



Brought to you by the TemPositions Group of Companies - www.tempositions.com

Social Media: Asset or Liability?

By Anne DeAcetis
May 27, 2011

It's a fact: most working professionals today use social media. And employers have the right to regulate its use. Before companies permit HR to use information available through social media platforms to evaluate candidates, or allow employees to spend time online, they must educate themselves on the benefits and legal risks—and establish clear, carefully-considered policies.

Richard H. Block, Esq., a widely recognized expert in labor and employment law, and his longtime associate, Jessica Catlow, Esq., visited TemPositions' HR Roundtable series on Thursday, April 28, 2011 to talk about the legal realities surrounding social media in the workplace. Together, they helped attendees analyze the pluses and minuses, and they offered practical tips for avoiding unlawful behaviors.

Block began by taking a quick poll. By a show of hands, he asked attendees to indicate if they used social media for a) personal activities, b) a mix of personal and professional activities, or c) professional tasks only. Most attendees raised their hands to indicate broad personal use, but very few raised their hands to indicate purely professional use. This result, he noted, illustrates just how new social media is to the HR toolbox.

Catlow then stepped in to ask attendees about the personal privacy settings on their social media accounts. Most attendees said they'd made some effort to safeguard their privacy online. But many also acknowledged they weren't 100% clear on their options, or how contacts' settings might affect them.

Privacy settings can be complicated, Catlow explained. But in the interest of leading by example, HR professionals should find out what others can discover about them via a simple Google search. They'll quickly find out whether their privacy settings provide adequate protection, and they may also discover which contacts do not safeguard their information.

Catlow then led the group through a summary of leading social media sites. Each, she explained, fills a specific online niche and reveals different types of information about users.

Twitter

With 190 million users, Twitter is currently the world's largest social media platform. As Catlow described it, it's a "microblogging service." Users post short messages called "Tweets" (limited

to 140 characters) to share information about recent activities or thoughts, or to post photos or links to other sites.

Twitter's default settings allow full public visibility of all Tweets. But users can restrict access to users they know and approve, called "followers."

Facebook

Facebook is another social media giant, with over 150 million worldwide users. Facebook describes itself as a "social utility," and Catlow noted its many interactive tools. Users can post personal notes and share images/links on each other's Facebook "walls." Through the site, they can send each other private emails and event invitations. There's space for large online photo and video collections, as well as longer texts called "notes."

Facebook also enables users to organize themselves into "groups." Users can join these online communities based on where they live or work, or where they were educated. Other groups are created around common interests, hobbies or causes. A number of Facebook-based games require multiple users to play as a community.

Facebook's privacy settings are complex, and the site frequently vexes its users by revising options and resetting preferences. The company advocates transparency, so its default settings grant broad access to users' information. But by changing these settings, users can restrict access to their personal information, comments and posts, photos, videos, etc. to "friends" and/or friends of friends. It's even possible to hide a Facebook profile from Google searches.

Friends' settings do impact your privacy, Catlow warned. In particular, access to "tagged" photos (images with names attached) can be hard to control. Photos you post within your own account may be protected. But if a friend with fewer privacy restrictions posts and tags a photo of you, it may be available for broader view. You must either prohibit all parties from tagging you—or stay vigilant, removing tags from any photos you wouldn't want the world to see.

LinkedIn

LinkedIn, which Catlow described as "Facebook for professionals," has over 101 million global users. It's an interactive site designed for purely business-related communications. Each user's network is made up of "contacts," not friends. And all the site's tools are intended to help users sell their services and expand their networks.

Profiles detail a user's professional background, education and expertise. But each page is more than an online resume. Users can include narratives about their experience and describe the kind of work they'd like to do. They can ask contacts for recommendations to appear on their profiles, which they can review and approve before they're posted. They can also interact with others in their network to pursue work or make referrals.

Again, users can choose how private or public they want their information to be. A LinkedIn profile can be fully visible to the general public, or information can be restricted to approved contacts.

Companies can also maintain LinkedIn profiles and connect to online employees, using the site for communications or to request employment referrals. They can also enforce standards. One attendee told the group that her company requires employees with LinkedIn profiles to follow a basic, HR-approved template.

Block interjected to note how useful LinkedIn can be for job-seekers. The site recommends contacts that might be relevant to you. And like Facebook, LinkedIn includes groups. The site can instantly connect users with common interests, priorities or ventures.

FourSquare

FourSquare is one of the newest social media platforms, with approximately four million users worldwide. Unlike the others, it's location-based. Users "check in" to different places (e.g., Grand Central Station), using the service to let their networks know where they are.

Users can post reviews about the businesses and locations they visit, and they can compete with one another for FourSquare honors. Visitors to a given Starbucks, for example, can earn "badges" and vie to become "Mayor" by returning repeatedly. (Businesses have embraced FourSquare, offering special discounts or giveaways to people who check in at their stores.)

Understandably, FourSquare offers fewer privacy settings. The service exists to help its users share their locations, and those who don't want this information widely known don't sign up.

FourSquare may be most interesting, Catlow noted, as a case study in the internet's ongoing evolution. The first web sites, examples of "Internet 1.0," broadcast information. But they didn't offer interactivity or create communities. As part of "Internet 2.0," web sites have become places where people socialize. FourSquare, simple though it may be, has pushed online contact to a new level: users don't only share what they're doing, but where they are.

Social media has gained respect in recent years, Catlow noted. People around the world have used it to support humanitarian causes and organize political movements. While some companies may continue to think of social media as a time-waster, its power is growing, and it's not going away. The only solution is to keep the online world in perspective, especially in legal terms.

"Evolving Technology, Evolving Case Law"

Catlow then asked attendees if they ever performed Google searches on candidates, and why. One attendee said she'd used Google to confirm items on a candidate's resume. Another used it to check the activities of an employee on a paid medical leave (i.e., making sure the leave was legitimate). Another used Google to look for "red flags" like criminal behavior. But no one in attendance had ever decided not to hire someone based on Google search results.

Catlow then handed the session over to Block, who seized the opportunity to warn attendees about their online search habits. Looking is easy, he said, but understanding how to handle what you find can be complex. There are significant legal risks in searching for information online, especially when visiting social media sites as part of a hiring process.

“This is an evolving technology with an evolving case law,” he explained. “And when you hear about all the laws that come into play around social media, your heads will spin.” He reminded attendees that the US is a “litigious nation.” And he stressed that they must understand the potential ramifications of their online activity.

Attendees who acknowledged looking at Facebook pages saw photos of their candidates, he noted. Even private profiles display an image. But the U.S. Equal Employment Opportunity Commission (EEOC) prohibits companies from requesting photos during recruiting. This is to protect candidates from discrimination (based on age, race, sex, etc.). By visiting Facebook, HR representatives expose themselves to information they’re not permitted to consider.

Similarly, the EEOC prohibits employers from discrimination based on criminal history, with narrow exceptions. (The conviction must be relevant to the position in very specific ways.) As a rule, he counseled, companies shouldn’t ask candidates about their criminal histories.

The moment these searches begin, Block explained, the risks begin to mount. If an applicant knows HR discovered evidence of criminal activity via Google, or viewed their photo on Facebook, they may claim that HR engaged in a discriminatory practice.

Some companies respond to these risks by prohibiting HR from visiting social media sites entirely. Others require it as a matter of published policy. Each company will have to come to its own decision based on existing law, evolving law, and what the company really needs to know.

“You have to make a decision,” Block challenged attendees. “Are you going to look for red flags, or are you going to avoid potential lawsuits by not using social media at all?”

Some Benefits, Many Risks

There are benefits to looking at social media and performing basic Google searches, Block conceded. HR will acquire more information about the candidate. And it’s relatively easy to confirm items on their resume. But online searches begin with a fatal flaw. We can never be sure that information we discover online is true.

Block shared this quote from a recent Fox News article: “The problem, [critics] say, is that the sites have no verification process. Wikipedia and Facebook can be edited by anyone with access to the internet. Sites such as YouTube and MySpace have no content requirements, beyond those that filter offensive or objectionable material. And nearly all sites allow users to make up a profile in someone else’s name....”

It’s just too easy for someone to post dishonest (and very damaging) information about someone else. If HR discovers a profanity-ridden blog entry attributed to a candidate, or online criticisms

about their work, they might consider it a “red flag.” But they may have no way to confirm its source. Similarly, a site that offers positive information about a candidate may be inaccurate.

Online “degree mills” now offer fake diplomas and credentials for undergraduate, graduate and post-graduate study (including transcripts). They look real on the screen, they sound legitimate (most fake schools have names that are strikingly similar to those of real universities), and they may even provide a contact to confirm the degree by phone. But they are fraudulent.

Assuming that what HR finds online is even true, remember that much of it can’t be considered in the hiring decision. For example, a candidate may post information about a personal medical condition like pregnancy, or mention a disabled family member. But the law protects workers against hiring discrimination based on pregnancy or association with a disabled person. Uncovering such facts offers no benefit, but involves plenty of risk.

Current Practices

A recent Career Builder survey found that—in spite of the dangers—one in five companies looks at candidates’ social media profiles as part of the hiring process. And they’ve sometimes based their decision not to hire on information they found online.

41% of respondents decided against candidates based on seeing them drinking or using drugs. 40% made their decision based on inappropriate photographs or language. 29% decided a candidate had poor communication skills after reading online content. 28% declined to hire after a candidate made negative comments about previous employers. 27% came to believe a candidate had lied about their qualifications after an online search, and 22% decided a candidate’s screen name was unprofessional.

But, Block stressed, many of these decisions were made on unlawful grounds. Criticizing an employer (within limits) is a “protected concerted activity” under the National Labor Relations Act (NLRA). Web sites exist that actually facilitate boss-bashing, making this activity very easy to discover. An otherwise qualified candidate who isn’t hired on these grounds could file an “unfair labor practice” charge with the National Labor Relations Board.

Legal extra-curricular activities are also protected. Those companies that decided not to hire because they saw evidence of alcohol consumption may well have acted unlawfully. And again, online information isn’t always credible. The candidates who were judged for their poor communication skills may not have written the copy that HR found lacking.

Even photos and videos that are real can be misleading. For example, HR may get suspicious if they see a photo of a man surrounded by young girls, all of them holding drinks. But they have no way of confirming the group was drinking alcohol or knowing the man’s relationship to the group (he could be standing with his daughter and her friends). Similarly, older photos are probably irrelevant to a candidate’s current lifestyle—and most photos are undated.

Most importantly, Block stressed, little of the information available through social media will be relevant to the job. “If someone is otherwise qualified and talented,” he asked with some exasperation, “why do we care if they had a drink in Aruba five years ago?”

When HR limits its searches to job-specific information, he went on, it reduces the risk of unfair labor practice suits. It saves HR the considerable time it takes to investigate candidates’ personal lives. And companies are less tempted to pass on the perfect candidate for all the wrong reasons.

Current Law

Block expects to see case law around social media expand and change in coming years. But there are many related laws currently on the books that employers must follow.

Negligent Hiring

There are times that HR *must* consider discovered information. Currently, an employer could be found negligent if they performed a Google search, discovered evidence of violence in a candidate’s past, hired the candidate anyway—and the candidate then assaulted a co-worker. This is true even though criminal histories can’t be used in the hiring decision.

Attendees responded to this reality with some frustration, which Block acknowledged. “These are tough judgment calls that must be made,” he said. For now, it may be safest for the company to remain ignorant...so it can claim ignorance.

In future, it’s possible that companies will be forced to search candidates’ pasts to protect their employees, as part of their due diligence. “A creative attorney will, at some point, say, ‘You could have gone online,’” Block explained. But for now, any search that isn’t required by law probably constitutes some risk.

Equal Employment Opportunity Commission (EEOC)

Per the commission’s web site, the EEOC “is responsible for enforcing federal laws that make it illegal to discriminate against a job applicant or an employee because of the person’s race, color, religion, sex (including pregnancy), national origin, age (40 or older), disability or genetic information.” These laws apply to “all types of work situations, including hiring, firing, promotions, harassment, training, wages, and benefits.”

Even a few moments on a social media profile, Block reminded attendees, will probably expose HR personnel to information they can’t lawfully consider. The law already prohibits requesting printed photographs, and Block anticipates that EEOC regulations will expand in some way to include digital images (as visible on Facebook).

There are narrow exceptions to EEOC law. Some positions require a “bona fide occupational qualification.” But in most cases, religion, age, sex, race, etc. are not bona fide occupational qualifications—and considering them is discriminatory.

The EEOC also requires HR to keep candidate information on file for extended periods—including anything that had an impact on the hiring decision. Online searches make this recordkeeping more complicated, but employers must still follow the law.

National Labor Relations Act (NLRA)

The NLRA protects the rights of employees to organize into unions and bargain collectively. Under this broad umbrella, it protects a wide variety of concerted protected activities. These include boss-bashing, within certain limits. Workers can complain about labor practices like hours or wages, but can't criticize the company's core offerings or defame a supervisor.

Extra-Curricular Activity Law

As noted, employers can't discriminate against employees based on lawful activities that take place outside of work. Smoking cigarettes, drinking alcohol (assuming the candidate is of legal age), attending political protests, etc. are all protected activities.

Fair Credit Reporting Act

Under this law, employers are required to obtain signed releases from candidates before they perform a variety of searches that qualify as "background checks." (All searches conducted by third parties require a waiver, and some company-conducted searches also qualify.) The law doesn't currently refer specifically to Google or social media. But if employers discover information that's typically found in a background check, they may be in violation.

Whistleblower Laws

The law protects workers who expose wrongdoing within a public company or organization against employment discrimination.

Genetic Information Nondiscrimination Act (GINA)

Under this law, an employer cannot discriminate against a worker whose family member suffers from a genetic disorder.

Sexual Harassment Law

These laws protect workers from unwanted sexual behavior in the workplace, including protecting subordinates from unwelcome advances by their supervisors. Managers cannot make employment decisions (firing, hiring or advancement) based on a subordinate's willingness or refusal to perform sexual favors, and they also can't create a sexually hostile workplace.

In the event of a lawsuit, social media contact (like Facebook friendships) will be scrutinized for evidence of harassment—and could become a link in the evidence chain. The friendship's very existence may look incriminating. Even if it was the accuser who initiated the friendship, that party could claim they felt pressured to do so in order to advance at work.

Under current sexual harassment law, Block warned, it's safest to avoid social media contact and relationships between supervisors and subordinates. The one exception may be LinkedIn, which is designed for strictly professional contact.

Several attendees noted that they receive friendship invitations frequently, and they asked for advice on how to respond. Block concurred with an attendee, who said she believed in being kind but firm. Speak to anyone who invites you to become Facebook friends personally. Explain that professional boundaries protect both the company and its employees, and assure them that the decision isn't personal.

After the Hire: Social Media in the Workplace

Once hiring decisions have been made, social media takes on a new, different significance for employers. The question is no longer how HR will use social media, but how—and if—employees will be permitted to use it at work.

Banning social media may seem tempting, considering the risks: lost productivity, disclosure of confidential information, posting of inappropriate content, and claims of defamation. But many professionals, especially young ones, feel entitled to social media contact throughout the day. Outright bans may prove impossible to enforce.

Ultimately, neither a complete ban nor unfettered access is practical, Block concluded. For a company to reap the benefits of social media while minimizing the risks, it must publish and enforce clear, common-sense policies.

Crafting Policies

Social Media and HR (Pre-Hire)

For the moment, companies have complete control over their policies in this area, Block noted. But to avoid suits, keep existing law in mind.

Confine online searches to job-related information and avoid sites that reveal personal details, images or video. It's easy to tell HR they can't use what they find online in the hiring decision, but it's smarter to remove all temptation.

If a company must instruct HR to look at social media, Block explained, they must control this activity to keep risks at acceptable levels. Employers should restrict the number of HR personnel who look at social media sites (and forbid hiring managers from performing their own searches), and then train those individuals carefully. Leadership must tell them exactly what to look for and what they must avoid viewing. And, regularly, they should be reminded about existing law.

To avoid being duped by degree mills, use only established, trusted means to confirm degrees and other credentials. Carefully investigate any new online services before instituting their use as a matter of policy.

Block strongly recommended partnering with counsel in this area. "Assume your policy will be scrutinized by the State Division of Human Rights and the EEOC in a 'refuse to hire' case," he warned. A skilled employment attorney can help craft a policy that is rational, enforceable and defensible—and also offer guidance on how to train HR.

Social Media in the Workplace (Post-Hire)

When considering how much to restrict employees' access to social media for personal use, align your policies with other reasonable, common-sense guidelines governing use of company technology and equipment. It's no more practical to ban use of company laptops to access social media than it is to ban use of company phones for personal calls.

Inform employees that intermittent personal use of company computers is acceptable as a means of communicating with friends and family (via social networks), but that excessive time spent online will not be tolerated. The ultimate gauge, of course, will be job performance. If an employee's work suffers because of time spent online, then their use can be deemed excessive.

Some employers choose to enforce slightly different policies for social media activity on company computers (across company servers) vs. personal technology like smartphones. This is a nod to NLRA, Block explained. If a company allows workers to use company servers to share information about personal events like school bake sales, they cannot prohibit workers from using the same servers to organize into a union.

And it seems obvious, but remember to include exceptions for those who spend time on social networks for the company's benefit. Retail brands drive customers to stores using Tweets, and recruiting firms search LinkedIn for candidates. Ensure what makes sense (and what's taking place) is reflected in your policy. There are many ways that a company can improve its image via social media—and inconsistently-enforced policies weaken a company's position in court.

There are down sides to a broad (corporate) online presence. Social media is interactive, and the company's detractors, internal and external, may prove as vocal as its fans. The employer will need to monitor all sites for vicious allegations or negative comments about the company, its practices or its employees—while safeguarding the workers' rights protected under NLRA. (Company policy should clarify permissible vs. impermissible content.)

Include a clause that prohibits employees from posting/sharing confidential information online, whether it's proprietary company data (like trade secrets or upcoming business plans) or personal details about other employees (like news of a co-worker's illness). Block recommended making this policy "reciprocal." Disclose clearly what information the company will share about its workforce and what information the company will keep confidential.

Including updated lists of new media in these policies is essential. Block shared the results of a recent survey by the online security firm Proofpoint, which tracked leaks of confidential information. 43% of security leaks were emails, 18% were blogs, 18% were YouTube videos, and 17% were social media posts. To cover all bases, avoid over-arching phrases about internet use in your policies, and itemize clearly: Facebook, YouTube, blogging, texting, etc.

Be sure to protect copyrighted information. Clarify what information (words, phrases, concepts, etc.) are protected. Either forbid workers from posting this information online, or instruct them specifically on how to do so.

Finally, include a grievance process in your policy. While certain types of complaints are protected under NLRA (e.g., “My hourly wage stinks”), defamation of a supervisor is not (e.g., “I work for Satan”). As always, allegations of racism, sexism, sexual harassment, etc. that arise through social media or any other channel must be thoroughly investigated.

Distributing Policies

Compliance begins with awareness, Block stressed, and the most defensible, ironclad policy is useless if employees don’t know about it. HR must make an extra effort to ensure employees behave lawfully.

Block’s suggestion? “Get creative.” Include company policies on computer log-in screens. Reserve time for HR announcements at company gatherings/meetings. If necessary, read the policy aloud to workers, one small group at a time.

“These policies protect the company; they are important,” Block stressed. “At this stage, they are legally complex and critical. However you have to do it, make sure everybody ‘gets it.’”

Choose Wisely, Define Clearly

Weighing the benefits and the risks, each company must ultimately come to its own decision on how to handle social media, both before and after the hire. But existing laws do provide important guidance. To ensure the company enjoys basic legal protections, it’s critical to institute policies that are consistent with existing law—and enforce them.

At the very least, Block said in closing, act with awareness. Understand the legal ramifications of spending time in social media—as an HR professional or an average employee. And only let your company take informed risks that it is legally prepared to defend.

Anne DeAcetis is a freelance writer based in New York. Reach her at anne.deacetis@gmail.com.

The HR Roundtable is a breakfast forum for human resources professionals in New York City sponsored by The TemPositions Group of Companies. TemPositions, one of the largest staffing companies in the New York tri-state area with operations in California, has been helping businesses with their short- and long-term staffing needs since 1962. Visit them online at www.tempositions.com or email them at info@tempositions.com.