts. This information is shared with other users to facilitate networking and to generate traffic for the site. Traffic represents people using the site, which is the key to making them attractive to their ultimate customer, advertisers. Whatever the values of the individuals running the site, this creates pressure to encourage users to share private information as freely as possible. This allows them to attract additional users, as well as to provide data for targeted advertisements.

These sites not only have the incentive to view privacy as a more nebulous concept than librarians might prefer, they also have the means to encourage their viewpoint. Because these sites are controlled by third parties, they represent a space whose owners create the parameters for what is possible. Even on MySpace, where users can use html to customize most profile features, including adding new graphics and videos, there are limits to how much control they can truly exert. For instance, users will find it almost impossible to effectively hide their age or gender. On Facebook, a user's choices are even more limited, and new "applications" are required in order to add features to a profile (Lenhart & Madden, 2007, p. 12).

In a sense, libraries are also beneficiaries of the popularity of these sites, or at least they aspire to be. While most libraries do not have the budget for advertisements, many are beginning to recognize the power of these websites and working to integrate social networking sites into their outreach efforts by creating profiles that allow them to interact with their patrons in this new space (See for example: Abram, 2008; Breeding, 2007; Chase, 2008; Farkas, 2007; Ishizuka, 2007; Mathews, 2007; Young, 2008). Some are even going further than creating simple profiles, and integrating services such as catalog searching directly into their social networking sites (Farkas, 2007). At the same time, if libraries do not simultaneously engage in a discussion about the consequences of these actions, they will not have time to examine the implications of their actions.

There is a relative dearth of academic literature on the specific privacy problems created by these websites (Chu & Meulemans, 2008). Given their rapid proliferation, it is unsurprising. Any detailed criticism of particular features would be out of date soon after its publication. As a result, information about social networking sites must be gleaned from more timely sources, such as newspapers and blogs. Even a casual perusal of this literature reveals that the social networking sites represented by MySpace and Facebook are not neutral spaces where anyone, including libraries, can simply add a webpage without consequence (See for example: Carter, Foulger, & Ewbank, 2008; Palmateer, 2007; Sanchez, 2008).

Nonetheless, a recent study suggests that only 19 percent of librarians surveyed expressed concern over privacy issues related to Facebook (Charingo & Barnett-Ellis, 2007). This is a problem, since a recent Pew study claims that 85 percent of adults "say it is 'very important' to control who has access to their personal information" (Madden, Fox, Smith, & Vitak, 2007, p. 2). While some argue that

teenagers appear to have an entirely different understanding of privacy, even the most generous estimates indicate that a significant minority of them still hold to a relatively traditional understanding of the value of privacy (Lenhart & Madden, 2007).

Despite the potential privacy concerns, libraries cannot afford to ignore this technology. Given their importance in the lives of our patrons, even librarians who choose not to participate in social networking sites should be aware of their basic features. Libraries that do not use Web 2.0 applications their patrons use risk creating unnecessary barriers that may cause their patrons to seek information from sources that do (Chad & Miller, 2005).

Libraries' Commitment to Privacy

The value of privacy and confidentiality is a foundation of librarianship that it is easy to take for granted. This has spawned best practices designed to help librarians maintain patron confidentiality. Works on these best practices often pre-suppose the existence of libraries' commitment to privacy and confidentiality.

Given the emergence of social networking sites, it is worthwhile to highlight the importance of privacy in librarianship. The American Library Association (ALA), has repeatedly emphasized the importance of privacy and confidentiality, by issuing statements such as the ALA Code of Ethics, which affirms these as general values for all librarians (American Library Association, 2008).

The notion of privacy specified in the Code of Ethics is narrow in scope. Slightly broader is the statement adopted by the ALA Privacy Council: An Interpretation of the Library Bill of Rights. In it, ALA affirmed that: "Protecting user privacy and confidentiality has long been an integral part of the mission of libraries. The ALA has affirmed a right to privacy since 1939" (ALA, 2006). Here, privacy, like democracy, is understood as integral to quality librarianship.

These documents make it clear that librarians as a profession consider privacy one of the core values of librarianship, but they fail to address how far-reaching librarians' concern for privacy should be. In part, this is because of the historical circumstances that shaped these documents. They are largely a product of a time when the most immediate threat to patron privacy was the possibility of outside agencies attempting to access the information libraries stored about their patrons. In part, this paper is an attempt to help librarians clarify the ethical grey area created by new technologies. For now at least, the question of how expansive the concern for privacy should be remains something to be determined by individual libraries and librarians. Their decisions in this area will affect how libraries interpret new information about the technology that they use to interface with their patrons. There is support by organizations like the ALA for an understanding of privacy that goes beyond the immediate concern of ensuring that patrons can access library resources without fear. The ALA Office for Intellectual Freedom is heading a new initiative, "Privacy for All: Rallying Americans to Defend Our Freedoms," which is designed to give librarians tools so that they can lead their communities in conversations about the importance of privacy (Caldwell-Stone, 2008). In doing so, ALA is recognizing that protecting patrons' privacy requires a broad conversation about a variety of issues including the very nature of privacy in an electronic age (Jokelley, 2008).

What Librarians Need to Know

What do librarians concerned about confidentiality need to know about this new world of social networking sites? While statistics rarely tell the whole story, they do reveal some interesting facts about these sites. Facebook's own data reveals that this is a world in which 25 percent of users cannot find the security settings provided by the website, leaving them at the mercy of the default settings (Vander Veer, 2008). Only 66 percent of teenage users report using their privacy settings to limit access to their profile in any way (Lenhart & Madden, 2007). Meanwhile, despite a growing awareness of the importance

of their “digital footprint,” the trail of personal information left behind by internet activity, only 3 percent of internet users monitor their online presence with any regularity (Madden, et al., 2007).

Studies of user behavior suggest that a significant minority are misinformed about how private their information truly is. Information that many users think is private can often be easily accessed by other users (Acquisti & Gross, 2006). To further complicate matters, there is a limit to how much control is helpful to consumers (Flatow, 2008). In fact, too many privacy options may lead to users making poorer choices about their privacy by confusing them (Flatow, 2008). For example, letting users define that only their self-designated “friends” can see blog posts can be helpful for ensuring privacy, but giving users multiple definitions of friends (ex: work friends, Tennessee friends, college friends) who all access the same profile, can actually lead to users to make more information about themselves available than if they were offered fewer, but easier-to-understand, choices (Flatow, 2008).

These factors combine to produce the “Illusion of Privacy” (Woodward, 2007, p. 61). The technology and culture of these sites are designed to encourage the disclosure of normally private information in a way that works against the spirit of informed consent. For example, the recent “Beacon” controversy caused many Facebook users to become outraged because Facebook began to broadcast users' recent purchases to their friends. This was perfectly legal because users had given Facebook permission to do this. But it was nonetheless incompatible with the implicit agreement users thought they had made (Story, 2007). Although Facebook reacted quickly and turned off the Beacon feature, it continues to look for ways to harness similar technology, without the public relations fallout (Lyons, 2008).

Evidence suggests that in many cases this is not simply the result of a casual disregard for privacy, but is the very nature of these websites. Social networking websites are predicated on the concept of social interaction, and many of their features exist solely to make their users' information more widely available. Unlike the “Beacon” feature described above, the newsfeed feature, although once controversial, is now largely accepted by users. It creates a “newsfeed” on each profile. This creates a constantly updated “feed” that broadcasts any activity within Facebook, such as adding a picture, or updated information about an upcoming party, and places that information on the main page of anyone designated as a “friend”. As of October 2008, this newsfeed is the first thing users see when logging into their account.

The economics of the situation dictate that the more information they can share without provoking user dissatisfaction, the better the companies do (Lyons, 2008). After all, it is the unprecedented ability to share personal information that attracts many users in the first place. The implicit threat is that users are lulled into a false sense of security by the websites who seek to profit from their information. Both MySpace and Facebook are based on an advertising model. In order to sell advertisements, the sites need users who are attracted by their content, and the primary content of these sites is the information that its users put into it. Despite having immense potential value, MySpace has a three-year, 900 million dollar contract with Google, and Facebook's stock has been valued at 15 billion dollars by Microsoft, although neither of these sites has yet managed to consistently turn a profit (Saporito, 2007; Stelter, 2008).

The lack of a profit only increases the pressure on social networking sites to find ways to monetize their users' information. Crucially, financial success is tied to their ability to bring in advertisers, who want people to advertise to, and ideally people who can be individually targeted by their interests. Similarly, what attracts new people to the site, and keeps the old people coming back, is the user-generated content. This usually takes the form of personal information (Chudnov, 2007). It is this personal information that enables the social networking sites to generate new viewers, and cause repeat viewings by old users, as well as to use that personal information to sell targeted advisements (Stelter, 2008).

Moreover, once their information has been entered into the website, the user loses direct control over it. It is notoriously difficult to have information permanently expunged from the servers of the websites, and impossible to be certain that nobody else will copy or distribute the information themselves

(Aspan, 2008). This latter point is particularly important, as websites such as the Internet Archive have proven that information released on the Internet can be stored and manipulated in ways the original users may not have intended (Kahle, 1997). Over time both MySpace and Facebook have worked to make it easier to remove personal information, but they have generally only done so after protests and problems (Cellan-Jones, 2008).

How this Concerns Libraries

All of these facts make for fascinating reading and exciting headlines to sell newspapers, but how do they affect libraries? After all, the library relationship is primarily a contract between the library and the user. Currently the confidentiality of library users remains completely intact, but the issue of privacy is less clear. If library patrons are increasingly unconcerned about sharing their information (Acquisti & Gross, 2006), as well as increasingly sophisticated in how they manage it (D. L., 2007; Lenhart & Madden, 2007; Madden, et al., 2007), then why should librarians worry about it?

Two facts stand out. One is the realization that social networking sites are not truly neutral spaces. They are controlled spaces whose owners have a vested interest in promoting certain activities over others. Often the interests of the user and the site correspond, but not always. Librarians must also understand that these sites are an inherently moving target. As with most things on the Internet, social networking sites are not static and can change rapidly. While it does not currently appear to be a problem, future updates to the sites could potentially track how people use library profiles; collect information about how their users access the library catalogue, or perhaps most worryingly, do something else entirely that librarians cannot anticipate.

An article on Wired.com brings this point home. This relatively brief article from June 2007 details how user's privacy is compromised by Facebook's search engine. On the day it was published, it had numerous updates and revisions as facts changed. The types of privacy concerns changed and mutated as the day went on. A similar article by the same author appeared on the ABC news website the next day, without any indication of the rapid changes in the situation. Viewing these articles side by side illustrates how deceptive a stable print article can be in this context, and how even recent newspaper articles can be out of day just days later (Singel, 2007a, 2007b).

More recently, both MySpace and Facebook have added features to make it easier for users to share their data on other websites, pushing their profile out into the rest of the Internet (Greenwood, 2008). In order for users to maintain control of their information, they must remain constantly informed about changes. Libraries with profiles on these pages will need to remain vigilant as these websites morph and take new shape. A social networking site that poses no confidentiality concerns one day can change its policies almost instantaneously within the limits of the law. These realities do not mean that libraries have an obligation to avoid social networking sites. But they are relevant when considering exactly how a library should implement and interact with these sites.

Conclusion

Facebook and MySpace are corporations beholden to their stockholders. Just as many libraries have entered into partnerships with corporations like Starbucks and Amazon that have been beneficial to both parties, fruitful relationships are possible within the context of social networking sites. These websites create spaces designed to encourage their users, in both subtle and not-so-subtle ways, to feed information into the system, often without regard for the best interest of the user (Jones & Soltren, 2005). If librarians do not grapple with these underlying issues beforehand, they will be forced to react to each new change as a unique crisis.

Once a user's information has been placed into the system, there is no way to retain full control over how it is used, regardless of the number of safety features the sites eventually add (Vander Veer,

2008; Woodward, 2007). Crucial to the very nature of Web 2.0 is the ability of others to manipulate the information on the sites. In this case it means that other users can feed information into the system about another user, and that information can be tied to the original user's account. For example, someone else can take an embarrassing picture of John Doe at a party, and upload that picture to their profile. That second user or one of their friends can "tag" John Doe's name to the picture, which will tie the picture not only to the original host's profile, but to John Doe's profile as well. As a result, users who are "friends" with John will see that picture on their main page as part of the "newsfeed" feature built into Facebook.

Depending on his security settings, strangers may be able to access this picture as well. All of this can occur without John's active consent if he, like many users, does not carefully control his privacy settings or constantly monitor his profile. Either constant vigilance or closed privacy settings would be required to restrict this kind of behavior, both of which would risk limiting the "fun" of the site. To stop this process, John would have to notice the picture, and contact Facebook to have the "tag" removed (Facebook Help, 2008). Getting the picture actually removed from the website is even more difficult (Lynch, 2008). Alternatively, he could hide his profile from all but his most trusted friends, effectively eliminating many of the social aspects of the social networking website.

While this particular example may change, the fundamental nature of social networking sites is unlikely to change. They are not simply neutral spaces for libraries to place outreach materials in, but websites controlled by companies who seek to maximize the amount of personal information contained in them (Jones & Soltren, 2005). If librarians are seriously concerned for the privacy of their users, it is imperative that we understand how social networking sites potentially threaten their privacy, not because any direct conflict currently exists, but because the spirit underlying each organization is so different that it can easily affect how libraries implement their service in this space. Libraries have a recent history of establishing fruitful partnerships with profit oriented businesses such as Starbucks, but ideally only after careful investigation into the details of how that relationship will work and after examining potential conflicts. Because the service provided by social networking sites is free, it does not make this investigation process any less important.

By creating a profile on these sites, libraries also risk further legitimizing them, and encouraging users to be passive regarding their own privacy. If libraries take a comprehensive view of privacy as a core value, encouraging their users to use products that do not have the same regard for privacy should give librarians pause. Furthermore, it raises the issue of the role that libraries should play in actively promoting awareness about the privacy issues inherent to these systems.

For many librarians the immense outreach potential of online social networking sites will ultimately outweigh the privacy concerns. Ignoring their dominance in the minds of our patrons is neither wise nor practical. Since the primary relationship exists between the librarian and the patron, the problem is not insurmountable as long as these sites do not interfere with the library's ability to maintain patron confidentiality. Few would argue that librarians should avoid maintaining prison libraries for instance, even though these spaces are heavily controlled and monitored. We cannot hide from these technologies, but neither should we automatically assume that such technologies are inherently beneficial or without consequence. It is vital that librarians stay informed about how these services affect the privacy of their patrons even as they move forward with innovative outreach programs. Patrons currently exist in the world of social networking sites, whether they are informed or not. By staying constantly alert we can make wise choices that both serve our patrons and maintain our ethical standards.

Works Cited

Abram, S. (2008). Did you hear that? *MultiMedia & Internet@Schools*, (Jan./Feb.): 26-28.
<http://www.mmischools.com/Articles/ReadArticle.aspx?ArticleID=13393>

Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. In Danezis, G., & Golle, P. (Eds.), *Privacy Enhancing Technologies* (4258/2006, pp. 36-58). Heidelberg: Springer Berlin.

American Library Association (2006). Privacy. Retrieved October 02, 2008, from <http://www.ala.org/ala/aboutala/offices/oif/statementspols/statementsif/interpretations/privacy.cfm>

American Library Association (2008, January 22, 2008). Code of Ethics of the American Library Association. From <http://www.ala.org/ala/aboutala/offices/oif/statementspols/codeofethics/codeethics.cfm>

Aspan, M. (2008). How sticky is membership on Facebook? Just try breaking free. (Business/Financial Desk). *The New York Times*, 157 (54217), C1(L).

Breeding, M. (2007). Librarians face online social networks. *Computers in Libraries*, 27 (8), 30-32.

Caldwell-Stone, D. (2008). Privacy, libraries, and ALA. *American Libraries*, 39 (8), 58-58.

Carter, H. L., Foulger, T. S., & Ewbank, A. D. (2008). Have you googled your teacher lately? Teachers' use of social networking sites; common sense doesn't necessarily prevail when teachers plunge into the world of social networking sites. disastrous consequences can ensue, and the authors urge educators to consider the potential outcomes before they post. *Phi Delta Kappan*, 89 (9), 681(685).

Cellan-Jones, R. (2008, Thursday, 24 January 2008). Social sites prove hard to leave behind. Retrieved October 01, 2008, from <http://news.bbc.co.uk/1/hi/technology/7206852.stm>

Chad, K., & Miller, P. (2005). Do libraries matter? The rise of library 2.0. *Talis White Paper*, November, from http://www.talis.com/applications/downloads/white_papers/DoLibrariesMatter.pdf

Charingo, L., & Barnett-Ellis, P. (2007). Checking out Facebook.com: The impact of a digital trend on academic libraries. *Information Technology and Libraries*, 26 (1), 23-34.

Chase, D. (2008). Using online social networks, podcasting, and a blog to enhance access to Stony Brook University Health Sciences Library resources and services. [Article]. *Journal of Electronic Resources in Medical Libraries* 5: 123-132.

Chu, M., & Meulemans, Y. (2008). The problems and potential of MySpace and Facebook usage in academic libraries. *Internet Reference Services Quarterly* 13 (1): 69.

Chudnov, D. (2007). Social software: You are an access point. *Computers in Libraries*. pp. 41-43.

D. L., W. (2007). Teens don't reveal personal info online. *School Library Journal* 53 (2): 18-18.

Facebook Help (2008). Help Center | Facebook. Retrieved October 17th, 2008, 2008, from <http://www.facebook.com/help.php?hq=remove+tag>

Facebook Statistics (2008). Statistics | Facebook. *Press Room*. Retrieved October 17th, 2008, from <http://www.facebook.com/press/info.php?statistics>

Farkas, M. (2007). Going where patrons are. *American Libraries* 38 (4): 27-27.

Flatow, I. (2008). Web privacy concerns prompt Facebook changes. On *Science Friday* [Radio Podcast]. New York: NPR ScienceFriday Inc.

Greenwood, B. (2008). MySpace, Facebook, Google integrate data portability. *Information Today* 25 (6): 27.

Ishizuka, K. (2007). Librarians on Facebook. *School Library Journal* 53 (10): 22.

Jokelley (2008). Office for Intellectual Freedom - Post details: ALA kicks off privacy initiative with program and survey. Retrieved October 20, 2008, from http://blogs.ala.org/oif.php?title=privacy_revolution_program_and_survey&more=1&c=1&tb=1&pb=1

Jones, H., & Soltren, J. H. (2005). Facebook: Threats to privacy. Retrieved October 1, 2008, from <http://www-swiss.ai.mit.edu/6.805/student-papers/fall05-papers/facebook.pdf>

Kahle, B. (1997). Preserving the Internet. *Scientific American* 276 (3): 82-83.

Lenhart, A., & Madden, M. (2007). Teens, privacy, and online social networks: How teens manage their online identities and personal information in the age of MySpace. *Reports: Family, Friends & Community*. Retrieved October 20, 2008, from http://www.pewinternet.org/pdfs/PIP_Teens_Privacy_SNS_Report_Final.pdf

Lynch, C. G. (2008). Facebook tip: Do damage control on unwanted photos. Retrieved October 22, 2008, from <http://www.itworld.com/internet/56363/facebook-tip-do-damage-control-unwanted-photos>

Lyons, D. (2008). Facebook's roar becomes a meow. (Enterprise; TECHTONIC SHIFTS). *Newsweek* 152 (16): E22.

Madden, M., Fox, S., Smith, A., & Vitak, J. (2007). Digital footprints: Online identity management and search in the age of transparency. *Reports: Internet Evolution*. Retrieved October 16, 2008, from http://www.pewinternet.org/pdfs/PIP_Digital_Footprints.pdf

Mathews, B. (Writer) (2007). Moving beyond the reference desk: Being where users need us [Article], *Reference Librarian* 48:9-13.

Owyang, J. (2008, January 9, 2008). Social network stats: Facebook, MySpace, Reunion. *Web Strategy by Jeremiah*. Retrieved 06-01, 2008, from <http://www.web-strategist.com/blog/2008/01/09/social-network-stats-facebook-myspace-reunion-jan-2008/>

Palmateer, J. (2007). Have risqué info or photos online? It could cost you. *The Daily Star* (Oneonta, NY) Retrieved October 16, 2008, from http://www.thedailystar.com/local/local_story_349040009.html

Sanchez, C. (2008, October 25, 2008). UNMH workers fired over photos: MySpace account showed injuries. *The America's Intelligence Wire*, p. NA, from http://find.galegroup.com/itx/infomark.do?&contentSet=IAC-Documents&type=retrieve&tabID=T004&prodId=GRGM&docId=A185425841&source=gale&srcprod=GRGM&userGroupName=tel_a_utl&version=1.0

Saporito, B. (2007). The 10 best / worst business deals.(TIME's Lists of the Year). *Time* 170 (26): 89.

Singel, R. (2007a). Facebook private profiles not as private as you think they are -- UPDATED with Facebook changes. Retrieved May 16 2008, from <http://blog.wired.com/27bstroke6/2007/06/facebook-privat.html>

Singel, R. (2007b, June 27, 2007). Private Facebook pages are not so private. Retrieved June 01, 2008, from <http://abcnews.go.com/Technology/Story?id=3325951&page=1>

Stelter, B. (2008). MySpace might have friends, but it wants ad money. (Business/Financial Desk). *The New York Times* 157 (54343), C4(L).

Story, L. (Writer) (2007). Apologetic, Facebook changes ad program [Article], *New York Times*.

Vander Veer, E. A. (2008). *Facebook: The missing manual*. Sebastopol, CA: Pogue Press/O'Reilly.

Woodward, J. A. (2007). *What every librarian should know about electronic privacy*. Westport, Conn.: Libraries Unlimited.

Young, J. R. (2008). Facebook lets users search library stacks. *Chronicle of Higher Education* 54 (19): A18-A18.