12

Social Networking Privacy and Its Effects on Employment Opportunities

Nicole Kennedy and Matt Macko

Prologue to Social Networking Overview

Imagine entering your final semester in college. Throughout the previous four years you have made it a goal to be involved with extracurricular activities at the university, to volunteer in the local community, to maintain a high grade point average and to receive recommendation letters from several well-known professors at the university. You are ready for your first interview, and have no doubt that you can land that dream job you have been working towards for the last four years. That is until the interviewer refers to direct quotes from your online social network profile and begins asking about your listed interests such as partying, drinking with friends, going to bars, and even your political views. You begin to wonder if they can use this information against you, and ask yourself the question: when did my online social life become a factor in my future professional life?

Unfortunately, this situation is not unrealistic. Currently, no regulations exist to protect job candidates from harassment of this sort. Government agencies work to resolve on the job issues with regards to fair hiring practices but the U.S. does not regulate an employers' search for incriminating information. This threat will remain a possibility as long as the world of social networking continues to expand and social profile privacy issues remain unresolved.

Overview of Social Networking

Social networking on the Internet began with a desire for people to quickly and conveniently share information with their friends and family. This form of communication blossomed rapidly and started competing in popularity with e-mail and text messaging. Entrepreneurs harnessed this technology and created various Internet sites, including Facebook and MySpace, designed to allow users to create a profile containing information about themselves that others can view. These sites also allow users to build social networks with hundreds or even thousands of people. Previously, the use of these websites posed little known threat to personal privacy and users' comfort levels changed.

They started by displaying the necessary information to construct an online persona. But the reality is, some information on these sites is very private and not something a person would share with their family at a reunion, a stranger on the street, and certainly not with a professional hiring manager.

As the world of social networking became more popular, Facebook increased the availability of its product, opening doors to new networks and members. What began with restricted access to students with valid university-issued e-mail addresses, spread to allow high school and corporate networks as well as users without verified e-mail addresses. These users can create profiles, and gain access to information on other members of the site (Facebook Opens Site to Everyone). College-aged students are beginning to see the mistake of providing private information on the Internet as more employers gain access to Facebook and use the information they find as a factor in hiring decisions. According to a July 2006 survey by the U.S. National Association of Colleges and Employers, "27% of employers have Googled their job candidates or checked their profiles on social networking sites" (George). These privacy issues are important to consider when creating a profile and interviewing for jobs. This chapter will shed light into the questions: Is it ethical for employers to use social profile information as a factor in hiring decisions? Are they currently using this information for decision-making? How do students feel about this "invasion of privacy?" What is happening today and what does the future hold for the confidentiality of social networking?

Facebook's Claim to Privacy Security

According to Facebook's Privacy Policy:

> Facebook is about sharing information with others — friends and people in your networks — while providing you with controls that restrict other third parties from accessing your information. We allow you to choose the information you provide to friends and networks through Facebook. Our network architecture and your privacy settings allow you to make informed choices about who has access to your information. We do not provide contact information to third party marketers without your permission. We share your information with third parties only in limited circumstances where we believe such sharing is 1) reasonably necessary to offer the service, 2) legally required or, 3) permitted by you (Facebook).

At first glance, this privacy policy appears all encompassing. It protects personal privacy rights, but under the auspices of the privacy clause listed on the Facebook website, the default account settings allow for anyone in a shared network to view a user's entire profile. In conjunction with the use of the Facebook Development Platform, third parties who agree to abide by the Platform's Terms of Service, including restrictions on access, storage and use of such data, are given limited rights to view members' personal information. "We have undertaken contractual and technical steps to restrict possible misuse of such information by such third parties, but of course cannot and do not

guarantee that all third parties will abide by such agreements" (Facebook).

Essentially Facebook states they will attempt to protect their user's information, but do not guarantee protection and refuse to take responsibility for certain breaches of protection. "Dan Hornig, a senior recruiting manager for Novo Recruiting, spends more than one-third of his day researching clients - and yes, that includes looking for information about them online" (Lupsa). This recruiting manager is an example of the third party who agreed to the Facebook Development Platform terms of service and now accesses thousands of college students' social profiles using that information however he pleases. All the while, Facebook escapes responsibility. Several cases in the past few years dictate the lack of privacy encompassed by the Facebook Privacy Policy.

Previous Case Involving the Threat of Social Networking Information

"A survey by CareerBuilder.com found that one in four hiring managers used search engines to screen candidates. One in ten also checked candidates' profiles on social networking sites such as MySpace or Facebook" (Lupsa). This is precisely what happened to an unsuspecting Louisiana State University student while interviewing for a job in 2006. He was a member of Facebook for over two years and maintained an "all-inclusive" online profile with pictures, quotes, and more. While interviewing for internship positions, he followed the advice of his mother as well as school advisors choosing to make his profile "private," so only his friends could see his information; or so he thought. Surprisingly, this security measure was not enough to protect his information from discovery.

> During the interview, something he was not prepared for happened. The interviewer began asking specific questions about the content on his Facebook.com listing and the situation became very awkward and uncomfortable. The student had thought that only those he allowed to access his profile would be able to do so. The interviewer explained that as a state agency, recruiters accessed his Facebook account under the auspices of the Patriot Act (LSUS Career Services).

This is one example of the unpredictability of current privacy controls and the misconception that only a member's friends can see their profile when they select "private" on Facebook. The consequences shocked the student. A seemingly innocent social networking site crushed his chances for the job and the company disappointed him with how far they went to unearth his private information. Extreme as this case may be, it accurately depicts privacy issues presented with social networking on the World Wide Web.

The Ethics Related to Social Networking Privacy:

The general definition of ethics is "a system of moral principles governing the appropriate conduct for an individual or group" (Encarta

Dictionary). How does this theory of ethics apply to the study of social networks and employers' use of them? Research of peoples' opinions on the ethics of employers using online information, especially that stemming from social profiles in a hiring or recruiting decision, shows continued controversy over this highly debatable topic. Current research finds one-third of students feel the practice of Facebook research is "unethical" (George). Students' worry employers will take information out of context and the purpose or rationale behind their social profiles will be misunderstood. In further research, "42% of students said that for companies to make hiring decisions using Facebook is a violation of privacy … whereas … only 21% of employers thought the same" (George). According to Philadelphia attorney Jonathan Segal, "the question is what employers do with the information they find on the Internet," (Segal). Clearly differences in opinion exist, but where should society draw the line between employer due diligence and applicant/prospective employee privacy?

Why Employers Are Researching Job Candidates Online

Due diligence is defined as "the degree of care that a prudent person would exercise, and a legally relevant standard for establishing liability" (Encarta Dictionary). Insurance companies conduct extensive research compiling information to value a policy and the inherent risks of a client. Companies now initiate the same techniques with background checks in an effort to acquire outside information regarding potential job candidates. Companies perform these necessary tasks to protect themselves and their organization by mitigating risks through due diligence and exercising a distinguished degree of care when evaluating job candidates and clients.

Is it reasonable to expect a corporation not to conduct proper background checks on job applicants? They limit their liability of choosing the wrong candidate and the majority of people agree to a background check when requested during the job application process. Can students and future professionals expect prospective companies to disregard information they willingly place on the Internet when being evaluated for possible careers and considerable responsibility within the company? Countless companies argue they simply perform due diligence when evaluating applicants based on personal information, including that found within their online social profiles. Others agree, believing people who voluntarily and knowingly place private and personal information on public networking sites should recognize the likelihood employers will access the information and use it to their discretion.

Chris Wiley, the study's other author, predicts that the debate over the increasingly blurred line between personal and professional life on the Web will eventually be settled in the legal system: Facebook is just a small part of the bigger issue of privacy on the internet. In the meantime, until members of the Facebook generation become bosses, keep your profile private, or don't put anything on there that you wouldn't want your mom to see (George 2007).

Keeping one's profile completely private may seem unnecessary, but as the information revolution progresses, and privacy becomes increasingly more important, private profiles may be the only safety net available to the next generation of social networking clientele. In order

to determine the use of this "privacy" function among current business students, the following research was conducted.

Survey and Statistical Research

This chapter's research looked to discover differences in students' as well as employers' opinions regarding online profile privacy. The student surveys asked questions to see what students felt was important to their privacy in regards to social networks as well as what they thought might affect them in a hiring decision. The employer surveys were very similar and were used to compare differences in student and employer opinions regarding social network privacy. The goal was to discover whether a difference exists in these opinions between male and female students, as well as any differences between students and employers. In the quest for employer diversity, opinions were sought from human resource departments at an engineering firm, several accounting firms, as well as a local bank. The surveys were distributed and returned by over 100 students and 14 employers before data analysis began.

The survey data was compiled and analyzed by employing several techniques to determine if the results were indicative of the general business student population. Due to the nature of the survey questions, median testing was required to properly examine the data. This is the result of using a small number of discrete variables (1-10: strongly disagree - strongly agree) as opposed to a continuous number format. The Mann-Whitney Test was employed, which specifically tests medians and assumes equal variances between numbers, and can be used where normality in data is not required; all of which pertained to the collected data. "The Mann-Whitney Test is a nonparametric test to compare two populations, utilizing only the ranks of the data from two independent samples" (Seward 706). A hypothesis test was also applied to compare two proportions. "A hypothesis test is a decision between two competing, mutually exclusive, and collectively exhaustive hypotheses about the value of a population parameter" (Seward 350). This test was primarily used to compare the original pre-conceived notions (null hypotheses) of the business student and employer population with survey sample results. These tests helped gain insight into how the business student population feels about their social network privacy as well as into how employers feel about this relatively new and powerful tool.

Survey and Statistical Research Results

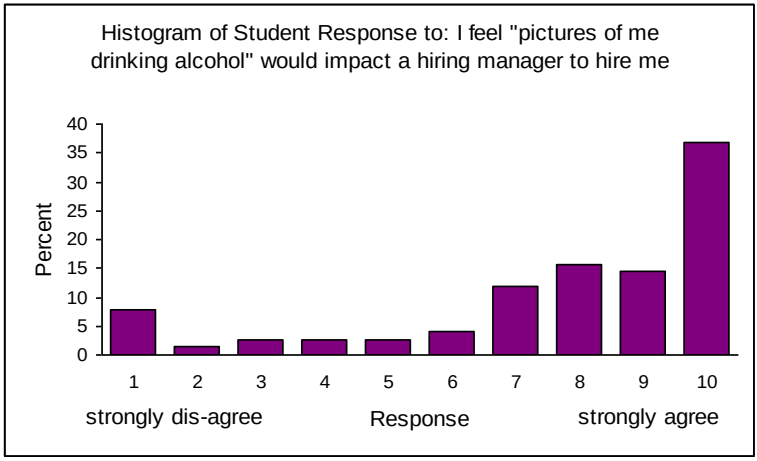
The analytical research results confirmed several pre-conceived notions regarding opinions on social network privacy, but also proved interesting in various unexpected facets. The Mann-Whitney Test was applied assuming women would rank a majority of the following: address, phone number, e-mail address, birth date, relationship status, class schedule, etc., as being more important to their personal privacy than men. The test showed a significant difference between women and men across the population for information such as address, phone, e-mail address, current employment, and class schedule, each having P-values of .05 or lower. This means female business students rank this information as more important to their personal privacy than male

students, which confirmed expectations.

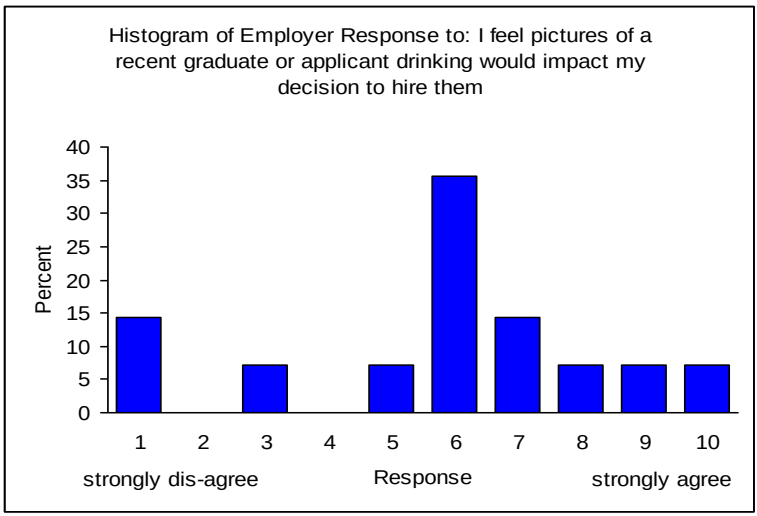
A hypothesis test then determined whether there was a difference in the population of men and women business students with regards to their profiles being classified as private. The null hypothesis stated that the proportion of women with private profiles was equal to the proportion of men with private profiles. This analysis went against previous assumptions that more women would have private profiles than men, thus a one-tailed test of the alternative hypothesis was used for verification of these results. The one-tailed hypothesis test resulted in a P-value of .04, which signifies a substantially greater proportion of women business students than men business students who have made their profiles private.

Earlier literature research quoted, "42% of students said that for companies to make hiring decisions using Facebook is a violation of privacy … whereas … only 21% of employers thought the same" (George), which set expectations for various survey outcomes, yet further analysis yielded surprising results. 41% of the 100 students surveyed actually found it ethical for employers to use social networking sites in hiring decisions, and 57% of employers thought the same. Further analysis using a hypothesis test determined the difference between men and women's feelings regarding the ethics of social networking privacy in hiring situations. Respondents were asked, "Do you think it is ethical for hiring managers to use information obtained from your social profile when making hiring decisions?" A two-tailed hypothesis test resulted in a P-value of .63, and produced the null hypothesis that women and men feel the same in regards to the ethics of using social networking sites in the hiring process. The survey data did not show a statistical difference between men and women's feelings on ethics across the population of business students, so a rejection of the null hypothesis failed. These sample results were surprising based on previous expectations that a difference would exist. Yet, it remained to be determined whether there existed a variation in opinions between students and employers.

Based on previous literature review, a greater percentage of employers view the use of social network sites in the hiring process as an ethical practice. Due to this original hypothesis a one-tailed test was used to determine if surveyed employers would agree, and resulted in



the P-value of .16. This P-value was not small enough to conclude that employers and students feel differently regarding the ethics of using social network sites for hiring decisions. In fact, several prior theories regarding differences between student and employer opinions proved inaccurate. Below are two histograms showing this unexpected difference:



Surprisingly, students were more apprehensive about an employers' viewing pictures of them drinking than the employers surveyed, who in the majority gave a nearly neutral answer on the topic. Although the employer sample was small, the results are

unanimous: employers ranked online pictures and videos, drinking and drug paraphernalia pictures, promiscuous behavior pictures, etc., all at a lower importance than students. These results were the most astonishing.

This survey data gathered provides insight into the differences in opinion regarding social network site privacy issues, but certainly does not give a comprehensive picture. Time constraints limited the extent of analysis of the survey data collected. Finding correlations as well as statistical comparisons between categories and between classes (Freshman, Sophomore, Junior, Senior) would be the next step. The Kruskal-Wallis test is recommended for this research as it compares the population medians across multiple categories. In addition, the limited amount of employer respondents was a restriction on conclusive decisions and broadened the possibility of error in statistical results. The students surveyed consisted primarily of a broad population within the Leeds School of Business, and do not accurately depict the opinions of the University of Colorado or scholastic institutions as a whole. Student opinions from the Leeds School of Business may have been altered by classes teaching privacy issues, or from their predispositions regarding business ethics. Tailoring the survey to include a more diverse student sample, acquiring data from more employers, and deciphering the data with a continuous number format to allow more statistical analysis would yield more accurate results for future research. Until that time, it is necessary to explore the current state of affairs regarding these rising privacy issues.

What is Being Done: The Present

To resolve these concerns, laws need to be enacted to protect the respective parties and regulate the use of the wealth of online social networking information. The decision to either empower employers by allowing them to use all public Internet information in hiring decisions, or to protect potential employees by restricting the information employers are legally able to use, is imminent in the U.S. However, as of March 2007, no evidence of lawsuits or legal actions against a company that used public Internet information against a job applicant exists.

Very few laws protect applicants and currently we found virtually no statutes in place to restrict discriminatory Internet practices. With the recent escalation in the importance of this topic within corporate America and the news, lawmakers may be forced to address this controversial issue sooner rather than later. With the abundance of public information pouring onto the Internet, laws will be necessary to protect applicants in the future.

New York currently protects applicants by prohibiting employers from “taking adverse action against employees’ off-duty, political, or union activities and recreational activities" (Segal). This is by no means a universal law, nor does it protect employees from persecution during the recruitment process; however, it does address a critical issue: the importance of distinguishing work life from an employees’ social life outside of work. The question is whether what one chooses to do outside the office should be their private business. Employees tend to characterize their company both at work and at home. Upper level

management is certainly expected to maintain a representational responsibility to their company:

> David Perry, an executive recruiter, says a candidate to become a chief financial officer was found to have a gambling problem. We actually found it out and tracked his profile back to an online gambling site on the Web. Now, you have to ask yourself, what's that got to do with his job? Well nothing, probably. But this is a multibillion-dollar corporation that we were putting a chief financial officer into and we just didn't think it was appropriate (NPR).

Where should the line be drawn? Laws will be necessary to determine whether due diligence background research should stop at mid-level management or continue all the way down to the mailroom employees, as is possible today.

Finland is currently the only country progressively handling these Internet privacy issues in a concrete way by passing nationally recognized regulations.

> Finland's Data Protection Ombudsman ruled in a November decision that employers cannot use Internet search engines, such as Google, to obtain background information on job candidates. Ombudsman Reijo Aarnio told BNA the decision was clear-cut. 'According to the [Privacy in Working Life Act], employers can only view personal data provided by their employees, and this includes data about job applicants'. He continues saying 'the act is based on the idea that everyone is in agreement on the kind of data collected' (Segal).

From an employee's standpoint, it may be a relief to see countries taking action to protect their individual privacy rights; however, an entirely different issue regarding the feasibility of monitoring and enforcing these laws will arise in the aftermath of their creation. What policies could stop an employer from searching possible candidates on the Internet, and who would enforce such conventions? When will laws govern these unique situations? Based on current U.S. regulations, the Equal Employment Opportunity Commission could become that governing agency.

Equal Employment Opportunity Commission

Currently, the Equal Employment Opportunity Commission (EEOC) protects employees from discrimination.

> The Equal Employment Opportunity Commission is an independent federal agency created by Congress in 1964 to eradicate discrimination in employment. The various statutes enforced by the Commission prohibit employment discrimination on the basis of race, color, sex, national origin, religion, retaliation, age and disability (EEOC).

This commission protects employees from discrimination in the interview process, employment process, and the firing or lay-off

process; however, finds difficulty regulating the pre-interview process. Below is a fictitious example of how the Internet and social networking sites may adversely affect an applicant.

A professional hiring manager is prejudiced to certain personal characteristics. He keeps his views secret within the workplace, but exercises these beliefs on a daily basis while reviewing and searching applicants' personal information on the Internet. Upon discovering conflicting information regarding the applicants' religion, racial preferences, or national origin, he simply disregards their résume. To avoid prosecution, he claims he never received the résume. This employer undeniably uses the Internet in a discriminatory way and it is likely these practices will not be discovered nor will he see legal action under the current set of laws governing hiring practices. To illustrate the purpose of this example and to understand its high likelihood, consider the following interview with Steven Viscussi explains:

> Interviewer: Does that mean the employer might find out about things they could not ask about in a job interview?
>
> Steven Viscusi: Absolutely, like your sexuality, which is often on MySpace or Friendster Connection. They can find out about how many kids you have, your family, who your looking for, even what your habits are. and by the way, its no longer a chance that they might find out, many human resources departments are actively pursuing these sites to find out all the questions that they can't legally ask you (NPR).

Hiring departments use the Internet to their discretion in order to narrow the applicant field without seeing repercussions from the EEOC. "Some employers worry that because of the access it gives them to information on race, sexuality, or religious affiliation, using Facebook as a hiring tool may be in violation of equal opportunity standards" (George). As long as this prejudiced screening process occurs before the interview, there is little an applicant can do to argue they should have been hired. While no litigations attributable to these laws and regulations currently exist, the controversy surrounding privacy and the Internet will press courts to address these issues.

Fair Credit Reporting Act

The Fair Credit Reporting Act and Accurate Credit Transactions Act of 2003 (FCRA) regulates third party background screening agencies who conduct comprehensive pre-employment screening, criminal searches and background checks for various corporate clients. Companies specifically contract these agencies to search for and scour information on employees, possible insurance policy purchasers, and an assortment of potential consumers of numerous industries. The FCRA defines a consumer report as:

> Any written, oral or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living, which is used or collected in whole or part for the purpose of serving as a

> factor in establishing the consumer's eligibility for credit or insurance to be used primarily for personal, family or household purposes; employment purposes; or any other permissible purpose authorized under 1681b (Sotto 3).

Invariably, these third party background screeners also use the Internet in their extensive searches. If screening firms find negative information on a candidate, federal law requires them to notify the candidate as well as establish a procedure to verify the information is current and accurate. Unfortunately, these regulated procedures are not always followed. Tena Friery, research director at the nonprofit consumer organization Privacy Rights Clearinghouse in San Diego, said, "screeners often turn up erroneous information by failing to properly match key 'data points,' such as first, middle, and last names; previous names; Social Security numbers; date and place of birth; and previous addresses" (Sotto 3). These laws and regulations cover only a portion of the issues currently confronted in new "ordinary" hiring practices, and the future is guaranteed to bring new opinions and regulations regarding these concerns.

What the Future Holds

If reputation protection is a concern, Claimid.com and a host of other Internet sites assist in this process. Fred Stutzman and Terrel Russell organized an online service to help people track, verify, annotate, and prioritize personal online information. The goal of the service is to provide a representative depiction of yourself when you are searched online (George 2). Other companies such as Naymz and ReputationDefender.com exist for the same purpose. For a small fee starting at about $5 a month, these sites monitor online profiles as well as provide the necessary tools to protect reputations and the accessibility of any negative information.

The goal for many of these sites is search engine flooding, which pushes negative press to the second and third pages of a search where the likelihood of its discovery drastically decreases. They also have the ability to contact the site administrator where they lobby on your behalf to remove any information you choose, especially useful when disputing the accuracy of information. ReputationDefender.com's motto is "search and destroy."

> For a small fee, Michael Fertik (ReputationDefender.com's creator) digs through clients' Internet profiles and then shows them how they appear online. If clients see something they do not like, ReputationDefender will contact whoever controls the Web page and urge them to delete the material. If they resist, Fertik -- a Harvard law graduate -- says his company is ready to use attorneys (NPR).

Services such as ReputationDefender.com provide a public relations service to the layman. These sites grow in popularity daily but are still underused and underappreciated. "Perry (creator of Naymz) says that with so many recruiters vetting people on the Internet, job candidates either need to background themselves or hire someone else to do it for them" (NPR). The reality is that more and more employers search the Web and social network sites everyday. Students and job candidates need to protect themselves whenever possible and should

consider using one of the aforementioned sites or protect themselves by maintaining a private and "clean" profile that is free of any information that could reflect poorly on their character.

Conclusion

The age of information distribution has arrived and regardless of the varying opinions concerning social networking sites, it is important that individuals are aware of the risks as well as the benefits that these services may inadvertently provide. This chapter focuses on the negative uses of social network information; however, there could be many arguments supporting the use of this information in hiring decisions as well as how these sites could indeed benefit the job applicant or student. Due to time constraints, it was impossible to research and focus on the possible benefits that could be obtained through positively networking oneself on these sites in order to gain contact with a potential employer. Many recruiters use these sites in addition to hiring sites such as Monster.com and Careerbuilder.com to get in touch with possible job candidates, and social networking sites could prove to be a powerful recruiting tool if created and maintained effectively by both students and employers.

In the present situation, regardless of whether someone posted the information or it simply exists in cyberspace, protecting oneself is a serious concern. A majority of people already do so by making their profiles private to outside viewers or by employing reputation defenders, but most do not understand the strict need for protecting an online persona from employers. Employer snooping occurs daily and will occur increasingly in the future; the question is a matter of what people will do about it until laws are created to overcome these obstacles. The goal of this chapter is to create an awareness of the seriousness of this issue and its contested existence. It is expected that the future will bring new laws and regulations regarding the knowledge and the use of this information that is provided so freely through the ever-expanding World Wide Web. Until then, student and job applicants beware, this information has the potential to harm reputations as well as career opportunities.

Works Cited

"Facebook, Myspace, etc. And Getting Hired." Louisiana State University Career Services. <http://www.lsus.edu/career/announcement_details.asp?ID=43>.

David P. Doane, Lori E. Seward. Applied Statistics in Business and Economics., 2007.

Encarta Dictionary. March 7, 2007.

"Facebook Opens Site To Everyone." September 26, 2006. <PCMagazine.com>.

"Facebook Privacy Policy." October 31, 2006. <www.facebook.com>.

George, Alison. "Facebook Follies Can Hurt Your Job Prospects." December 8, 2006. <USNEWS.com>.

George, Alison. "Living Online." New Scientist 2006. February 5, 2007.

Lupsa, Christian. "Do You Need a Web Publicist." Christian Science Monitor November 29, 2006: 13.
"NPR.org." <http://www.npr.org/templates/story/story.php?storyId=6462504>.
"NPR.org." <http://www.npr.org/templates/story/story.php?storyId=5695383>.
Segal, Jonathan. "Vetting Via." Abstract.
Sotto, J. Lisa, and M. Elisabeth McCarthy. "An Employer's Guide to Workplace Privacy Issues." 24.1 (2007)