

Legal Update

November 2009

Social Media and Employment Practices – From Hiring to Firing, and Potential Pitfalls Along the Way

By Orley Moskovits Desser

Last month, we published the first in a series of *Legal Updates* discussing legal issues surrounding social media. Our first *Legal Update* provided an overview of social media's intersection with employment law, confidential information and intellectual property, as well as issues relating to publication and deceptive practices. This *Legal Update* focuses on the impact of social media in the workplace –from hiring to firing, and potential pitfalls along the way.

As lawyers, it would be easy for us to cite the unique risks posed by use of social media in the workplace as cause to recommend prohibiting the practice altogether. For many businesses, however, such advice would be unrealistic and regressive. Social media is here to stay, and since employees are online, employers should also be online – but cautiously. With exercise of care and good judgment, employers can and should have a positive view toward how social media can be used in the workplace.

Screening Candidates

With just a few keystrokes, employers can gather self-published and uncensored online information about a prospective hire (or current employee). The employer can learn about an individual's experience, reputation, and possibly the person's proclivity for wild escapades, violent tendencies, or illicit drug use. By using social media to discover information about a candidate, employers may not only decrease the likelihood of hiring an individual that lied on his or her resume, but also reduce risks and costs associated with a bad hire.

While investigating potential hires this way may seem productive, employers must be careful when using Facebook, LinkedIn, MySpace, Twitter or other Internet sites or search engines such as Google to recruit new talent or weed out weak candidates. Employers using social media to screen applicants may expose themselves to potential discrimination claims by discovering otherwise unavailable information regarding an applicant's disability, age, race, religion, sexual orientation, or other information that places the applicant in a protected class. Further, an employer may discover information about a candidate's past work history – such as an applicant's workers' compensation claim or discrimination charge or lawsuit against a former employer – that, if used to reject an applicant, could put the employer at risk for a retaliation or discrimination claim. Since information off-limits in the hiring process may be featured prominently online, an employer who comes across a candidate's personal web page may be hard-pressed to deny that such information influenced the

FVLD®

hiring decision. Indeed, many social media websites enable users to readily track who accesses their personal pages for a period of time.

If an employer desires to browse the Internet to screen candidates, the best practice may be to (i) identify the type of information the employer can legally use, (ii) screen candidates uniformly, and (iii) if possible, use a neutral third party to search for and filter out information from the employers' reach which could lead to an allegation of discrimination. Although it may be impractical or counterproductive, employers may also consider obtaining a candidate's written consent to search social media sources.

Monitoring Employees

Employers should similarly tread cautiously when using social media to learn about current employees and basing personnel decisions on any findings. While certain online activities may be unlawful and a good reason for termination, other online activities – while potentially inconsistent with an employer's taste, culture or ideology – may expose the employer to a charge for wrongful termination. For example, an employer would probably be justified in terminating the employment of an employee who disseminated confidential business information, used the Internet to harass other employees, accessed illegal websites, or posted content damaging to the employer's reputation.

Indeed, in some circumstances, checking current employees' online activities may help employers fend off claims for employees' unlawful use of company property. In *Doe v. XYZ Corporation*, for example a New Jersey appellate court permitted a plaintiff to proceed to trial against her ex-husband's employer after the plaintiff discovered that her ex-husband (the employee) had used a company computer to post nude photos of his step-daughter. The plaintiff's negligence claim against the employer was based on allegations that even though the employer knew its employee was accessing pornography at work, it failed to affirmatively take action to stop the online conduct and report the illicit behavior to law enforcement authorities. (If this case were in Illinois, the employer would also be in violation of the Illinois Abused and Neglected Child Reporting Act, which requires employers to report child pornography discovered on work computers.)

An employer, however, who terminates the employment of an employee in a protected class because the employer discovers online information that is lawful, but tasteless or contrary to the employer's culture – but not other employees who do the same – may face a charge of discrimination or wrongful discharge. Indeed, some states, including Illinois, have laws (such as the Illinois Right to Privacy in the Workplace Act) expressly prohibiting employment discrimination based upon an employee's use of lawful products (*e.g.*, smoking cigarettes) provided such use is “off the clock” and not at the workplace.

Furthermore, accessing employees' restricted websites without permission may also expose an employer to liability. Recently, a federal jury in New Jersey found that an employer violated the Stored Communications Act (prohibiting unauthorized access to electronic communications) and other privacy laws by accessing a password-protected website where employees vented about their

FVLD®

employer. The employer claimed an employee voluntarily shared a password, but the jury was not impressed and decided the password was “shared” under duress by an employee who feared for her job.

An employer seeking to satisfy its curiosity may be able to do so to some extent by accessing e-mails and web activity conducted on company-operated networks. In other words, if the employer provides the service to store the electronic information, the employer may monitor the employees’ use thereof. Of course, this does not include third-party websites servers or e-mail (like Facebook or Gmail). As one court held earlier this year, an employee suing under the Stored Communications Act may recover punitive damages from an employer for impermissibly logging on to the employee’s personal AOL e-mail account (even if the employee suffered no actual damages). A prudent employer will not only inform employees that company equipment and networks will be monitored but also will obtain employees’ acknowledgment that the employer is engaged in such monitoring. Of course, if, despite the risks, the employer wants to access an employee’s non-password protected social networking site, the employer should, at the very least, confirm that it is not violating the terms and condition of the site.

Recommending Former Employees

Social media poses another potential pitfall for employers after an employee’s employment has ended. Users of websites like LinkedIn can “invite” friends, colleagues, acquaintances, former employers (and anyone else) to post recommendations on their profiles for other users, including prospective employers, to view. While accepting such a request to post a note may seem harmless and greatly advantageous to a “recommendee,” it can be risky to the “recommender.”

Even outside of the “Web 2.0” context, employee references may expose an employer to defamation suits (when providing negative information) or discrimination suits (when providing positive references after terminating an employee due to poor job performance). Posting a recommendation online, however, carries this risk to an even greater extent since the recommendation is publicly available.

Employers should also be mindful that separated employees, particularly those separated for “cause,” will often approach their former colleagues employed in non-management capacities for online recommendations on job performance. Because of the informal nature of an online recommendation, the recommender may not deem it necessary to consult with a superior before complying with recommendee’s request. This scenario could be problematic for the employer. For example, if the employee was discharged for poor performance, a positive online reference from the employer or a former employee (especially one in a management position) could undermine the reason for termination and be used as evidence of wrongful termination. To avoid this problem, we strongly suggest that employers implement and enforce a “name, rank, and serial number” policy in the workplace that, in response to a request for a job reference, an employer will only provide dates of employment position and compensation. Employers should make clear to their employees that all reference requests should be referred to management, and mention that posting references for



employees and former employees on social media websites such as LinkedIn would violate their policy.

A Few Parting Suggestions

Social media, if used unwisely at each stage of an employment relationship, may expose an employer to potential liability. There are, however, many benefits (such as camaraderie and business development) to allowing social media in the workplace. Implementing a policy specifically addressing use of social media in the workplace by the employer, on the one hand, and by employees on the other hand, may be the best way to protect the employer. A policy for the employer should cover use of social media in employment decisions and parameters for accessing employee websites; whereas a policy for the employees should cover matters such as employee use of social media during working hours, a description of misuse of social media, and consequences of such misuse. Legal counsel should be consulted in preparing a social media policy so that it fits the unique culture and particular needs of the employer.

FVLD publishes updates on legal issues and summaries of legal topics for its clients and friends. They are merely informational and do not constitute legal advice. We welcome comments or questions. If we can be of assistance, please call or write Jon Vegosen 312.701.6860 jvegosen@fvldlaw.com, Jim Groth 312.701.6830 jgroth@fvldlaw.com, Neil Rosenbaum 312.701.6824 nrosenbaum@fvldlaw.com, Orley Desser 312.701.6873 odesser@fvldlaw.com or your regular FVLD contact.

FVLD®

© 2009, Funkhouser Vegosen Liebman & Dunn Ltd.
All rights reserved.