"ON BEYOND E-MAIL" – THE EMERGING LABOR AND EMPLOYMENT ISSUES WITH SOCIAL MEDIA

STATE BAR OF MICHIGAN ANNUAL MEETING & SOLO AND SMALL FIRM INSTITUTE

LABOR & EMPLOYMENT LAW SECTION MEETING

SEPTEMBER 30, 2010

Tiffany A. Buckley-Norwood, Esq., *Dickinson Wright PLLC*
Carole D. Bos, *Bos & Glazier*
Adam S. Forman, *Miller Canfield*
Jeffrey J. Fraser, *Varnum*
Brian E. Koncius, *Law Offices of Kathleen L. Bogas, PLLC*

TABLE OF CONTENTS

I. INTRODUCTION

As technology continues to change, labor and employment practitioners must apply labor and employment law standards to the new technology. Social media sites and participation in those sites has grown exponentially. So, as the social networking "craze" continues (until the next big "thing") all of us get the opportunity to participate in, stretch and mold the application of labor and employment relations law to social media.

Some social media statistics are worth repeating (and are constantly changing) as all of us begin to think about social media in the labor and employment relations context. For instance:

- The average social network user: 37 years old
- The average Facebook® user: 38 years old
- The average Twitter® user: 39 years old
- The average LinkedIn® user: 44 years old

Approximately 25% of all social network users are between the ages of 35-44. The average Facebook® user spends 55 minutes per day on the site. It's hard to imagine that at least some (and just maybe much) of this time is spent during work time.

Facebook® currently has over 500 million users. Twitter® currently has approximately 106 million users sending 55 million tweets a day. LinkedIn® currently has approximately 65 million users. According to a 2009 survey, approximately 55% of employees admit to using social networking sites during work time. Approximately 60% of managers surveyed believe they have the "right to know" what employees say about their organization in all employee personal social networking pages.

None of us know what the next new "thing" is going to be. If you want to have a better idea, ask your teenage kids. They generally know before we do. Regardless, the current social media explosion requires that employers, employees, and unions work through labor and

employment issues that arise. We attempt to highlight a number of those issues through this white paper.

II. WHAT IS SOCIAL NETWORKING?

The terms "social media" and "social networking site" are frequently used interchangeably. According to Wikipedia, social media is media designed to be disseminated through social interaction and is created by using highly accessible publishing techniques. There are a number of different types of social media sites, including:[1]

- Blogs
- Microblogs, such as Twitter®
- Social Networking Platforms, such as Facebook®, LinkedIn® and MySpace™
- Virtual Worlds, such as SecondLife®
- Sharing Sites, such as Flickr®, YouTube® and Slideshare®

A social networking site is a subset of social media. It is an online community of people who share ideas, interests, activities and/or events within their individual networks. Usually, social networking site users create a profile for themselves and then connect with other users. Most social networking sites provide a variety of ways for users to interact, such as e-mail and instant messaging.

III. LEGAL CONSIDERATIONS

Employers face two types of risk related to employee usage of social media: (1) legal risks stemming from hiring, firing or taking other adverse action due to social media and (2) business and legal risks stemming directly from employee use of social media. This section addressed the first type of risk.

---

[1] *See* Wikipedia, A List of Social Networking Sites, *available at* http://en.wikipedia.org/wiki/List_of_social_networking_websites.

A. The Hiring Process

In the "olden days" applicants submitted paper resumes and sent letters to prospective employers through the mail. Now, through current technology, there are on-line job postings, LinkedIn® references and video clip resumes. You can hire a consultant to manage your social media websites to be sure that if any prospective employer conducts a Google name, Google images, Google videos, or other search, that the prospective employer sees only appropriate and positive applicant attributes.

There are many practical and legal considerations that arise if an employer decides to use social media sites as part of the employment "screening" process or as an investigation tool related to current employees. As well, applicants and employees need to spend a few minutes thinking through whether there really is a line between work and private life anymore. A few of the issues are highlighted below.

Some practical issues for employers include:

- Is the social media information accurate?
- Is the information really about the applicant or employee?
- How do you verify the information once you have it?
- Are you uniformly applying a social media screening process to all applicants?
- Is the information private?
- How did you obtain the information?

Some practical issues for employees include:

- Are my social network forays public or private?
- Have I created a public diary?
- Am I willing to give a prospective employer my access codes to private social media spaces?
- How many videos (with me in them) have I uploaded to YouTube?

- How many videos (with me in them) have my friends secretly uploaded to YouTube?
- How many blogs do I have and what is the content?

Some of the legal issues include:

- Protected characteristics (age, height, sex, weight, marital status, disability, religion, national origin, personal health information, genetic characteristics)
- Fair Credit Reporting Act obligations
- Applicant tracking obligations for OFCCP
- Invasion of privacy
- Negligent hire
- Negligent retention
- Discrimination (adverse impact)
- Investigation protocols
- Work time access to social media

Some private employers have decided to fully embrace social media. These employers ask applicants to identify all social media sites they frequent and to provide access codes for private spaces. Other employers simply conduct applicant "due diligence" through the internet which includes checking social media sites. Many employers confront the social media issue during employment investigations related to current employees. One of the significant risks related to employer access to applicant or employee social media sites is that the employer obtains protected information about the applicant or employee. If an employer obtains protected information, then the employer/prospective employer must determine what to do with that information.

Employers/prospective employers are legally prohibited from acting on protected information. Even if the employer/prospective employer does not act on the protected information, a rejected applicant or a disciplined employee can certainly allege that the employer/prospective employer did act on the protected information. As well, employers

sometimes receive information about employee A from co-employee B who has access to employee A's private social media information. What obligation does an employer have to investigate typical employment disputes, such as harassment, discrimination, employee violence, drug use, alcohol use, etc., based on this information?

Establishing a social media policy and a comprehensive internet background search policy, as well as training supervisors and other company personnel regarding how to obtain legitimate information without running afoul of legal obligations, is imperative.

1. Background Checks

Social media is an attractive and growing source of information about employees and applicants. Employers must use these resources with caution when making employment decisions. Appropriate review of the information available on such sites may be prudent to guide the hiring process. However, planning and forethought are essential before the employee uses such resources to gather information.

First, the information may not always be accurate. The employer may not be able to verify that the information is legitimate or complete. For example, a social networking site may indicate that the applicant has been arrested. However, the site may not state the circumstances of the arrest, whether the arrest involved a felony or whether the arrest resulted in a conviction. Under Section 205a of Michigan's Elliott-Larsen Civil Rights Act an employer cannot request, make or maintain a record of information regarding a misdemeanor arrest if there was no conviction.[2] As another example, a third-party may be motivated to make false, disparaging comments about the applicant on a social networking site. The employer may have no indication that the information is inaccurate.

[2] M.C.L. § 37.2205a

A background check performed by a "consumer reporting agency" on behalf of an employer, using social networking sites or information, may implicate the Fair Credit Reporting Act ("FCRA"), 15 USC § 1681 *et seq*. While the FCRA does not prohibit employers from receiving or using a consumer report that contains information gained from the sites, it does require them to follow specific notice and procedural guidelines. Generally, the employer must notify applicants or employees, and obtain their consent to, any such investigation of them.

On the other hand, Michigan law recognizes a claim for negligent hiring or negligent retention of a worker who is known – or *should be known* – to present a hazard to other workers or members of the public with whom the employee comes in contact, and who harms someone in the performance of her or his duties. Recent social networking decisions suggest that employers may have an affirmative obligation to consider publicly-available social media information in evaluating employees' fitness for duty or proclivity toward violence.

2. Discrimination

Using social networking sites to research employees and applicants may also expose the employer to an increased probability of discrimination claims.

Such activity increases the possibility of a typical disparate treatment claim alleging intentional discrimination. Most employers are wise enough not to ask questions regarding protected characteristics such as race, gender, marital status, age, disability or religion on their employment application or during the interview process. However, social networking sites make such information readily available to employers. An employee's MySpace™ blog may disclose that he suffers from a physical or mental condition. LinkedIn® users have the option of posting their birthday on their page.

Whether or not the employer considers this information, it is deemed to have knowledge of any information it comes across; and, thus, may place itself in the position of having to prove

it did *not* use or consider such internet intelligence. There is no question that the employer's practice of accessing social network sites, or the specific information it obtains from those sites for a particular applicant or employee, is discoverable in employment litigation. Further, relatively recent electronic-discovery rulings emphasize that the employer has an affirmative obligation to maintain copies of all sites, blogs, or media reviewed or consulted.

An employer that uses social networking sites as the source of information for hiring, may expose itself to "disparate impact" discrimination claims. Actionable disparate impact occurs when otherwise facially neutral criteria, procedures or policies, disproportionately impact upon applicants or employees due to the protected characteristics of those persons. Importantly, a disparate impact claim does *not* require the plaintiff to prove that the employee *intended* to discriminate. Certain social networks are targeted towards specific age, racial, religious, gender or political groups. So, for example, employer reliance on information obtained from these sites may give rise to a disparate impact claim, where use of certain social network sites may result in a less diverse applicant pool or have a disparate impact on certain protected groups.

Prior to 2009, the EEOC did not explicitly address employer use of employee information gained from social networking sites. However, on October 5, 2004, the EEOC published an informal letter on *Title VII / ADA: Recordkeeping Responsibilities for Electronic Resumes with Video Clips / Employer Knowledge of Ethnicity, Gender, and Disability Prior to Interview.*[3] Based on that letter, the EEOC treats an employer's recordkeeping obligations for video resumes the same as paper applications and all other records having to do with hiring. Solicited resumes should be retained for one year, and resumes of people hired need to become part of the employee personnel file and kept for three years. Unsolicited resumes do not need to be kept.

---

[3] *available at* http://www.eeoc.gov/eeoc/foia/letters/2004/titlevii_ada_recordkeeping_video.html; *see also* 29 C.F.R. 1602.14; 29 C.F.R. 1607.4.

The first explicit EEOC mention of social networking sites appeared in the proposed regulations for Title II of the Genetic Information Nondiscrimination Act ("GINA"). Among other things, GINA prohibits covered entities from intentionally acquiring genetic information regarding employees. In proposed regulation 29 C.F.R. §1635.8(b)(4), one exception to this prohibition is the acquisition of publicly available materials that may include genetic information. For example, an employer would not violate GINA if it learned that an employee had the breast cancer gene by reading a newspaper article profiling several women living with knowledge that they have the gene. While the proposed regulation would not apply to the internet collection of information concerning other types of protected characteristic information, it is clearly the position of the EEOC that even where information is obtained through a publicly available source, genetic (or, presumably, other protected characteristic information) may not be used to discriminate.

B. Anti-Harassment and Anti-Retaliation Statutes

Despite the legal considerations above, employers may have an obligation to respond to inappropriate online communications. On-line harassment of co-workers is one such area. In *Blakey v Continental Airlines*,[4] the district court denied summary judgment of a female pilot's hostile work environment claim premised on Continental's duty to prevent another worker's derogatory electronic bulletin postings, once Continental knew or had reason to know of the alleged work-related harassment.

An employer policy prohibiting such misconduct may help to establish the employer's *Faragher/Ellerth*[5] affirmative defense to harassment claims. This rule allows the employer to

---

[4] 2 F. Supp.2d 598 (D.N.J. 1998).

[5] *Faragher v City of Boca Raton*, 524 U.S. 775 (1998); *Burlington Indus., Inc. v Ellerth*, 524 U.S. 742 (1998).

defeat an otherwise valid harassment claim by showing that it exercised reasonable care to prevent and correct promptly any discriminatory harassing behavior, and that the plaintiff employee unreasonably failed to take advantage of any preventive or corrective opportunities provided by the employer.

Anti-retaliation provisions, found in a wide range of remedial statutes, are also a probable source of future claims for protection of employees' online communications. Such statutes are ubiquitous and include the *National Labor Relations Act*, the *Family and Medical Leave Act*, *Sarbanes-Oxley*, and the *Surface Transportation Assistance Act*.

C. National Labor Relations Act

The *National Labor Relations Act* ("NLRA")[6] and its state analog, the *Public Employment Relations Act,* ("PERA")[7], prohibit adverse treatment of employees engaging in protected "concerted activity." Employee messaging critical of the employer, or engaging other employees to discuss workplace issues (wages, hours, working conditions, etc.), constitutes protected activity, whether or not the employer's communication facilities are used. Unknown to some employers, these statutes and the rights they establish apply to workers in both unionized *and non-unionized* settings.

The National Labor Relations Act, 29 U.S.C. §157 ("NLRA") states:

> Employees shall have the right to self-organization, to form, join, or assist labor organizations, to bargain collectively through representatives of their own choosing, **and to engage in other concerted activities for the purpose of collective bargaining or other mutual aid or protection,** and shall also have the right to refrain from any or all of such activities . . .

---

[6] 29 U.S.C. §§ 151-169.

[7] MCL 423.201 *et seq.*

To be protected under NLRA Section 7, the activity must be (1) concerted and (2) for mutual aid and protection. Any employee, unionized or not, that believes he/she has been disciplined/discharged for engaging in protected concerted activities for mutual aid or protection can file an unfair labor practice charge with the NLRB. The NLRB has been grappling with social media and employee access to employer email and social media sites both during work time and after work time.

The NLRB has long-established guidance regarding employee solicitation (verbal) / distribution (paper) rules during and after work time. Essentially, if an employer permits employees (or employees by past practice) to engage in non-work-related solicitation/distribution during work time, then employers cannot discipline/discharge employees for engaging in union-related solicitation or distribution during work time. In a case called *The Guard Publishing Company d/b/a The Register-Guard*, 351 NLRB 1110 (2007), the NLRB analyzed whether The Guard Publishing Company violated the NLRA through a policy which prohibited employees from using the company email system for all non-job solicitations. In a 3-2 decision, the NLRB held that the Company's employees did not have the statutory right to use the email system for protected concerted activity.

In the case, the company disciplined an employee after she used the company's email system to send union-related messages to her co-workers. The company's written communications policy prohibited using email for commercial, political, and religious solicitations, as well as solicitations for "outside organizations" and "non-job-related" matters. The NLRB held that in determining whether the email policy violated the NLRA, the NLRB would look to activities or communications of a similar character and not activities of a different character because "discrimination means the unequal treatment of equals." In essence, the

NLRB said it was okay to send personal emails on any topics, but the email related to the union matter was prohibited because it related to an outside organization.

Interestingly, on July 7, 2009, the DC Circuit Court of Appeals remanded *Register Guard* back to the NLRB because the DC Circuit found that there was not substantial evidence to support the NLRB's finding that the company lawfully disciplined the union president for sending two union solicitation emails because they were organizational, not personal, solicitations. *Register-Guard* is currently pending before the NLRB. The current NLRB is a much different NLRB than the 5-member NLRB that issued its decision in the original *Register-Guard* case in 2007. The only remaining NLRB member from 2007 is Member Liebman, who now chairs the NLRB. There are only four (4) current NLRB members. Three (3) of those members are democratic appointees. I suspect there might be a different conclusion in the *Register-Guard* case at some point.

Likewise, the NLRB General Counsel issued an advice memo on December 4, 2009, analyzing whether Sears Holding Company's Social Media Policy could be reasonably construed to chill Section 7 protected activity. The General Counsel concluded that Sears' Social Media Policy did not violate NLRA Section 8(a)(1) because it could not reasonably be interpreted in a way that would chill Section 7 activity. In the *Sears* case, the IBEW was attempting to organize the in-home service technicians. The in-home service technicians used on-line media, including a website, Union4sears.webs.com and public pages on Facebook and MySpace. As well, the service technicians communicated with their colleagues around the country using a Yahoo ListServe. Sears did not sponsor or administrate the ListServe.

Sears issued a Social Media Policy in June 2009. Sears' stated purpose for the policy was to minimize risk to the Company and its associates, but not to restrict the flow of useful and

appropriate information. Sears prohibited employees from discussing specific topics in any social media forum, including: confidential and proprietary information; information about clients; intellectual property; and **"disparagement of company's or competitors products, services, executive leadership, employees, strategy, and business prospects."**

The NLRB General Counsel's office analyzed whether the quoted language above could be viewed as an attempt to chill Section 7 rights. Sears did not attempt to discipline service techs who were regularly talking about the social media policy on ListServe. In order for the NLRB to have reasonable cause to believe that Sears' Social Medial Policy violated the NLRA, the NLRB would need to show that:

> (1) employees would reasonably construe the language to prohibit Section 7 activity; (2) the rule was promulgated in response to union activity; or (3) the rule has been applied to restrict the exercise of Section 7 rights.

If Sears had only precluded discussion in social media regarding disparagement of the company's executive leadership, employees, or strategy, then the NLRB would likely have determined that Sears' Social Media policy would chill Section 7 rights. However, since the statement was made in the context of prohibiting discussion of many other topics, the NLRB General Counsel's office decided that Sears' Social Media Policy would not chill Section 7 rights. Employees simply could not reasonably construe Sears' Social Media Policy to prohibit Section 7 activities. Moreover, Sears did not try to discipline any service tech for discussing the Social Media Policy on the ListServe.

The NLRB General Counsel's office continues to review social media policies raised through unfair labor practice charges. Disciplinary actions taken against union or non-union employees related to application of social media policies will be carefully reviewed if raised as potentially violating the NLRA.

D. Invasion of Privacy and the Stored Communications Act

Most states, including Michigan, also recognize an employee's right to privacy. An invasion of privacy claim may be brought against an employer who intentionally and unreasonably intrudes, physically or otherwise, into the employee's private affairs. These cases often turn on whether the individual had a reasonable expectation of privacy, and whether the employer used a method to intrude into that privacy that a "reasonable person" would find objectionable. An employee's expectation of privacy is usually decreased on social networking sites because they are forums open to the public. However, if the employee restricts access to his or her profile and the employer uses improper means to access the profile, then the employer may violate the employee's right to privacy. Such improper means could include pretending to be another person or entity.

Unauthorized access to an employee's social networking site may also violate the federal Stored Communications Act ("SCA"),[8] which addresses access to stored wire and electronic communications and transactional records. The SCA establishes civil liability for anyone who intentionally accesses stored communications either without authorization or exceeds the authorization given. The SCA only applies to stored communications in facilities that are not readily accessible to the general public.

The case of *Pietrylo v. Hillstone Restaurant Group,*[9] demonstrates a claim of improper employee access. In that case, the plaintiff-employee established a group on MySpace™ that was only accessible by invitation. No upper-management was invited to join the group and the group was to only be accessed during non-work hours and on non-work computers. However, an

[8] 18 USC § 2701 *et seq.*

[9] Case No. 06-5754, 2009 WL 3128420 (D.N.J. Sept 25, 2009).

employee who had access to the group gave her password to her manager. Despite the privacy warning on the group's page, two managers accessed the group site on multiple occasions; and eventually used the information obtained as a basis to terminate the plaintiff. The district court held that a jury could infer, from testimony provided, that the employee who gave management her password only did so because she feared she "would have gotten in trouble" if she had refused. Notably, there was no testimony that management actually threatened this employee. However, management continued to access the website even after they became aware that the employee was uneasy about providing them with her password. The practical rule taken from this case is that employers should access private sites only with highest caution.

If the employer is a public employer, fraudulent or unauthorized access to the employee's social networking profile, blog or forum may also violate the Fourth Amendment's protections against unreasonable search and seizure. Access may also violate the Fourth Amendment if it is excessive in scope. In *City of Ontario v. Quon*[10], the City purchased pagers capable of sending and receiving text messages for its SWAT team. Before acquiring the pagers, the City already had a "Computer Usage, Internet and E-mail Policy," which essentially stated that the City reserved the right to monitor all e-mail and internet usage with or without notice. After the issuance of the pagers, SWAT team members were advised orally, then in writing, that text messages sent over the pagers were considered e-mails by the department. When the plaintiff continuously exceeded his monthly text message character allotment, an internal investigation revealed that many of the messages the plaintiff sent and received were not work-related, and some were sexually explicit. The Court ultimately held that because the search of the plaintiff's

[10] Case No. 08-1332, -- U.S. -- (June 17, 2010), *available at* http://www.supremecourt.gov/opinions/09pdf/08-1332.pdf.

text messages was motivated by a legitimate work-related purpose and because it was not excessive in scope, it was reasonable under the Fourth Amendment.

Fraudulent or unauthorized access of an employee's social networking information may also violate the social networking site's Terms and Conditions of Use.

E. First Amendment Rights

Public employers must consider the public employee's First Amendment right to free speech. State constitutional law may also be relevant to private employers, depending on where employees are located. States, such as Connecticut, extend constitutional protections to private employees.[11]

In determining whether speech is protected, a court will balance the employer's legitimate interest in delivering efficient services against the employee's interest as a citizen in commenting on a matter of public concern.

F. Off-Duty Conduct Statutes

An employer should be aware of any "off-duty conduct" protection statutes in the states where they have employees. Such statutes limit an employer's ability to regulate employee conduct off the job. Michigan does not have an off-duty conduct statute. However, other states, such as California, Colorado, New York and North Dakota have such statutes.

G. Other Potential Risks

There are a number of other potential risks involved with employee use of social networking sites. Employees may inadvertently disclose employer or customer trade secrets or other confidential information through pictures, status updates or blog posts. Additionally, if the employee is acting within the scope of his or her employment, the employee comments critical or

---

[11] *See* Conn. Gen. Stat. § 31-51q (adopting by reference state and federal constitution protections).

disparaging of other persons, other companies, products or services, may expose the employer to defamation or "false light" claims. Moreover, depending on the content of the employee's social networking posts, the employee may be protected from adverse employment action by state and federal whistleblowing and anti-retaliation statutes.

IV. CREATING A SOCIAL NETWORKING POLICY

The rise in social networking use generally, has led to an increase in social networking site use in the workplace. For example, a study conducted by Workplace Media in May 2009 determined that 43% of workers access their social networking site at work.[12] A July 2009 study conducted by Nucleus Research found that one in 33 workers built their entire Facebook® profile at work.[13]

A. Considerations Regarding Appropriate Employer Policy

In crafting a social media policy, the employer must first determine the purpose of the policy. The employer may wish to strongly restrict social networking activity. This would entail prohibiting employees from using company electronic resources for anything other than business-related matters. Alternatively, the employer may wish to encourage employees to contribute to social networking sites because the benefits of employee contributions to such sites outweigh the risks. As a third approach, the employer may wish to recognize that employees participate in social networking sites and simply outline company expectations regarding usage. In deciding which approach to use, the employer should be cognizant of how it intends to enforce the social networking policy.

---

[12] *See* WorkPlaceMedia, Brand Impact Social Networking Survey (May 2009).

[13] Nucleus Research, Research Note - Facebook: Measuring the Cost to Business of Notworking (July 2009).

The following issues, among others, should be considered in the development of an appropriate employer policy:

- Specify the forms of online communication and conduct covered by the policy;
- Outline how the company's name and logo may be used, if at all;
- Describe what financial, confidential, sensitive or proprietary information must be excluded from such sites;
- Address whether employees may discuss specific clients and whether the employee may post pictures of the workplace;
- Remind employees that postings on social networking sites are public;
- Encourage employees to engage in responsible and respectful conduct regarding current, former, and potential customers, partners, employers and competitors;
- Warn employees to avoid conflicts of interest and harm to the employer's business interests;
- Contemplate the legal considerations discussed above and the employer's other employment policies and guidelines, such as the anti-discrimination policy or other code of conduct;
- Avoid violation of protected communication rights, as discussed in this paper; and
- Outline possible disciplinary action for violation of the policy.

The policy may also include a discussion of how the employer's electronic resources and work time may be used for social networking sites. The personal use of social networking sites should not interfere with working time.

B. The "Company Spokesperson" Appearance

Most employers will prefer to prohibit employees from appearing as an official or unofficial "spokespersons" for the company. Employees may be prohibited from communicating

or appearing to communicate on behalf of the company. Employees may also be required to state that anything posted is the employee's view alone, not that of the employer.

The Federal Trade Commission regulates the use of endorsements and testimonials in advertising. 16 C.F.R. Part 255. Under the regulations, employees who use social networking sites to make statements about their employer's products may create unintended liability for the employer if a consumer later claims that they were misled into purchasing the employer's product. The regulations impose liability on both "endorsers" and companies for false or unsubstantiated statements made through an endorsement or for failing to disclose material connections between the company and the endorser. Thus, employers must ensure compliance with the regulations if endorsements may be made.

C. Supervisor Recommendations

The social networking policy may also address whether evaluations and recommendations may be given informally through social networking sites. LinkedIn® encourages users to obtain recommendations to complete their profile. As a result, employees have started obtaining recommendations from their supervisors. Most LinkedIn® recommendations tend to be positive, whether drafted accurately or simply as a courtesy to the employee. This could prove problematic if the employee is later terminated for poor performance or misconduct. The employer's legitimate basis for the employment action may be rebutted by an on-line commendation, or the recommendation may be used as evidence to claim the legitimate reason is merely pretext for unlawful discrimination. A Facebook® wall post stating "Great job today" or "you are a real asset to the company" poses the same risk.

It may be preferable to restrict performance reviews to the employer's regular review system and prohibit supervisors from giving informal reviews on social networking sites or

anywhere else. Where the employer prefers to allow such recommendations, it should be clear that the supervisor is speaking on his own behalf, rather than on behalf of the company.

D. The Blurred Line Between Supervisor and Employee

Aside from addressing supervisor recommendations, employers should also consider addressing the relationship between supervisors and employees generally. As supervisors are increasingly "friending" employees on Facebook® and making connections on LinkedIn®, the lines of appropriate conduct between supervisors and employees are blurring.

It may not be advisable to prohibit supervisors from "friending" employees. However, employers should at least train their supervisors on the legal risks of such relationships. Employers should also consider updating their anti-harassment, anti-discrimination, code of business conduct and other policies to cover social networking. At the very least, such policies should be reviewed to make sure they do not conflict with the new social networking policy.

E. The Ability to Take Disciplinary Action

Finally, regardless of the approach taken, the policy should state that the employer reserves the right to take disciplinary action against an employee if his or her social networking activity violates the employer's policies and guidelines.

V. CONSIDERATIONS FOR ATTORNEYS REPRESENTING EMPLOYEES

Social networking is not going to go away. The percentage of adults using these sites grows every year. The next employee who walks into your office is likely to have left fingerprints on the internet. This is true of potential defendants and witnesses too. Attorneys need to ask about an employee's use of social media and about the technology they use to access that media. Attorneys need to know what is out there, how and when it is accessed, created, and changed, and by whom it is viewed. The employee may not know to tell you about her

Facebook®, LinkedIn® and MySpace™ pages or Twitter® account. The employee may not know to tell you about his posts, blogs, and "tweets" or those he receives from or follows regarding potential defendants or witnesses. You need to know where to look for dirt on the employer and individuals involved, including your own client.

Once you ask, you need to explain to the employee why you are asking so they do not feel that you are prying and explain how this may help them protect themselves and gather information to use against a potential defendant. Walk them through the discovery process and explain why this information is important to review, why it may be at issue and relevant, and why they may need to provide it to the employer and its attorneys during the litigation of any potential employment claim. An employee may not want to show you. You may not like what you see. On the other hand, you may find a goldmine of useful information and evidence that is helpful or possibly hurtful to any potential claim. During this review you are gathering valuable information that will allow for a more informed decision regarding taking a case as well as what type of client the employee may be and the type of defendant or types of witnesses you are likely to encounter.

You will need to counsel your clients about the use of social media and its related privacy concerns and how it may be used for or against them. Direct them to review their privacy settings and the social media site's own policies. Ask them to review their list of friends and those with whom they are connected online and to tell you who may have knowledge of any claims and whether that person may be helpful or harmful to the case.

It may be appropriate to remove some of these individuals or restrict their access, especially those connected with the employer or potential defendant(s). It may also be in your client's best interest to stop posting altogether and to clean up any online content. You need to

bring to the client's attention any information posted by an employee about an employer or potential defendant that may open that employee up to counterclaims or attacks on damages. However, you also need to inform the employee of the need to preserve evidence and the potential issues raised by destruction of evidence. Explain that, short of smashing and burning the computer and all of its component parts, it is hard to get rid of its content and it is nearly impossible to take back content that has been posted on social media sights where the content can be used by others, copied, saved, printed, forwarded, or commented on. The Library of Congress is archiving every "tweet" sent out on Twitter.[14]

VI. CONSIDERATIONS FOR ATTORNEY USE

Many attorneys use social media to garner business and for personal use. Consider treating your social networking accounts in the same manner as you do your trust accounts. Do not comingle your clients with personal or business friends, just as you would not comingle client funds with personal funds or general business funds. Wait until you have earned your fee, the Settlement Agreement is signed, and your business is concluded before adding them to your social network. The reason behind this is simple, many employees use social networking to communicate in place of e-mail and you do not want to risk inadvertently destroying the attorney-client privilege by having dialogues with or questions from a client that may be seen by individuals who are not parties to the dispute and in some cases even opposing counsel that are within the attorney's own social network.

VII. CONCLUSION

Social Networking sites have great benefits for both employers and employees. When used correctly, as the name suggests, they are great tools for networking. Employers can

[14] http://blogs.loc.gov/loc/2010/04/how-tweet-it-is-library-acquires-entire-twitter-archive/

advertise their products and services, recruit new employees, gather background information on applicants, and connect with employees. However, certain risks accompany these benefits. As the use of social networking sites continues to increase, employers must be aware of these risks and take, and update, appropriate preventative measures.

SPEAKER CONTACT INFORMATION

Tiffany A. Buckley-Norwood
Dickinson Wright PLLC
500 Woodward Ave, Suite 4000
Detroit, MI 48226-3425
313.223.3470
TBuckley@dickinsonwright.com

Carole D. Bos
Bos & Glazier
990 Monroe
Grand Rapids, MI 49503
616-458-6814
cbos@bosglazier.com

Adam S. Forman
Miller, Canfield, Paddock & Stone, P.L.C.
150 W. Jefferson, Suite 2500
Detroit, Michigan 48226-4415
313-496-7654
forman@millercanfield.com

Jeffrey J. Fraser
Varnum
333 Bridge Street NW
Grand Rapids, Michigan 49504
616-336-6624
jjfraser@varnumlaw.com

Brian E. Koncius
Law Offices of Kathleen L. Bogas, PLLC
31700 Telegraph Road, Suite 160
Bingham Farms, MI 48025
248-502-5000
bkoncius@kbogaslaw.com

SOURCES AND RESOURCES

- AMANDA LENHART ET AL., PEW RESEARCH CENTER, Social Media & Mobile Internet Use Among Teens and Young Adults 17-18 (2010), *available at* http://www.pewinternet.org/~/media//Files/Reports/2010/PIP_Social_Media_and_Young_Adults_Report.pdf

- Cision Executive, Engaging Social Networks: How to Find Your Community, Build Relationships and Gauge Your Influence Online: (November 2008), *available at* http://us.cision.com/assets/whitepapers/Cision_Engaging_Social_Networks_WP.pdf

- DELOITTE LLP, Ethics & Workplace Survey Results: Social Networking and Reputational Risk in the Workplace (2009), *available at* http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/us_2009_ethics_workplace_survey_220509.pdf

- Federal Trade Commission, Using Consumer Reports: What Employers Need to Know, *available at* http://www.ftc.gov/bcp/edu/pubs/business/credit/bus08.shtm

- Nucleus Research, Research Note - Facebook: Measuring the Cost to Business of Notworking (July 2009), *available at* http://nucleusresearch.com/research/notes-and-reports/facebook-measuring-the-cost-to-business-of-social-notworking/

- Patrick R. Martin & Gene Sheih, Tweeting From A Work Meeting Or "Do I Really Have To Friend My Boss?": Emerging Issues Raised By The Use Of Social Networking Sites (2009)

- The Nielsen Company, Global Faces and Networked Places: A Nielson Report on Social Networking's New Global Footprint (March 9, 2009), *available at* http://blog.nielsen.com/nielsenwire/wp-content/uploads/2009/03/nielsen_globalfaces_mar09.pdf

- WorkPlaceMedia, Brand Impact Social Networking Survey (May 2009), *available at* http://www.workplacemedia.com/includes/uploads/pages/Brand%20Impact%20Social%20Networking%20Survey.pdf