

INTERNET

## Proceed with caution: social networking websites and blogs

Faced with huge numbers of job applicants, an increasingly Internet-tethered workforce, and the reality of an Internet-dominated world at large, employers are at a crossroads. Social networking sites and blogs are useful to gather information about potential and current employees, as a means of keeping the workforce engaged, and to communicate the company message. But in light of the largely uncharted legal landscape, employers and employees alike should exercise caution when turning to the World Wide Web for employment-related purposes.

### Inside

Legal risks and best practices associated with employment-related use of Internet social networking sites and blogs are the subject of comments by:

- **Dennis J. Merley**, Felhaber, Larson, Fenlon and Vogt, PA, Minneapolis, MN. Merley has devoted his 27 years of practice to advising management on a broad range of work place issues, including employment discrimination, harassment claims, disability accommodation, wrongful termination, minimum wage and overtime, downsizing, severance agreements, unemployment compensation, drug and alcohol testing, the FMLA, and affirmative action.
- **Paul W. Mollica**, Meites, Mulder, Mollica & Glink. Mollica and his firm have represented plaintiffs in class, collective and public interest litigation covering all aspects of the federal civil rights laws (including employment, constitutional and voting rights, housing and public accommodations), as well as ERISA, securities, qui tam, insurance law and other complex litigation.

### Trolling social networking sites

**Many employers utilize social networking websites such as MySpace and Facebook to gather additional information about job candidates or existing employees. Why do employers troll these websites? What benefits do they hope to gain?**

“Using social networking sites can provide an unfiltered look at the applicant in a context that is perhaps more genuine than the standard pre-employment process,” explains attorney Dennis J. Merley of Felhaber, Larson, Fenlon and Vogt, PA in Minneapolis. “Pre-employment procedures often fail to elicit much in the way of true insight into the applicant’s personality, characteristics and attitudes.” Merley also points out that interview responses are often well rehearsed, resumes heavily polished, and references rarely given.

Website trolling is a method employed by individuals who are used to getting their information from the Internet, observes Paul W. Mollica, partner in the firm of Meites, Mulder, Mollica & Glink of Chicago. These employers “are looking for possible warning signs (arrest records, disciplinary actions, court-martials, lewdness or drunken activity) and a ‘truer’ picture of who the candidate is,” he explains.

### Legal risks

**Although the upside to trolling social networking websites for information about job candidates and existing employees may seem obvious, what are the legal risks associated with the practice?**

“The downside,” cautions Mollica, “is you expose yourself to information that you shouldn’t necessarily have, such as age, religion, pregnancy, sexual orientation, and disability status.” In fact, antidiscrimination statutes may be implicated by such trolling in several ways, agrees Merley. Pictures posted on the site provide information to the employer regarding certain of the applicant’s protected classification such as race and gender.

**Early knowledge of protected class.** Moreover, the Facebook “Basic Information” template includes spaces for an individual’s age, sexual orientation and religion. “By acquiring this information early in the process, employers lose the opportunity to defend refusal to hire claims based on the

absence of knowledge regarding protected class,” he advises. “If you don’t know an applicant’s race or religion, you can’t intentionally discriminate on that basis.”

**Different treatment.** Employers may also face problems if they have searched social networking and other Internet resources for one particular group, but not others, Merley suggests. “If female applicants were evaluated in this way but not male applicants, an inference of sex discrimination might arise. Similarly, if the employer drew different conclusions from similar postings (e.g., Caucasians are ‘assertive’ or ‘forceful’; African-Americans are ‘militant’), a discrimination claim might be in the making.” While these claims may be difficult to prove, as are most failure to hire claims, they should be anticipated and prevented, Merley advises.

**Online trail.** Moreover, there is “a tangible risk” that if the hiring manager leaves an online trail, as is practically inevitable, the employer could get hit with an antidiscrimination or retaliation charge for looking up this information and then not hiring or promoting the individual, Mollica points out.

**Other laws may be implicated.** Some of the other legal risks include the Fair Credit Reporting Act, which probably would be implicated if the search was performed by a third party, Merley advises. It is difficult to generalize as to whether the practice of trolling social network sites for background information implicates privacy laws because they differ markedly from state to state.

“However, one of the standard formulations of the tort of invasion of privacy is an ‘intrusion into seclusion,’ *i.e.*, intrusion into one’s private affairs in a manner that would be highly offensive to the reasonable person,” instructs Merley. “Of course, it seems likely that a reasonable person would not expect content on an Internet site to be all that private,” he notes. “Even social networking sites that have various levels of privacy are inherently public since they are intended to be seen by other people.”

## Benefits vs risks analysis

**Are the benefits employers hope to gain by trolling social networking sites outweighed by the legal risks associated with the practice?**

“The law in this area is relatively undeveloped, and a reasonable search into social networking sites and other Internet resources does not seem to involve any practices that were not already being used prior to their advent,” Merley notes. “Criminal background investigations, reference requests and other sorts of background searches have been around for a long time – the Internet just carries the search a little further.”

Mollica illustrates the dilemma for employers. For example, an individual is hired or promoted to a sensitive position and the employer discovers only later that the individual had a notorious track record. “Imagine some awful incident involving an employee, only to discover after the fact that the information about that employee’s criminal or other history was easily discovered online,” he hypothesizes.

## Policies and best practices

There are a few guidelines that employers should consider implementing in order to limit or avoid legal exposure associated with the practice of trolling. Merley recommends that employers maintain a policy addressing this recruitment technique. “The policy should disavow any interest in protected class information, excessively private data or other potentially illegal or inappropriate information,” he advises. Moreover, recruitment staff should be trained on how to conduct proper searches and required to screen out improper information before the applicant is referred for further pre-hiring consideration, he suggests.

“Employers should also avoid creating false identities to ‘friend’ applicants or solicit information from them, limit searches to job-related matters and avoid jumping to conclusions about the content being accessed,” Merley instructs. For example, he notes that many of an employer’s most successful employees go to large parties on the weekend – why should employers expect applicants not to do so?

Documenting recruitment efforts is also recommended by both attorneys. “Maintaining records of what sites were reviewed will help dispel a claim that different standards are employed for different groups,” notes Merley.

**Professional networking sites.** Merley and Mollica agree that the same legal risks apply when employers troll professional networking sites like LinkedIn. “However, there might be a greater chance that an applicant could claim to have been misled into divulging private information because they thought they were interacting with a networking peer when it was actually an employer’s recruitment staff member,” Merley points out.

“If employers are going to allow their agents to use the Internet to investigate employees and applicants, then they should choose the sites they’re allowed to visit and keep records,” suggests Mollica. Otherwise, it’s like having the “file” and then a second backed up file showing the search, which lends “a hint of skulduggery to even an innocent job search,” Mollica explains.

*If employers are going to allow their agents to use the Internet to investigate employees and applicants, then they should choose the sites they’re allowed to visit and keep records.*

**PAUL W. MOLLIKA**

**Labor Law Reports *Insight***

EDITOR: Pamela Wolf, JD

*Most importantly, employers have a legitimate interest in what employees say about them and what they do to impact or undermine the business.*

**DENNIS J. MERLEY**

### **A word of caution to users**

#### **What are the pitfalls for social networking site users?**

These same pitfalls confront social networking site users, and even worse, Mollica suggests. Social networking sites “are where people (communicating socially) are most likely to communicate facts about themselves that employers should never know covertly,” he observes.

“Individuals should screen their networking sites and other Internet resources to insure that all unflattering or inappropriate material has been removed,”

Merley advises. “Ask friends to remove such items from their sites as well, especially tagged pictures that might be too revealing or subject to misinterpretation.”

**Be careful what you say.** Moreover, Merley implores users to be very careful of what they say and to whom, and above all else, not to denigrate their current employer in any manner. “Employers have a right to expect that their employees won’t undermine them in the outside world, and future employers will be unimpressed by applicants who have bad-mouthed their current or previous employers,” he advises. “In short, remember that your online life is very much a part of an extended job interview and you should work hard to put forth the best possible image of yourself.”

### **User discrimination lawsuits**

A job applicant who believes he or she was rejected by an employer based on unlawful criteria obtained from social networking sites, such as race, sex or religion, may resort to filing a discrimination claim. But, like all other refusal to hire cases, those rooted in Internet trolling practices can be difficult to prove, Merley notes.

“Employers always have a wealth of data to evaluate in the hiring context and often have several very well qualified applicants from which to pick.” Moreover, employers are well versed on what characteristics are off limits for consideration in hiring and employment decisions, he points out. “Although the Internet might make it easier to learn an applicant’s race or religion, I don’t think many employers actually care to use those factors as hiring criteria,” Merley observes. “Therefore, easier access to that information may require the employer to work a little harder or longer to dispel the notion that the information influenced a hiring decision.” But ultimately, assuming that protected class information did not contribute to the employment decision, the employer should still prevail, Merley opines.

**E-discovery issues.** Mollica points out that in the event of a lawsuit, the employer will be subjected to very intrusive e-discovery about the hiring process, and all electronics used by people in charge of the decision during that period. “Since some statutes and regulations specifically ban inquiries into particular areas, the very search itself might violate the law,” he cautions.

### **Social networking during work hours**

#### **Should employers permit employees to visit social networking sites during work hours using employer-owned equipment?**

“These sites can be extremely valuable in making a quality hire and for enhancing professional interaction by employees,” Merley observes. Social networking sites can expose current employees to new ideas and innovative solutions to workplace issues, and help generate referrals of qualified applicants for existing or future vacancies, he points out. Employers can also present a very positive image through interaction on these sites.

Banning employee use of social networking sites is “a double-edged sword,” according to Merley. On the one hand, these sites can be very useful to employees as a means of keeping updated in their industries. They also help employers present a positive company image and recruit new employees. “On the other hand, they can lead to substantial unproductive time and perhaps some real problems in the area of harassment, defamation, or misuse of trade secrets if employees misbehave on these sites,” he cautions.

**Monitor employee use.** Employers should monitor social networking sites regularly, Merley advises. Employers need to know what employees are doing, whether it is a productive use of their time, and whether they are behaving inappropriately. “They also need to engage in ORM—Online Reputation Management—to see (and perhaps respond to) what is being said about them, especially by their own employees.”

“Employers should always make sure their employees know that their use of company computers and Internet connections are subject to monitoring,” Merley suggests. “In addition, employees must be advised not to engage in unlawful or harmful practices, such as harassment or discrimination, disclosure of trade secrets, and defamation.” Employees should also be restricted in their use of the company name or identifiers, and should be reminded to issue disclaimers that they speak for themselves, not the employer, he adds.

### **Employee postings on websites and blogs**

**Reactions to negative postings. What can or should employers do if they learn that an employee has posted embarrassing or negative work-related information on a website, or even on YouTube? What lessons can we learn from the case of the two Dominos employees who posted YouTube videos of themselves engaging in conduct that included health law violations, and their employer’s response?**

Mollica suggests that employers may legitimately need to watch out for such things as theft of proprietary information or trade secrets, defamation, and Lanham Act (Trade Secrets Act) violations. “But where the video is purely parody and poses no legal threat, the issue then becomes consistency – is the employer meting out the same penalties to all people committing the same violation, or singling out some folks for unlawful retaliatory or discriminatory reasons (such as whistleblowing)?” There is also “a whole PR problem of how customers may respond to an overreaction,” Mollica warns.

The best lesson, according to Merley, is not to do anything that might cause embarrassment. “With cell phone cameras, Blackberries and the like, an embarrassing or harmful moment can be recorded and broadcast to the community in a matter of seconds,” he points out. “Beyond that, employers should be clear in identifying prohibited conduct and spelling out the consequences of such conduct, and then monitor what people say and do that affects their business or reputation, just as they did in the era before computers,” Mollica advises.

**Taking disciplinary action.** The risks associated with taking disciplinary action against employees who have posted unflattering material about their workplaces on the Internet are really not that different from those associated with other areas of employee behavior, Merley notes, reminding that private sector employers are not impacted by free speech issues—those protections only relate to the government. He also points out that whistleblower laws tend to protect only reports of misconduct or illegal activities to legal authorities; generalized complaining or accusations are typically unprotected.

“Most importantly, employers have a legitimate interest in what employees say about them and what they do to impact or undermine the business,” Merley advises. “While employees should not be expected to be walking infomercials for the company, it seems reasonable to expect that they will not intentionally undermine the company by publicizing their grievances or badmouthing them, or by engaging in behaviors that are conflicts of interest.” Merley cites the case of a Microsoft employee who was discharged for advocating the use of Macs on a blog – why should Microsoft ignore something like that?

**Best practices.** Merley offers two suggestions for employers’ consideration when developing policies regarding employee postings of work-related information on Internet websites and blogs:

- First, such information should be posted only if it is done for the purpose of the employee accomplishing his or her job responsibilities.
- Second, employees must not divulge confidential information or act in any manner that would be a conflict of interest.

### Employer-sponsored blogs

More and more employers are venturing into the territory of employer-sponsored blogs, both internal and external. But

similar to other modes of Internet communication, employer-sponsored blogs provide both opportunities and risks of harm.

**Internal blogs.** What are the benefits and pitfalls related to internal employer-sponsored blogs? “These can be valuable tools for enhancing the flow of information between departments or geographically separated employees,” Merley points out. “They also can build a sense of community among employees, and can be a powerful recruitment tool if applicants are permitted to participate and learn about the company from its employees.”

Merley notes that the policies affecting internal blogs and networking sites are essentially the same as those pertaining to use of other social networking sites and Internet resources, but the risk of some harms may be diminished—such as public disclosure of trade secrets – while the risk of others – such as sexual harassment – might be increased.

**External blogs.** Most of the issues that apply when considering whether to sponsor an external blog are the same as those related to internal blogs, but with the “added concern that the company might be seen as endorsing statements or conduct taking place on the blog,” Merley cautions. “The employer would have to be vigilant in monitoring activity on the blog.” As to best practices, Merley suggests they are the same for internal and external blogs. “The vigilance in monitoring the blog should be greater but the methods for doing so don’t appear to differ.”

### Clarify expectations

“Because these are still largely uncharted waters, employers should make sure they have clearly spelled out the behaviors that they expect of their employees,” Merley advises. “There are a great many opinions out there as to what behavior is public or private, and it can be expected that employees and employers will differ on that issue. As a result, employers should be very clear in articulating, for example, that even if employees are blogging on their own time, on their own computers, and in their own home, the content may still be work-related if it affects the company or its business position.” Employees should also be properly advised as to what they can and can not do while acting on the company’s behalf, Merley urges.

### Stay tuned

There is much yet to be explored in the area of social networking sites and blogs. “For example, would a Facebook site encouraging people to work for a current employee be considered a violation of an agreement not to solicit former coworkers? Would it matter who is on the person’s ‘Friends’ list?” Merley asks. Another open question is whether there is a difference between an employee’s behavior in real life and his otherwise offending behavior in his ‘Second Life’? “There’s a lot more to come on this subject,” Merley assures us. ■