BERNSTEIN SHUR

COUNSELORS AT LAW

Do You Want to Be My Friend? Pros, Cons and Traps of Facebook and Other Social Media in the Life Cycle of the Employment Relationship

by,

Ron Schneider, Lori Dwyer & Kai McGintee

Bernstein Shur Labor & Employment Practice Group

May 16, 2012

BERNSTEIN SHUR

COUNSELORS AT LAW

Do You Want to Be My Friend? Pros, Cons and Traps of Facebook and Other Social Media in the Life Cycle of the Employment Relationship

By Ron Schneider | Lori Dwyer | Kai McGintee
Bernstein Shur Labor & Employment Practice Group

Introduction

Social media has ushered in a new frontier of compliance challenges for even the most sophisticated companies and seasoned human resources professionals. The issues arise at the speed of data transfers and in every phase of the employment relationship. It is critical that companies understand the technological infiltration of the professional by the personal and be trained in the legal and business risks posed by social media.

Social media touches every aspect of the contemporary employment relationship, from pre-employment through employment and into the post-employment phase. Companies can no longer avoid social media uses and abuses in the workplace. However, addressing social media use presents companies with an opportunity to engage employees and senior executives in important conversations about company values, the appropriate role of personal information in the workplace and the importance and dangers of technology. This paper focuses on the employment issues and complications that can arise when applicants, employees and ex-employees use (or misuse) social media, and outlines best practices for dealing with the often complex legal and cultural questions that arise as a result of social media use.

What Can Employers Do During the Pre and Post Employment Phase of a Relationship?

a. *Social Media and the Hiring Process*

Social media presents several new opportunities and challenges for the employee screening process. In the hiring process, employers can now obtain more information about applicants through the Internet. In fact, one survey indicates that nearly 80 percent of employers are using social media to screen potential job applicants. Regardless of whether or not that figure is accurate, it is easy to understand why employers would use search engines or social media as a hiring tool given the wealth of information they can yield about candidates in a matter of minutes and at virtually no cost.

"Cybervetting" candidates is not illegal *per se*, nor is there any reported increase in failure-to-hire cases based on information obtained from social media. Still, there are significant legal risks for employers who base hiring decisions on information revealed in an online search. Thus, before entering the brave new world of social media, employers should think carefully about the kind of information they want to obtain about job applicants and how they are going to get it.

Internet sites and social media contain all sorts of information about potential applicants, including their protected status under state and federal discrimination laws. For instance, even though they could never ask in an interview, potential employers may discover a potential candidate's age, marital status, race, national origin, sexual orientation and medical issues simply by checking his or her social networking sites. If the employer decides not to

hire the applicant, he or she could sue the employer alleging that the reason was discriminatory. Moreover, once an employer has accessed this information online, the employer cannot argue in defense of such a claim that it lacked knowledge of the applicant's protected status.

If employers ask third parties to conduct social media searches on candidates, they may also become subject to the Fair Credit Reporting Act. The FCRA requires the consent of the applicant before a potential employer can ask a third party to conduct a background check. Employers that then use the reports of third parties to make an adverse employment decision (i.e. not hiring the applicant) must then make a copy of those reports available to the applicant and give that person an opportunity to respond.

Another risk of using social media and information obtained on the Internet to screen applicants is that the information discovered may be inaccurate or misleading. False information may be posted on blogs and other social networking sites and it is easy to turn up information about the wrong person on the Internet. However, by ignoring disturbing information about a candidate on a social networking site, such as criminal behavior, employers may expose themselves to a negligent hiring claim.

In navigating the risks and benefits of using social media in the hiring process, employers should:

- Decide whether information obtained through social media will be useful to the hiring process based on the particular job position(s) being filled.
- Develop a policy on whether the employer will search the Internet or social media in hiring.
- Perform searches on candidates in a consistent and uniform manner.
- Perform searches on the last two to four applicants after you have most likely met them to help make the final decision.
- Notify applicants, in writing, about the organization's use of social media in the hiring process and give applicants a chance to respond to any negative information obtained if that is the basis for the decision not to hire him or her.
- Designate a non-decision maker to conduct the search who is properly trained to avoid improper access and to screen out information that cannot be lawfully considered in the decision-making process.
- Ensure employment decisions are based on lawful, verified information by making it only one of several sources on which the employer relies for hiring decisions.
- Identify legitimate, non-discriminatory reason for the hiring decision with documentation supporting the decision.

b. Social Media and Post-Employment Issues

Social media issues can also creep into the post-employment relationship between the employer and the former employee. Supervisors and co-workers are increasingly asked to "recommend" former employees on LinkedIn after separation from employment. Supervisors may unintentionally run afoul of the employer's post-employment reference policy by posting a recommendation of a former employee on LinkedIn. An individual supervisor's recommendation on LinkedIn could also conflict with the official position taken by the employer regarding the employee's performance. To avoid such situations, the employer's

general post-employment reference policy should specifically cover recommendations given via social media. Employers may also want to consider adding to their post-employment reference policy a prohibition on managers from "recommending" or commenting on the job performance of former employees on social media without prior specific authorization from the human resources department.

In addition, with the advent of social media networking sites, departing employees are now in a position to disseminate information about their new endeavors and solicit customers in a paperless, cost free and relatively easy manner. Non-compete and non-solicitation agreements should therefore address these possibilities by expressly prohibiting the contacting of clients, vendors or employees via social media. Of course, social media may also have the advantage of allowing employers to monitor the communications of a departing employee in some instances or obtaining useful evidence during the course of a lawsuit.

I. What Should Employers Do During the Employment Relationship to Manage the Use of Social Media?

During the employment relationship, employers have a different set of concerns related to social media use. Employers often confront situations involving an employee's misuse of social media by, for example, harassing or threatening co-workers or management, disparaging the company's products or services or wrongfully disclosing trade secrets or other confidential information. To minimize the legal risk of acting on violations of company policy via the use of social media during the employment relationship, employers should (1) implement a social media use policy, (2) train supervisors and employees (separately) on social media use and company policy, (3) enforce the policy through workplace monitoring and appropriate responses to employee concerns, (4) reinforce the policy periodically with reminders to employees and additional training, and (5) understand the legal risks associated with the technology.

a. Implement a Social Media Use Policy and Train Employees

More than half of employees are social network users and access their accounts at work. Even so, less than one-third of employers have implemented social networking policies. Social networking policies are critical to ensuring the effective use by employees and proper oversight by management, of social media. Importantly, well-crafted policies educate workers and put them on notice of the employer's monitoring practices and expectations.

An appropriate social networking policy must be tailored to each employer's business needs, as there is no one-size-fits all solution. Employers should honestly assess their business culture and risk tolerance and weigh the benefits of social media use against the various risks before developing and implementing a social media use policy. Benefits include enhancing employees' access to cutting edge information and news, helping your employees stay connected with personal and business contacts and ensuring the workforce remains educated on the use of these important new technologies. Disadvantages of social media use include loss in productivity and the potential for its misuse to negatively impact employee relationships.

However the company weighs these considerations, the policy should be developed in conjunction with experienced employment counsel to avoid the many potential legal pitfalls.

In addition, policies should clearly state what employees can do with respect to social media, as well as what they cannot do.

Although there are no one-size fits all solutions, certain key elements are universal. A social media use policy should:

- Instruct employees to use good judgment and take personal and professional responsibility for what they publish online.
- Instruct employees to not post or blog during working time, whether on their personal hand held devices or company-issued devices, unless for official business purposes (unless your company culture or other business reasons warrant a more liberal policy).
- Prohibit employees from using company email addresses to register for social media sites.
- Strongly encourage (but not require) employees to bring work-related complaints to human resources before blogging or posting about such complaints.
- Prohibit posting false or maliciously defamatory information about the company or its employees, customers or affiliates.
- Inform employees that policy covers posts made on personal time, if it relates to work.
- Inform employees that the policy covers posts made on personal devices during the workday.
- State that employees have no expectation of privacy in any communications made on or with company property, including personal communications on their personal webmail and social network pages. Explain how the company's electronic monitoring policy works and exactly what the company reserves the right to monitor.
- Include a "savings clause" which states that the company will not interpret or enforce the policy in a manner that violates state or federal labor laws.
- Reinforce policies by conducting periodic trainings of both employees and supervisors. Management should be trained separately because employers have broader latitude to restrict the use of social media by managers.
- Remind employees that other company policies also apply to social networking regarding work, including EEO, anti-harassment and confidentiality policies.
- Notify employees that violation of social networking policy can be grounds for discipline, up to and including termination.
- Update all existing policies to keep pace with the new technology. Consult with the IT department regularly to coordinate policies with actual practices.

In addition, a workplace policy may:

- Require employees to temporarily and/or permanently suspend posted communications if the employer believes it advisable to ensure compliance with securities regulations or other laws.
- Prohibit the use of social media to post or display comments about coworkers or supervisors or the employer that are vulgar, obscene, threatening, intimidating, harassing or a violation of the Employer's workplace policies

against discrimination, harassment or hostility on account of any of the legally protected categories under state or federal law (gender, disability, etc.).
- Prohibit employees from participating in or conducting any informal reviews of colleagues, supervisors or direct reports on Internet posting sites, such as LinkedIn.
- Prohibit supervisors from "friending" their direct reports, and prohibit retaliation against any employee who declines or ignores a "friend" request from a manager, supervisor or employee to whom they report.
- Ensure that only one person (or office) officially speaks for the company, as long as the policy clearly does not prohibit employees from individually talking with the media about wages or working conditions, activity which is protected by the federal law (see discussion, below, for guidance from the National Labor Relations Board on "protected, concerted activity").

Finally, in promulgating and enforcing social media use policies, public employers have some unique considerations and risks. They must ensure they do not infringe free speech rights in the text and enforcement of their policies and they need to be aware of the heighted privacy concerns in light of U.S. and Maine Constitutional protections.

b. Enforce the Social Media Use Policy

Once an employer issues a social media use policy and trains employees, it should monitor use and enforce the policy. This is critical, as lax enforcement can lead courts to find a "waiver" of the employer's right under the policy and potentially reverse a challenged employment action taken on the basis of a violation of the social media use policy. Enforcement is therefore critical to ensure employers are able to avoid or quickly address situations such as the following:

- An employee commits a tort via social networks. For example, an employee's Facebook post might defame another company's product, threaten a co-worker, supplier or other business associate with violence, etc. Employers could be held liable for any of these activities if they are or should be aware of them and fail to correct the problem.
- An employee violates a contract via social networks. For example, the employee might disclose confidential information of a third-party business partner in violation of a business contract. The employee might also violate her own non-solicitation or non-competition agreement by individually soliciting the company's clients for work outside her official duties.

- An employee violates anti-discrimination laws via social networks.
- An employee commits a crime via social networks on workplace computers or during working time. For example, an employee may engage in unlawful sexual communications with minors via Facebook, view pornography or otherwise engage in criminal activity. If employers are monitoring workplace activity, they could be held liable for negligent supervision if they fail to take action against employees engaging in such behavior during working time.

In addition, employers may discipline employees for their off-duty use of social media if the conduct implicates the employee's job, assuming the information being used as the basis for

discipline was obtained lawfully (i.e., not by unauthorized access to a password protected site), and the employer determines that the conduct is not protected, concerted activity under the National Labor Relations Act (see further discussion of NLRA below). Courts have upheld an employer's discipline of employees when the employee's postings on a social network site exploited the employer's image or products or contained threats of violence.

Finally, a word of caution regarding monitoring and accessing information, provided employers put employees on notice that they will monitor the use of workplace electronic communications, they can generally view employees' Internet usage and other electronic information accessed through the employer's computer systems that is stored on the employer's servers. However, the federal Wiretap Act (part of the Electronic Communications Privacy Act or "ECPA") prohibits the actual or attempted interception of any wire, oral or electronic communications without express authorization. Enacted to protect people's expectation of privacy in electronic communications, the Wiretap Act, again part of the ECPA, provides stiff civil and criminal penalties for violations. Importantly, aggrieved parties in Wiretap Act cases need not show any harm as a result of the violation. If a violation is proved, an aggrieved party can recover a minimum award of $10,000 or $100/day of violation, whichever is greater. In addition, individual employees (officers, supervisors, etc.) as well as the company can be subject to criminal charges.

Plaintiff/employees are increasingly alleging Wiretap Act violations against their employers, either by affirmatively bringing claims against the employer or to suppress evidence collected unlawfully by the employer that the employer tries to use against the employee in court. In light of these developments, employers that engage in real-time, content-based monitoring of their employees' computer use in the workplace or who activate the auto-forwarding e-mail feature to monitor a particular employee's activities, must understand that they could be in violation of the Wiretap Act if they do not provide explicit notice of the company's monitoring practices. Courts will not lightly imply consent to this type of monitoring. Employers must provide clear disclosures, describing precisely the form of monitoring the company employs. Additionally, employees should be required to sign an annual acknowledgement of the electronic communications policy, acknowledging their understanding of and consent to the company's monitoring practices.

Finally, employers should avoid accessing information stored on third party servers, unless they have clear authorization to do so. Employers may not force employees to provide passwords to password-protected social media sites or they risk violating the Stored Communications Act, nor can they access those servers in a deceptive manner. In one case out of New Jersey (2008), a supervisor asked one of his employees to show him a password-protected MySpace page, from which he learned information later used against another employee in a disciplinary process. Although the employee did not object at the time and voluntarily gave the password to her supervisor, she later testified that she felt "coerced" because the request came from her supervisor. The jury found against the employer in that case and the federal district court upheld the jury's verdict, awarding damages to the employee under the Stored Communications Act on grounds that the employer did not have authorization to view the MySpace page.

II. What May Employees Do That Employers Wish Employees Would Not Do?

As employers have struggled to control the negative effects of social media in the workplace with policies and discipline for inappropriate behavior, the National Labor Relations Board has

stepped into the fray to protect employees even when the employees have engaged in what many would consider inappropriate online behavior. The National Labor Relations Act protects any employee, regardless of whether the employee belongs to a union, from being disciplined for engaging in "concerted activity." Specifically, Section 7 of the NLRA provides, "Employees shall have the right ..... 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 ...." 29 USC § 157. Employers will be surprised at what the NLRB presently seeks to protect pursuant to Section 7.

First, to be protected, an employee's activity must be undertaken by two or more employees or by one employee with the authority of others. The employee could also engage in a call to group action. However, activity taken solely by and on behalf of the employee alone is not protected because an employee's conduct is not "concerted" unless it is engaged in with or on authority of other employees or for the purposes of inducing group activity. An expression of a personal complaint that does not concern the rest of the workforce is not concerted activity.

The activity must also be for the "mutual aid and protection," which means that the activity must relate to the terms and conditions of employment. The conduct must be reasonably related to wages, hours or other terms and conditions of employment, such as co-worker or supervisor performance that adversely affects the working conditions. Activity that does not bear a reasonable relationship to the conditions of employment is not protected. For example, complaints about the quality of an employer's product or service would not be considered activity related to the terms and conditions of employment.

It is very important to understand that the NLRB construes Section 7 rights very broadly. In other words, when deciding whether an employee's conduct constitutes "protected concerted activity" the NLRB seems inclined to resolve close questions in favor of the employee. By contrast, the NLRB applies exceptions to Section 7 protections very narrowly.

To be clear, an employee may lose Section 7 protection if the employee engaged in "opprobrious conduct." Again, the NLRB narrowly construes the meaning of what conduct is consider opprobrious, that is conduct so indefensible, abusive, egregious or flagrant, such that the employee loses his Section 7 protection. The decision as to whether the employee has crossed that line depends on several factors:

(1) The place of the discussion;
(2) the subject matter of the discussion;
(3) the nature of the employee's outburst; and
(4) whether the outburst was, in any, way provoked by an employer's unfair labor practice

The employee may not make statements that are extremely disloyal, reckless or maliciously untrue. The NLRB has not found many statements to be so problematic as to cost the employee his Section 7 protection. Employees have been allowed to call their supervisors explicit and demeaning names. For employers, such construction of the law may seem disheartening.

Employees, however, are not entitled to make disparaging comments about an employer or its products in the context of appeals to outside or third parties, i.e. friends but not co-

workers. But, the NLRB has concluded that an employee is not appealing to third parties when her Facebook friends simply "overhear" her conversation with her co-workers. Even though an employee might post disparaging remarks about her employer on her Facebook wall and even though those posts are pushed to the "walls" of her, say, 340 "friends" only 10 of whom are co-workers, the NLRB might not consider her posts to be an appeal to third parties, which would be unprotected, so long as the posts were not specifically directed toward third parties and not designed to harm the employer independent of her complaints about her working conditions. The NLRB seems to continue to support the fiction that people's Facebook "friends" are real friends or people an employee actually knows and not in many instances the equivalent of the general public.

With respect to social media policies, the NLRB has concluded that policy provisions that restrict or chill protected concerted activity are unfair labor practices. Generally, policy provisions that are categorical in their restrictions could present problems for employers. The NLRB has struck down policy provisions that restrict employees from:

- Making disparaging, defamatory, embarrassing or harassing remarks or engaging in "inappropriate discussions" about the company, management, coworkers and/or competitors, without including limiting language informing employees of their Section 7 rights.
- Posting pictures of themselves in any media which depict the company in any way (including company uniforms, corporate logos, etc.) without company permission.
- Posting pictures of or comments about the company or its employees that could be construed as "inappropriate."
- Using any social media that may "violate, compromise, or disregard the privacy or confidentiality of any person or entity."
- Using the company name, address or other information on their personal profiles.
- Posting anything that they would not want their manager or supervisor to see or that would put their job in jeopardy.
- Publishing any representation about the company without prior approval by senior management and the law department.
- Requiring that all social media communications be made in an honest, professional and appropriate manner, without defamatory or inflammatory comments regarding the company, management, employees, customers, suppliers or contractors.
- Requiring that employees who identify themselves as employees of the company on social media expressly state that their comments are their personal opinions and not those of the Employer.

The major problem with the above policy provisions is that they were stated and applied categorically.

Whether a policy actually runs afoul of the law depends on how the policy is drafted and applied. For example, whether an employer can prevent an employee from using its company name or logo on Facebook depends on the circumstances. If the employee uses the company logo as she displays a photo of herself while she pickets outside her place of business, such behavior cannot be restricted. But, if the employee identifies herself as working for a company and posts a photo of herself dressed in a company t-shirt standing in front of a Nazi flag, the employee could be disciplined for that conduct, especially if she were warned that using the company logo on Facebook could be a problem depending on the circumstances.

Policy provisions should seek to educate and advise employees of the possible consequences of their online behavior depending on the circumstances and context of their action.

Not all is lost despite the NLRB's broad application of Section 7 rights and its narrow application of exceptions that would protect the employer. While employers must be careful and examine the context and the circumstances of each situation before disciplining or terminating an employee for online behavior, it is probably fair to say that when employees use social media improperly, many, if not most of them, use it to serve their own individualistic and personal desire to rant with no attempt to engage in a call to group action. Employees also continue to use social media to post inappropriate pictures and other content that are unrelated to working conditions. The clearest rule for any employer to follow is to investigate, understand the context and circumstances of an employee's posts and to consult with legal counsel before making a decision about how to deal with social media behavior that the employer does not like.

This paper is not intended as legal advice to any client and receipt of it does not create an attorney-client relationship.