UNIVERSITY STUDENT ATTITUDES TOWARDS EMPLOYERS ACCESSING THEIR PRIVATE SOCIAL MEDIA

Hal Records, Bryant University, hrecords@bryant.edu
Suhong Li, Bryant University, sli@bryant.edu
Robert Behling, Arrowrock Technology, behlingr@gmail.com

ABSTRACT

Many of today's students spend a great deal of time online, and social networking is an important part of their daily communications. This study investigates students' perception of risks associated with the use of Social Media as it relates to their search for employment. It is based on a survey of 216 students from a northeast university. Findings indicate that 1) Social Media policies and the laws impacting them are in an evolutionary phase; 2) employer scrutiny of Social Media use by employees is increasing; 3) the impact of Social Media scrutiny by employers is having a significant impact on employees; 4) respondents are learning that Social Media can become a personal liability if not managed properly; and 5) there exists a dichotomy in that many respondents view obtaining a job as paramount but insist that privacy is more important.

Keywords: Social Networking, Social Media, Risks of Social Networking, Social Networking and Employment and Privacy of Social Networking

INTRODUCTION

The continued growth in the use of Social Media has brought about a significant change in the way students interact and socialize. Social networking sites have evolved into virtual communities where students share information and images, and build and maintain personal relationships. Social networking sites such as Facebook, Twitter, LinkedIn and Google+ have become a part of the daily life of most college students, with the potential for playing a significant role in how they are viewed by others, including potential employers (Wolfe, 2007). At the time postings are made students may not be aware of the long term impact of those postings, therefore they may not exercise care in deciding what text and images to place on their site for others to view. They may also have a false sense of security, thinking that only their friends will have access to their private postings. The reality is that often others, including potential and existing employers, find ways to access personal sites and review content (Gallagher, 2009). This review may be done with or without the knowledge of the individual, and may fall somewhere between "due diligence" and "snooping." The goal of this paper is to better understand how about-to-become employees of the current generation view their Social Media rights to privacy that are under attack by employers.

Protecting sensitive and personal information: Social Media sites allow users to control the exposure of, and access to, posted information through various security devices (Smith & Aplin, 2012). However, the security is not fool proof, and establishing yourself as a Social Media friend can often provide a window of access to personal information without the individual knowing others can see what they believe to be restricted personal information and images they have posted (Gaudin,2010). Social networking sites are only as safe as the user makes them. Many of the privacy settings are not the default settings, therefore are not activated unless the user specifically changes and/or activates them.

The rapid growth of the web and networking applications has transformed the way people communicate. Utilizing these sites is generally thought to be harmless when they are used properly, however carelessly posted information may inadvertently lead to negative consequences. For example, when personal information posted on a Social Media site includes pictures, obvious personal characteristics such as race and age become readily available to

anyone accessing the site, and when these characteristics are factored into hiring decisions, they may constitute discrimination (Smith & Alpin,2012).

After studying 20 mobile and traditional social networks, including Facebook, LinkedIn, and Twitter, researchers at Worcester Polytechnic Institute found that all 20 sites leaked some kind of private information. This leaked information often allowed third party sites to connect user's browsing behavior with their profiles on social networking sites without the users' knowledge, and to use this to their advantage (Gaudin,2010).

Accessing sensitive and personal information: Accessing Social Media postings provides recruiters and employers with an inexpensive way to screen and do background checks on individuals, often without their knowledge. There is an increase predicted for companies monitoring employees Social Media profiles as a part of their security monitoring programs, highlighting the ethical gray area surrounding social networking privacy (Liebowitz,2012). Mielach (2012) discusses whether it is ethical for a company to use what you post on a Social Media site in employment decisions, and suggests that individual postings may be fair game for employers to review.

Asking applicants to share names and passwords for Social Media sites may pose major ethical challenges for employers. One concern is the lack of consistent Social Media policies both within and throughout organizations. Without carefully crafted policies to guide human resource professionals, errors are bound to occur. Bluvshtein (2012) reports that while the number of businesses with Social Media policies is increasing, there are still about one-third of these businesses with no formal policy to guide the employment process relating to reviewing an individual's Social Media.

Evolving Ethical and Legal Treatment of Social Media Privacy: Facebook is on record as being opposed to employers asking applicants and employees for Social Media user names and passwords, and many states have pending legislation restricting employers from requiring job applicants to provide user names and passwords for personal Social Media sites as a condition of employment (Smith & Aplin,2012). Also, a number of U.S. Senators are concerned that accessing Social Media by employers may lead to discrimination and invasion of privacy. Employers utilizing logon credentials to collect sensitive information under the guise of a background check may be a pretext for discrimination, and Senators Schumer (NY) and Blumenthal (CT) have asked the Department of Justice to investigate whether companies are violating the Computer Fraud and Abuse Act by doing this (Smith & Aplin,2012).

Much of the current protection of Social Media Privacy stems from the National Labor Relations Board where employer policies governing the use of Social Media by employees are restricted so as to insure that the use of Social Media in discussion of work conditions and unionization cannot be impeded by employers. A default by-product of this action appears to be that non work condition related use of Social Media can be controlled by employers (NLRB,2012).

Employer access and use of Social Media postings: Employer's use of Social Media sites to gain inappropriate access to private information on presumed secure media sites is increasing (Smith & Alpin,2012). A simple question that has a complicated answer is "Is an employer accessing Social Media sites of candidates or employees due diligence or is it invasion of privacy?" (Huffpost,2012). Employers often use information found on sites such as Facebook as a window into candidate's and employee's personalities (Liebowitz,2012), however, asking or requiring individuals to share their Social Media user names and passwords could pose major ethical challenges for employers (Smith & Aplin,2012).

At the national level, Congress has been unable to come to agreement on the Password Protection Act, so states are starting to take action, and the list of states not allowing employers to demand employee's Social Media passwords is growing (Kerr, 2013). In 2012 California, Maryland and Illinois enacted legislation prohibiting employers from

requesting or requiring employees to disclose Social Media user names or passwords, and other states have similar legislation under review (Thompson, 2012). As of early 2013, three additional states have enacted similar legislation making it illegal for employers to demand employee's Social Media passwords, bringing the number of states with statues to six (Kerr, 2013). The practice of employers requiring employee's passwords is not as commonplace in Europe because such practices breach the Data Protection Act provisions, and may subject employers to discrimination allegations (Hodgkiss,2012).

Employers will likely find what is posted online. Thirty five percent of surveyed employers report using Social Media to pre-screen candidates, with Facebook being used two thirds of the time (Huffpost,2012). This screening is not always made known to candidates, and Liebowitz (2012) and Smith & Aplin (2012) report inappropriate Social Media screening is on the rise.

Outcomes of employer use of Social Media: In 2012, 68.9 percent of employers said they've created policies specifically for Social Media use, compared to 55.1 percent in 2011. Among the nearly 250 multinational businesses surveyed in the past two years, Social Media monitoring by employers increased from27.8 percent to 35.8 percent in the last year. (Proskauer,2012)

Of the more than 2000 hiring managers surveyed, twelve percent said when they were investigating a person's Social Media site they were looking for reasons not to hire a person, and *34 percent said they came across something that caused them not to hire a candidate (Huffpost,2012).*

Few studies have investigated employees' attitudes towards employers viewing their private Social Media. It is unknown whether a potential employee is more willing to provide employee access to their Social Media to obtain a job or is more likely to reject the access in order to maintain the privacy of their Social Media. To further explore this question, four situations are designed in this study to investigate a student's response when required by an employer to provide access to their Social Media account. Students could either agree to the request and increase the likelihood of being employed, or deny the request and maintain the privacy of their Social Media communications.

Situation 1: College Sophomore applying for an internship with a large insurance company.

> Location: You are talking with a company recruiter in your college's placement office, interview room.

> Discussion: Recruiter asks student about professional skills and interests, teamwork skills, flexibility for travel, geographical preferences, salary issues. The recruiter gives you company materials and her business card. She also invites you for a site visit. You give her your resume, at which point the recruiter requests access to your Facebook, and Twitter accounts.

Situation 2: College Senior applying in person for a job with a global distributor of sunglasses.

> Location: You are at the company's corporate headquarters located in a beautifully landscaped office park outside Boston.

> Discussion: You are interviewed first by the manager of the marketing department, then given a tour of site facilities and you are introduced to people who might become your coworkers if you are hired. At the end of the day you are interviewed by an associate in the human resources department, who indicates that it is standard policy for the company to look at prospective employee Social Media accounts.

Situation 3: College Senior applying on-line for a job.

> Location: You will be graduating in May and are at home on spring break. You find a position posted on Monster.com for an entry level data analyst with a major health insurance provider.

Discussion: The job posting seems to be exactly what you are looking for and is located exactly where you would like to be. The site requests that you submit an electronic copy of your resume with a cover letter. It also requests that you provide access to your Facebook and Twitter accounts.

Situation 4: You are a recent college graduate who is just starting work for a large defense contractor.

Location: You are at one of the company's primary manufacturing plants located on beautiful Narragansett Bay just south of Providence, Rhode Island.

Discussion: Since you are working for a defense contractor you have already successfully passed a federal security background check and are in the human resources office on your first day of work. After completing the required payroll, tax and benefit forms you have been asked to sign a release giving your employer authority to access to your e-mail accounts.

Based on the above situations, the following hypotheses will be tested:

H1:   Students are willing to accept an invasion of privacy on their Social Media accounts to obtain or keep a job.

H2:   Student class status does not influence student attitudes towards employer or potential employer viewing Social Media postings.

H3:   Student gender does not influence student attitudes towards employer or potential employer viewing Social Media postings.

H4:   Student Frequency of use of Social Media does not influence student attitudes towards employer or potential employer viewing Social Media postings.

H5: Students are not influenced by whether the job application process is on-line or in-person.

Survey design and respondents: The survey was administered on-line using SurveyMonkey to students attending a small private University located in the northeast United States. The survey contains six questions about student demographics, and four scenario/situation based questions. A total of 216 useable surveys were returned. Demographics of respondents are as shown in *Table 1*.

Table 1 *Demographic Information*

Variable	Criteria	Number (Total: 216)	Percentage
Status	Freshman	23	10.6
	Sophomore	105	48.6
	Junior	34	15.7
	Senior	54	25.0
Gender	Male	126	58.3
	Female	90	41.7
Number of Respondents using Each Social Media	Facebook	206	95.4
	Twitter	145	67.1
	Linked-In	119	55.1
	Google+	25	11.6
Number of Hours Per Day Spent Using Social Media	<= 1 hour	53	24.5
	> 1 hour and <=2 hours	69	31.9
	>2 hours and <=3 hours	47	21.8

	>3 hours	47	21.8
To Whom a Respondent Uses Social Media to Communicate	Classmates	198	91.7
	Friends	211	97.7
	Family	165	76.4
	Businesses	71	32.9
# of Estimated People Viewing a Respondent's Social Media Postings	<100	78	36.1
	100-199	43	19.9
	200-499	40	18.5
	500-999	35	16.2
	>=1000	20	9.3

Analysis of Survey Results

Response tabulation of the four situations and Chi-Square Testing were used to analyze the impact of status, gender, usage frequency of Social Media, and privacy perception as they relate to student views of privacy versus their need for employment.

Exhibit 1 *Analysis of Four Situations* shows how respondents reacted to choices of whether to forego privacy in each of four employment scenarios. As previously described the first relates to an internship, the second applying in person and on-site for a job, the third applying on-line for a job and the fourth being asked on the first day of employment for access to private Social Media.

Exhibit 1 - *Analysis of Four Situations*

	Decision	Number	Percentage
Situation 1: College Sophomore applying for an internship with a large Insurance Company.	Provide the requested addresses along with passwords and access code	63	29.2
	Deny the request	153	70.8
Situation 2: College Senior applying in person for a full time job with a global distributor of sunglasses.	Provide the requested addresses along with passwords and access code	99	45.8
	Deny the request	117	54.2
Situation 3: College Senior applying on-line for a full time job.	Provide the requested addresses along with passwords and access code	63	29.2
	Deny the request	153	70.8
Situation 4: You are a recent college graduate who is just starting work for a large defense contractor	Provide the requested addresses along with passwords and access code	91	42.1
	Deny the request	125	57.9
In General, which is more important to you?	Getting the job/internship	149	69.0
	Maintaining the privacy of your Social Media accounts and possibly losing the internship/job.	67	31.0

Exhibit 2 *Respondent Classification* defines three distinct groups based on responses to each situation. Group 1 that we call Job Seekers includes respondents who agreed to provide the requested accounts with passwords for all four situations. Group 2 that we call Privacy Protectors are the respondents who denied access for all four situations.

Group 3 that we call Middle Group includes respondents who agreed to provide access in some situations and denied it in others.

Exhibit 2 - *Respondent Classification as a Percentage of Respondents*

	Percentage
Job Seeker	12.0
Privacy Protector	35.6
Middle Group	52.3

Impact of Status: As shown by Exhibit 3 *Chi-Squire Test of Impact of Student Status*, whether a student is a freshman, sophomore, junior or senior does not have a significant impact on a respondent's reaction to each situation and hence to the group to which they belong, yet juniors and seniors do have a somewhat higher tendency toward job seeking versus privacy.

Exhibit 3 - *Chi-Square Test of Impact of Status*

Status	Job Seeker		Privacy Protector		Middle Group		Chi-square Test
	Actual Freq.	Expected Freq.	Actual Freq.	Expected Freq.	Actual Freq.	Expected Freq.	
Freshman	3	2.8	6	8.2	14	12.0	χ^2=6.985 df=6 P=0.32
Sophomore	8	12.6	43	37.4	54	54.9	
Junior	7	4.1	12	12.1	15	17.8	
Senior	8	6.5	16	19.3	30	28.3	
	26	26.0	77	77.0	113	113.0	

Impact of Gender: As shown by Exhibit 4 *Chi-Squire Test of Impact of Gender,* again, the results show that gender does not have a significant impact on a respondent's reaction to each situation, though males may be somewhat more likely to forego privacy. Based on earlier studies we have done in this area it appears that the gender gap is decreasing over time.

Exhibit 4 *Chi-Squire Test of Impact of Gender*

Gender	Job Seeker		Privacy Protector		Middle Group		Chi-square Test
	Actual Freq.	Expected Freq.	Actual Freq.	Expected Freq.	Actual Freq.	Expected Freq.	
Male	19	15.2	43	44.9	64	65.9	χ^2=2.655

Female							df=2
	7	10.8	34	32.1	49	47.1	P=0.27
	26	26.0	77	77.0	113	113.0	

Impact of the Frequency of Social Media Use: As shown by Exhibit 5 *Impact of the Frequency of Use of Social Media,* time spent using Social Media does not have an impact on a respondent's response to each situation.

Exhibit 5 - *Chi-Square Test of Impact of the Frequency of Use of Social Media*

Time Spent Using Social Media	Job Seeker		Privacy Protector		Middle Group		Chi-square Test
	Actual Freq.	Expected Freq.	Actual Freq.	Expected Freq.	Actual Freq.	Expected Freq.	
<= 1 hour	8	6.4	20	18.9	25	27.7	χ^2 =2.597 df=6 P=0.86
> 1 hour and <=2 hours	7	8.3	23	24.6	39	36.1	
>2 hours and <=3 hours	7	5.7	15	16.8	25	24.6	
>3 hours	4	5.7	19	16.8	24	24.6	
	26	26.0	77	77.0	113	113.0	

Impact of Privacy Perception: As shown by Exhibit 6 *Chi-Square Test of Perception on Privacy Importance*, a respondent's perception on the importance of getting the job or maintaining privacy is directly related to his/her response to each situation. For the respondents who think getting the job/internship is more important, they will provide the account information in all situations. However, for the respondents who denied the request to access their accounts, about half of them (38/77) still consider getting the job/internship is more important which is a dichotomy. In real situations they will be forced to make a choice. For the respondents in the middle group, the majority of them (75%, 85/113) again consider getting the job/internship is more important.

Exhibit 6 - *Chi-Square Test of Perception on Privacy Importance*

Which one is more important?	Job Seeker		Privacy Protector		Middle Group		Chi-square Test
	Actual Freq.	Expected Freq.	Actual Freq.	Expected Freq.	Actual Freq.	Expected Freq.	
Getting the job/internship	26	17.9	38	53.1	85	77.9	χ^2 =26.615 df=2

Maintaining the privacy of your Social Media accounts.						P=0.00
	0	8.1	39	23.9	28	35.1	
	26	26.0	77	77.0	113	113.0	

Impact of Application Process (on-line or in-person): Situation 2 relates to a college senior applying in person for a full time job and situation 3 refers to a college senior applying on-line for a full time job. A paired sample t-test was used to see whether a student responds differently to those two situations. This result is significant with a p-value at 0.00, indicating application process does impact a student's willingness to provide the access to his/her Social Media account. Exhibit 1 shows that for situation 2 (when applying in person for a full time job), 46% of the students will provide the requested addresses along with passwords and access code, however, this number decreased to 19% in situation 3. The result indicates that a student is more willing to grant the access to his/her Social Media account when asked in person than when asked online.

RESULTS

H1:   Students are willing to accept an invasion of privacy on their Social Media accounts to obtain or keep a job was found to be a dichotomy.

H2:   Student class status does not influence student attitudes towards employer or potential employer viewing Social Media postings was found to be largely true.

H3   Student gender does not influence student attitudes towards employer or potential employer viewing Social Media postings was found to be true.

H4:   Student Frequency of use of Social Media does not influence student attitudes towards employer or potential employer viewing Social Media postings was found to be true.

H5:   Students' attitudes toward employers viewing their Social Media postings are influenced by whether the job application process is on-line or in-person.

CONCLUSIONS

* Social Media policies and the laws impacting them are in an evolutionary phase;
* Employer scrutiny of Social Media use by potential employees is increasing;
* The impact of Social Media scrutiny by employers is having a significant impact on potential employees;
* Students' behavior clustered them into 3 groups, the Job Seeker, the Privacy Protector, and the Middle group;
* Students are more likely to forego Social Media privacy when applying for a job in person than when on-line;
* Students are learning that Social Media can become a personal liability if not managed properly;
* There exists a dichotomy in that many respondents view obtaining a job as paramount but insist that privacy is more important.

Future Research: It will be useful to repeat this study in future years to track changes over time in the relationship between employers seeking to monitor Social Media of their potential employees, and how potential employees view this challenge to their privacy. Likewise it will be important to see how governments attempt to regulate, and courts interpret what is likely to be an ongoing and uncertain saga of privacy as it relates to hiring in the 21st century.

REFERENCES

_____ (2012) "37 Percent of Employers Use Facebook to Pre-Screen Applicants, New Study Says," *Huff Post Business*, April 20, found at: www.hufingtronpost.com/2012/04/20/employers-use-facebook-to-pre-screen-applicants-n_1441289.html.

_____ (2012) "The NLRB and Social Media: "National Labor Relations Board, April 18, found at: http://www.nlrb.gov/node/5078.

Bluvshtein, N. (2012) "Looking for Insight Into How Other Businesses Use Social Media," November 29, found at: www.networkedlawyers.com/category/emplpyument-policies/.

Gallagher, C. (2009) "Prospective Employers Checking You out on Facebook Not Ethical? Get Over it," November 8, *Word Press*, found at: http://chuckgallagher.wordpress.com/2009/11/08/prospective-employers-checking-you-out-on-facebook-not-ethical-get-over-it/.

Gaudin, S. (2010) "Social Networks Leak Your Information, Study Says," *ComputerWorld*, June 28, found at: www.computerworld.com/s/article/9178648/social_networks_leak_your_information_study-says.

Hodgkiss, K. (2012) "Monitoring or Snooping? When Employers Social Media Checks Cross the Line," April 19, found at: www.thenewrepublic.com/blog/european-technology/monitoring-or-snooping-when-employers-social-media-checks-cross-the-line/524.

Kerr, D. (2013) "Six States Outlaw Employer Snooping on Facebook," January 2, *CNET*, found at: http://news.cnet.com/8301-1023_3-57561743-93/six-states-outlaw-employer-snooping-on-facebook/.

Liebowitz, M. (2012) "Huge Spike Expected in Employer Facebook Snooping," June 1, *TechNews Daily*, found at: www.foxnews.com/tech/2012/06/01/huge-spike-expected-in-employer-facebook-snooping.

Mielach, D. (2012) "Are Facebook Profiles Fair Game for Employers?," *Business News Daily*, July 24, found at: http://smallbusiness.foxbusiness.com/legal-hq/2012/07/24/are-facebook-profiles-fair-game-for-employers/.

Poskauer Rose LLP (2012). "Social Media in the Workplace Around the World 2.0"*, April 18, found at: http://www.proskauer.com/files/News/c4f04351-44a6-4343-9bf6-bcf6e5d0a265/Presentation/NewsAttachment/a7c0c180-df76-4383-9297-b75d70dd24c9/2012_ILG_Social_Network_Survey_Results_Social_Media_2.0.pdf

Records H, Li S, and Behling R, (2012) "Does Social Networking Expose Students to Excessive Risk?", *Issues in Information Systems, Vol 13, Issue 2,* October 2012, 380-389.

Smith, E. and D. Aplin. (2012) "Employers Should Tread Carefully in Asking For Facebook, Other Social Media Passwords," April 12, found at: www.bna.com/employers-tread-carefully-128849087182/.

Thompson, T. (2012) "Emerging Issues in Social Media – The Status of Social Media Password Legislation, November 6, found at: www.networkedlawyers.com/category/employment-policies/.

Wolfe, A. (2007) "Student Attitudes Towards Social Networks and Learning Modalities," found at: http://alisonwolfe.com/wordpress/wp-content/uploads/student_attitudes_social_networks2.pdf.