

Privacy and Online Social Networks: A Proposed Approach for Academic Librarians in University Libraries

Greg Hutton

Abstract: This paper analyzes the ways in which academic librarians in university settings can educate the staff, students, and public involved in the library community of both the risks and benefits of involvement in online social network sites such as Facebook. The concerns addressed range from maintaining users' basic privacy and protecting themselves from physical and mental harm, to making users aware of how the information being shared on these sites may be used in newly emerging marketing practices. The paper recommends that academic librarians utilize social networking sites themselves in order to provide current, relevant information to the relevant parties in the university library community.

About the Author: Greg Hutton is a first year MLIS student at Dalhousie University who grew up in rural southern Alberta. The research and writing process of this paper, which was originally written for the Master's level course INFO 5500 "Information In Society," allowed Greg to pursue his interest in how online social networking sites can be used beyond keeping in contact with friends and instead used as a professional tool. Greg's career ambitions to work as an Academic Librarian coincide with the decision to write the paper from the perspective of someone similarly employed.

Introduction

As online social networks such as Facebook gain popularity, it becomes increasingly important for information professionals to educate those utilizing these sites about its potential negative effects. It is arguable that the more popular these sites become, the less likely it is that users are going to consider the ramifications of their online actions; if the vast majority of a person's peer group is already participating in an online social network, there is an assumption that such involvement must be safe. This assumption needs to be called into question for a myriad of reasons, including basic privacy concerns, targeted marketing ploys, and use by employers as a screening tool. Conversely, there are a number of arguments for the use of sites such as Facebook as effective educational tools in schools and libraries, as well as for use as professional networking tools. Considering patron needs from the perspective of an academic librarian, an understanding of the potential impact on users of online social networks with regard to their lives and privacy must be established. After understanding how library patrons' information can potentially be accessed and used negatively, academic librarians can take steps to educate these users as to how possible risks can be minimized.

Potential Unconsidered Privacy Risks Inherent with Involvement in Online Social Networks

Privacy concerns need to exist at the helm of potential risk to any user participating in online social networking, including students and staff involved with university libraries. It is reasonable to state that a site's popularity, in creating a false sense of security, may hinder people from considering how the information they share could potentially be used in harmful ways. One of the most basic examples of this idea is with regard to personal safety and how much information a person would be willing to share publicly in locales that exist outside of computer-based environments. For example, it is extremely unlikely that someone would post a picture of him or herself on a telephone pole which also listed his or her interests, relationship status, list of friends, and contact information due to the fear of attracting unwanted attention. This is essentially the attention that users of online social networks are inviting if they do not protect their information from people not listed as friends. Shirley Atkinson (2007), while discussing possible harms involved in using online social networks, suggests that "a significant number of individuals experience mental or physical harm because of the abuse of personal information" (p. 383) which they make available online. There are indications that some users have experienced such situations directly because of their involvement in online social networks. For example, one study of university student Facebook usage found that "10% of students said they felt stalked because of constant messaging by an individual" (Stern & Taylor, 2007, p.15). Other articles report similar findings, with security at Virginia Commonwealth University receiving notices that Facebook was "being used to abet 'cyberstalking' — using the Web to harass people or dig up information on them" (Read, 2006).

Compared to real-world stalking or harassment, the aggressor in an online stalking situation has the benefit of increased anonymity which may make it more difficult for authorities to track down aggressors. The variety of forms of online harassment and the range of victims gives academic librarians an opportunity to educate a wide audience of internet users of the potential risks inherent in making personal information available to the public. In the case of a university library this education would extend to both students and staff and would need to stress that the same type of routine behaviours users undertake in the physical world to ensure their physical and mental security are exhibited in their online presence.

Expanding on the basic idea that students and staff using university libraries need to protect themselves from physical or mental harm as a result of their online activity is the fact that identity theft is also a threat to Internet users. This threat may be bolstered by online social networking sites which may readily provide identity thieves with exactly the type of information they require from users who share information of a sensitive nature such as address, birth date, and phone numbers, among others. Christine Sund (2007) argues that use of online social networking sites poses “increasing online security risks” since “a name, address and birth date (let alone a social security number) provides more than enough ammunition for criminals to hack into financial records and compromise a user’s personal information” (p. 568). This largely unrecognized or unconsidered danger illustrates the idea that the popularity of a service coupled with the relative newness and uncharted electronic territory of online social networking makes educating users pivotal. Sund goes on to cite a survey done by European SchoolNet which indicated “that 57 per cent of young people make their online social network profiles public and disclose personal information” (p. 569). Statistics quoted in another article claim that not only do 55 percent of “all online American youths ages 12 to 17 use online social networking sites with most listing either MySpace or Facebook,” but also that only “66 percent say that their profile is not visible to all internet users” (Topper, 2007, p. 378).

If these numbers are accurate, then a definite lack of basic knowledge about protecting information is lacking in younger populations – the remaining 33% of American youths are exiting high school without being made aware of the inherent risk of letting anyone access their information. The fact that not all of these younger people are learning these skills in high school means that university libraries need to step in and provide resources that deal with these privacy concerns. While it is difficult to blame online social networks exclusively for instances of identity theft, it is not difficult to surmise that the easier it is for an identity thief to access a person’s information, the easier stealing his or her identity becomes. It may seem like common sense, but because this is not necessarily a topic that is on the minds of students entering post-secondary settings, it would be beneficial to provide online safety guides for both staff and students which describe the potential harm implicit in using the web and online social networking in particular. Making new university students step back and consider how their

online behaviour with regard to sharing information may differ from their real-world interactions is an important first step in giving them the opportunity to protect themselves. And while there is no way to guarantee that identity theft will not occur even if users take precautions with sharing their information, instruction in protecting personal information would at the very least reduce identity thieves' access to potentially exploitable data.

Even though Facebook provides a thorough analysis of users' privacy settings, as well as a detailed synopsis of how these settings affect which parts (if any) of a user's profile that other visitors can see, [1] producing privacy guides within the context of a university library could clarify what this summary actually means to the user. In addition to alerting students and staff to the potential dangers of using online social networks, it would be feasible to create targeted privacy guides that make it explicitly clear what each aspect of the Facebook privacy settings means from a user perspective and to make a list of recommendations for how users can keep their information as safe as possible. Meredith Farkas (2007) writes in her book, *Social Software in Libraries*, that libraries "have an important role in educating patrons about the dangers of putting personal information online and the ways they can participate in online communities while protecting themselves" (p. 123). In order to effectively educate patrons while avoiding appearing preachy or paranoid, convincing arguments supporting privacy awareness would first need to be contextualized by explaining the real-world risk potential that exists. This goal could best be accomplished by providing relevant statistics and examples in order to instill how imperative it is to consider online privacy. From there, concise guides could be created for the online social networks used by library clients that describe how best they can protect themselves. Stressing that patrons consider option, such as limiting or completely denying access to their profiles to anyone not considered a "friend" and ensuring that they understand how posting addresses, phone numbers, and other sensitive information is inadvisable would be key components of these guides. Making these guides available on online social networking groups created by a university library would be one approach to reaching users, as would scheduling privacy training events and inviting users of online social networks to attend through the networks themselves. Approaches such as these would prove to be more effective than written guides to social networking, such as Meredith Farkas' book, since technology continually evolves. Ultimately, while the approaches taken by academic librarians in educating students and staff will vary, concentration must be placed on the underlying idea that users of online social networking sites in university libraries must be aware of how their privacy can be comprised through using these sites.

Understanding Newly Emerging Advertising Strategies

While being aware of the possible negative repercussions of posting personal information online for rudimentary self-protection purposes may be obvious for some library users, it is also

important to educate users about more insidious uses of information posted online. One example of a less obvious exploitation of personal information is targeted marketing. For example, a guide for how corporations can effectively use Facebook as a tool to connect with consumers is presented in Joan Voight's (2007) article, "Social Marketing Do's and Don'ts". The article describes how chain-outlet store Target created a successful Facebook presence, citing part of the success of their sponsored initiative to an "already strong brand identity with younger consumers and a Facebook page in tune with its brand values of design and affordability" (p. 14). While Target's ability to identify with younger audiences may be debatable, the underlying idea of the article is that in order to seem "hip," companies should be establishing online identities for themselves. The overall effectiveness of the campaign is also addressed, as Target's "back-to-school campaigns in their entirety helped lift sales 6.1 percent in August 2007 compared to August 2006" (p. 14). The article also warns potential marketers of the scepticism towards advertising exhibited by Facebook's primarily post-secondary based on an explanation by Facebook's vice president of media sales Mike Murphy. Murphy suggests that Facebook's "insider college orientation means the site has a community wary of advertisers" (p. 14). Voight goes on to quote Murphy as saying that users of the site are "very generous with their opinions, [and this group] will act on those opinions" (p. 14). This article warns agencies contemplating this route to consider their audience before plunging into online social networking. The article goes on to discuss the failure of ventures similar to Target's that were undertaken by McDonald's and Wal-Mart as attributable to the outspokenness of those using the sites and their negative perceptions of the corporation's practices. Users expressed their displeasure with the corporate practices of the companies through wall posts and discussion topics, communication tools which generally are available on the pages created for specific groups. While Voight's article is summarized in a positive light by describing how "an affiliation with a social network lets a brand show it understands its customers as well as provide a forum to offer solutions" (p. 30), the underlying message is that marketers can create successful online presences for corporations. As this strategy becomes more prevalent, given the unfamiliarity many new users will have with such marketing techniques, educational tools need to exist that teach the same type of critical thinking skills that would apply to making choices in "real-world" environments. In academic settings, where critical thinking skills are considered as fundamental to a university education, creating awareness of such corporate marketing tactics becomes especially important in contributing to the overall awareness such an education should entail. Again, creating a strong presence for university libraries via social networks would be an extremely beneficial tool for an academic librarian to implement and use to educate his or her patrons.

Furthermore, critical thinking skills are required in challenging marketing strategies similar to those expounded by Voight (2007). One such article entitled "i-Branding" extols the virtues of utilizing "viral marketing", describing it as an opportunity "to exploit pre-existing social networks

to produce exponential increases in brand awareness, through processes similar to the spread of an epidemic” (Simmons, 2007, p. 551). In explaining this principle, the author describes how:

one person ‘infects’ several people with an offer, who then spread it to several friends and acquaintances, until the entire virtual neighbourhood has been exposed. The global nature and ease of communication online makes the internet a powerful viral marketing tool. (Simmons, 2007, p. 551)

The abundance of messages such as these makes it clear that even if big business did not come in on the ground floor with online social networking, it is now very aware of the potential to reach a wide customer base. As efforts are increased to use these networks to market goods and services, users need to be made aware of the fact that what may seem like a simple online tool to communicate with friends needs to be subject to scrutiny as to the underlying motivations behind the creation of the sites. As advertising methods become more advanced, the importance of the role of academic librarians to educate the students and staff increases with regard to the critical thinking techniques that should be employed. Internet users, in general, need to be aware of the advertising implications inherent in the time they spend on the web, and also be aware that their interests may be used for marketing purposes. While many consumers may not have a problem with this principle and may actually appreciate being introduced to offers for certain goods and services, they must still be made aware that they may be passively participating in passively contributing to market research data. This is important if only to allow users the choice to prevent marketers and advertisers from accessing this information by protecting what they share about themselves online, including what they choose to include in their online social networking profile.

As the popularity of sites like Facebook increases, so too do the advertising strategies employed by the sites and outside marketing companies. The most widely criticized example to date of an advertising strategy that offended users’ notions of privacy is the “Beacon” system which Facebook attempted to implement in late 2007. A November 2007 article written for CBC’s “In Depth Technology” column by Jesse Hirsh brought the workings of the advertising system to the attention of many Facebook users. In the article, Hirsh addresses the fact that corporate bodies are currently creating Facebook communities to communicate with and attempt to sell goods to consumers. More disturbingly, he focuses on the ability of the Beacon technology to monitor what a user has bought online and notify his or her online contacts of these purchases. Hirsh states that inherent to the Beacon system is a computer code where when you “engage in consumer activity at a partner website, such as Amazon, eBay, or the New York Times, not only will Facebook record that activity, but your Facebook connections will also be informed of your purchases or actions”. It is possible to imagine any

number of situations in which sharing the details of a purchase could cause a range of effects from simple embarrassment to problems in a user's personal or professional lives. As well, the article suggests that the original Beacon system could not be turned off by users, as Hirsh states that "there is no way to opt out of this system, although the site will introduce controls that allow you to block the sharing of data with specific individual websites". Similarly, according to a press release from Facebook dated November 6, 2007, "[i]n keeping with Facebook's philosophy of user control, Facebook Beacon provides advanced privacy controls so Facebook users can decide whether to distribute specific actions from participating sites with their friends" (Facebook press release, 2007). Further investigation into what this meant for users showed that while it was possible for a user to block incoming information about friends' purchases, it was not possible to block their own information from being shared with those friends who have the option enabled. It is important to note that concise privacy information is not provided for users by the CBC article or the Facebook press release. Instead, users are left wondering what privacy controls will be available to them, as neither source clearly states these options, instead offering only vague descriptions of the how the system operates. Academic librarians can help stem this confusion by being aware of the emergence of these technologies and remaining informed of the implications for users. Interpreting the implications of new advertising systems and then circulating recommendations or answers to questions frequently asked by the student body could curtail confusion on campus.

There was a considerable outcry from Facebook users once the realities of the Beacon system were made known. According to BBC News (2007), "[m]ore than 50,000 Facebook users signed a petition calling on the company to alter or abandon its Beacon advertising technology" thanks to the activist group MoveOn (BBC, 2007; MoveOn, 2007). These signatures were gathered between the November 20th 2007 creation of the petition and the November 30th 2007 publication of the BBC article. A similar "Facebook Users Against Facebook Beacon" group was created by a Dalhousie Master's of Library and Information Studies student, and as of February 15, 2008, the group has over 2000 members (Barrett, 2007). Mark Zuckerberg (2007), the founder of Facebook, responded to this outcry in a blog posting dated December 5, 2007, by stating: "We've made a lot of mistakes building this feature [Beacon], but we've made even more with how we've handled them". Speaking directly to the confusion regarding Beacon's opt-in options, Zuckerberg states: "People need to be able to explicitly choose what they share, and they need to be able to turn Beacon off completely if they don't want to use it". The speed at which the Beacon system was introduced and reworked is indicative of the need for academic librarians to remain aware of the developments of online social networking sites, as it is pivotal to keep those using a university library informed of potential privacy intrusions. Ultimately, the development of Beacon created a definite shift in the way many people view the purpose of online social networking; while there has heretofore been an underlying suspicion

that users may have been sharing information in a way that could be exploited by advertisers, the creation of Beacon suggests that these suspicions have been confirmed.

While more questions are raised by Hirsh's (2007) article than answers provided, it directly addresses the notion that online social networks do not exist for idealistic purposes but instead to make money. Most interestingly, Hirsh directly addresses the fact that "Facebook has a huge database of consumer information and this new system allows advertisers to get at it". This sentiment bluntly assumes that the point of the existence of online social networking sites, and Facebook in particular, is to gather data for advertisers that people may otherwise be reluctant to share, by capitalizing on people's desire to be socially connected at all times. Hirsh also poses a series of questions that speculates whether or not the Beacon system will push users away or prevent new users from signing up. While the by line from Facebook's press release states that Beacon means that "Users Gain Ability to Share their Actions from 44 Participating Sites with their Friends on Facebook" (Facebook press release, 2007), the overwhelming public outcry that led to Zuckerberg's re-evaluation of Beacon and subsequent apology signals that this notion is misguided. The evolutionary path of aggressive advertising systems such as Beacon in online social networking sites, and Facebook in particular, remains to be seen, but these new marketing strategies are another aspect of privacy of which users need to be made fully aware if they are going to continue to use the sites. While Hirsh's article may not represent a scholarly source of information, it does exist in a medium that both students and staff of university libraries are likely to read and may consequently raise questions to be answered. Yet again, the opportunity exists for academic librarians to sort through the bombardment of information that events such as the announcement of Beacon will produce and generate guides that concisely illustrate the facts behind the technology.

Professional Concerns

One area of particular caution for professionals in particular that also applies to students who will soon be entering the workplace is the reliance on online social networks in recruiting. Users need to be aware of the fact that any potentially compromising information they share that may be accessed by employers when considering an applicant for a position. These possible repercussions are not necessarily deliberated upon when a person posts pictures from the previous weekend's antics wherein the depicted participants may not be portrayed "at their best." Many users may not stop to consider the ramifications of these types of images or even of posting messages describing participation in questionable activity. One source suggests that among human resource professionals, "about one in four [...] are using Internet search engines to investigate job candidates, and 12% say they have accessed social networking sites for this purpose" ("Using social networking...", 2007, p. 8). This usage is not surprising, as any person who makes this information readily available online is inviting such scrutiny. This human resources strategy is certainly one that can provide a more accurate

overall picture of a candidate instead of the composed image in an interview setting. There is an indication that decisions are being made on the basis of the information available about an applicant via online social networking, as “[of] those [HR professionals] who checked social networking sites, 63% did not hire the applicant because of the findings” (“Using social networking...”, 2007, p.8). A similar potential for problems is discussed in the article “Checking out Facebook.com” wherein the authors argue that there is a very “real possibility that potential employers may scan Facebook profiles for the ‘real skinny’ on job candidates” (Charingo & Barnett-Ellis, 2007, p. 25). While there is some debate expressed in the articles about whether or not searching within online social networks constitutes discriminatory hiring practices, it does serve as a strong word of warning for users to monitor what information they share online. Again, students and professionals looking for a job should not assume that just because their peer-group is involved in sharing similar information online means that they are necessarily safe from negative repercussions. This is also an issue that can be brought to the fore by academic librarians.

The Approach of the Academic Librarian

With all of the concerns that have been brought to the forefront regarding safety, privacy, advertising, and professional capacities, there are steps that can be taken to educate staff and students in university libraries as to how they can protect themselves. With such a vast number of different demographics involved, users of university libraries could certainly benefit from the establishment of an online identity for their respective institutions. Meredith Farkas (2007) argues that libraries “can create value in MySpace and Facebook by offering a space for patrons to give feedback, by providing news and information, or by providing a portal to library services” (p. 122). Her points about information and services would represent a prime online environment in which to address the privacy guides and training for staff and students which have been mentioned in this paper. While it may be possible for academic librarians to incorporate privacy concerns into library orientations or in-class educational sessions, these ideas may prove to be more effectively conveyed through the media which they address. Farkas’s book, for example, which was published in 2007, contains information about Facebook that is no longer current, namely that she discusses the fact that only educational institutions and certain companies can create accounts; since the publication of the book this is no longer the case, as anyone with a valid e-mail address can create an account (although there are certain age restrictions in place that are supposed to limit use, but can easily be bypassed by a user willing to lie.) Similarly, significant portions of this paper needed to be rewritten for submission to this journal as the Beacon technology introduced in November 2007 had been largely reworked by January 2008. Given the propensity for change in online social networking communities, developments such as Beacon could be more effectively addressed through an online presence that can evolve along with the sites to ensure that relevant, timely information is available. The speed at which technologies such as online social networking

evolve would suggest that a dynamic medium in which to present information would be more effective than print resources. The sentiment that online social networking can be used as an educational tool is echoed in several sources, including an educator who is quoted as saying that “[s]ocial networking technologies speak to all that is fresh and innovative in research, teaching and learning, and outreach” (Topper, 2007, p. 380). Ultimately, new privacy concerns are going to emerge, and new advertising and marketing techniques are going to be invented; to be effective as educators of university patrons and staff members, the media that academic librarians use to share information cannot be static if they are to remain effective.

As important as it is to educate users as to how their information could potentially be used in an investigative capacity or by marketing campaigns, there is also an opportunity for university libraries to learn from the marketing strategies employed by big business to reach a greater client base and provide greater customer satisfaction. As suggested by Meredith Farkas (2007), the marketing potential for this idea “is tremendous, as evidenced by the level of business activity within MySpace and Facebook” (p. 123) and she suggests that “libraries can engage in viral marketing, integrating themselves into their patrons’ social networks and using that ‘in’ to promote library services” (p. 119). Similar sentiments have been expressed in other sources, including an article reporting on a survey of librarians’ feelings regarding Facebook, which states that “[s]ome librarians were so enthusiastic about Facebook that they suggested libraries use the site to promote their services. Using the site to advertise library events and creating online library study groups and book clubs for students were some of the ideas expressed”(Charingo & Barnett-Ellis, 2007, p. 30). As shown by the business articles cited in this paper, corporations are becoming increasingly involved in online social networking to varying degrees of success. In order to best represent a university library in an online social network, lessons could not only be learned from the libraries that are currently participating in such ventures, but also from the successes and failures of the business community. In order to appeal to the widest range of patrons, steps would need to be taken to ensure that a library’s presence is effective in engaging library patrons and providing them with pertinent information.

Maintaining an active involvement in encouraging responsible usage by students and staff will ensure that the library’s online social network presence does not legitimize irresponsible use; focusing on privacy as absolutely pivotal to online interactions will ensure that academic libraries do not mistakenly condone inadvisable actions. Students and staff may misinterpret relaxed or non-existent attention to privacy policies in an academic library as meaning that such considerations do not need to be taken into account. Conversely, active involvement by libraries in crucial areas of student and staff participation will ensure that such misconceptions do not occur.

Conclusion

The potential exists for university libraries to implement effective online social networking programs to serve their patrons. As has been illustrated, there are several important areas that academic librarians need to focus on, which include raising awareness of basic privacy and safety concerns, illuminating new marketing campaigns, and making students aware of how their online interactions can negatively impact their professional lives. In order to be able to effectively educate students, academic librarians need to follow the developments that are intrinsic to each of these areas as well as any others that may emerge. This will require familiarity with a number of different information outlets, as online social networking is being addressed in a wide variety of business and trade papers, technology reports, and library publications. Further to this, the constantly evolving nature of online social networking requires a medium that can evolve equally as quickly; this means that library-run Facebook groups or e-mail lists will be significantly more effective in keeping students informed than printed materials which in many cases will become outdated soon after publication. Providing privacy guides through online social networks and having a library presence on such networks actively encourages the type of responsible behaviour that those using the sites need to exhibit. While the specific details of how to best maintain user privacy continue evolve along with the technology, certain core tenets will remain consistent; at the basic level, users must be fully aware of who has access to their information and be very careful with regard to sharing sensitive information such as addresses and phone numbers. Ultimately, these are steps that need to be taken in order to ensure university students and staff maintain a safe online presence and are aware of the wide-ranging implications of online social network use.

Footnotes

[1] Users who are logged into their Facebook account can view these settings and the analysis of the level of security of their profile at <http://www.facebook.com/privacy.php>.

References

- Atkinson, S., Johnson, C., & Phippen, A. (2007). Improving protection mechanisms by understanding online risk. *Information Management & Computer Security*, 15(5), 382-393. Retrieved November 20, 2007 from EMERALD database.
- Barrett, Creighton. (2007). *Facebook Users Against Facebook Beacon*. Retrieved February 15, 2008 from <http://www.facebook.com/group.php?gid=19940635616>.
- BBC News. (November 30, 2007). *Protests force facebook to change*. Retrieved January 14, 2008 from <http://news.bbc.co.uk/2/hi/technology/7120916.stm>.
- Charnigo, L., & Barnett-Ellis, P. (2007). Checking out facebook.com: The impact of a digital trend on academic libraries. *Information Technology & Libraries*, 26(1), 23-34. Retrieved November 14, 2007 from LISTA database.
- Cyber bullying: Understanding and preventing online harassment and bullying.(2006). *School Libraries in Canada*, 25(4), 17-22. Retrieved November 10, 2007 from LISTA database.
- Facebook. (2007). *Facebook press release - leading websites offer facebook beacon for social distribution*. Retrieved November 14, 2007, from <http://www.facebook.com/press/releases.php?p=9166>
- Farkas, M. G. (2007). *Social software in libraries: Building collaboration, communication, and community online* (1st. ed.). Medford: Information Today, Inc.
- Hirsh, J. (November 14, 2007). Beware of facebook's beacon? [Electronic version]. *CBC News - In Depth Technology*. Retrieved November 14, 2007 from <http://www.cbc.ca/news/background/tech/hightech/facebook-beacon.html>.
- Hitchcock, J. A., Nixon, C., & Burmood, J. (2003). The wild, wild web: Cyberstalking. *Collected Presentations of the 18th Computers in Libraries Conference*, 160-172. Retrieved November 10, 2007 from LISTA database.
- MoveOn.org: Democracy in Action*. Retrieved January 15, 2008 from <http://www.moveon.org/>.
- Read, Brock. (2006). Information technology. *Chronicle of Higher Education*, 52(20), A38 – A41. Retrieved February 8, 2008, from Academic Search Premier database.

- Simmons, G. J. (2007). "i-branding": Developing the internet as a branding tool. *Marketing Intelligence & Planning*, 25(6), 544-562. Retrieved November 14, 2007 from ABI/INFORMdatabase.
- Stern, Lesa A. Taylor, Kim. (2007). Social networking on facebook. *Journal of the Communication, Speech & Theatre Association of North Dakota*, 20, 9-20. Retrieved February 8, 2008, from International Bibliography of Theatre and Dance database.
- Sund, C. (2007). Towards an international road-map for cybersecurity. *Online Information Review*, 31(5), 566-582. doi:10.1108/14684520710832306. Retrieved November 10, 2007 from EMERALD database.
- Topper, E. F. (2007). Social networking in libraries. *New Library World*, 108(7/8), 378-379. Retrieved November 14, 2007 from LISTA database.
- Using social networking sites for recruitment: Pros & cons.(2007). *HR Focus*, 84(4), 8-9. Retrieved November 15, 2007 from ABI/INFORM Global database.
- Voight, J. (2007). Social marketing do's and don'ts. *Adweek*, 48(36), 14-17. Retrieved November 14, 2007 from ABI Inform Database.
- Zuckerberg, Mark. (December 5, 2007). *Thoughts on Beacon*. Retrieved January 14, 2008 from <http://blog.facebook.com/blog.php?post=7584397130>.