How You Can Safely Use Social Media with Employees

There's no denying it, social networking is all the rage.

Everywhere, people are tweeting, texting, emailing, blogging and IM'ing. People of all ages have Facebook, MySpace and LinkedIn accounts. They are on Twitter day and night. There is even a new set of vocabulary associated with social networking. For example, "dooced" means to get fired because of your website. Innovations for communicating electronically are moving at lightning speed, making it difficult for employers to strike the delicate balance between monitoring and restricting employee use of social networking sites, and giving employees enough freedom to allow them to be productive and content in the workplace.

By Larry Silverman and Terri Imbarlina Patak

Recent statistics show that Facebook, launched in February 2004 as a social network for Harvard undergrads, has more than 300 million active users. More than two billion photos are loaded to the site each month. MySpace, which typically has a younger audience, has more than 185 million active users. And Twitter, which is only four years old, and suggests users broadcast responses to the question, "What are you doing?" boasts more than 25 million users.

Employers and employees alike are posting to and viewing these sites. There is no question that social networking impacts the employment arena from the time an employee fills out a job application, through that employee's ongoing relationship with his or her employer. It is critical, therefore, for employers to understand how these sites affect their workplace and impact their employment-related decisions. There are a myriad of issues that present themselves when discussing social networking and the workplace. This article adresses pitfalls and best practices of using social networking sites at the pre-employment screening stage, and monitoring and regulating use of social networks by current employees. It focuses solely on practices for the United States. A discussion of unique issues applicable to other jurisdictions, especially in the European Union, is beyond the scope of this analysis.

LARRY SILVERMAN is senior vice president and general counsel for the Pittsburgh Pirates Baseball Club. He provides legal counsel to the Club on a wide variety of issues including contracts and employment and assists with contract negotiations and other player-related matters. Silverman received his JD from Duquesne University School of Law. He can be contacted at *larry.silverman@pirates.com.*

TERRI IMBARLINA PATAK is of counsel with Dickie, McCamey & Chilcote, P.C., and has more than a decade of experience in the area of employment and labor law. She regularly trains companies in employment discrimination and harassment, best practices for human resources management and more. She received her JD from the University of Pittsburgh School of Law. She can be contacted at *tpatak@dmclaw.com.*

When Too Much Knowledge Is Bad

Federal laws such as the Civil Rights Act of 1964, the Americans with Disabilities Act and the Age Discrimination in Employment Act, prohibit employers from discriminating against applicants and employees because of their race, color, religion, gender, national origin, age and disability. For years, employment lawyers have advised employers not to ask questions on their applications about these protected categories.[1] Furthermore, they've recommended avoiding questions that might cause employers to assign a specific stereotype to an applicant. Questions about the applicant's children's ages and how many sick days the applicant took on his or her last job could prompt stereotypes about parents of young children missing more work, or about individuals who took sick days suffering from a disability. Basically, any questions that could elicit information about personal attributes that are not job-related and/or are protected by law, are taboo during the application and interview process.

Nevertheless, employers today are throwing caution to the wind and stepping into this minefield of improper pre-employment inquiries when they conduct applicant screenings online. Employers are "Googling" applicants, checking out their Facebook and Myspace pages, and learning information that could cause end them up in court, defending their decision not to hire. Any personal information learned from social networking sites could become a potential basis for a lawsuit wherein the individual claims that the adverse employment action was based upon that personal, non-job-related information.

Before the internet offered countless ways to dig up information about an individual, employers using well-drafted applications to screen applicants had no way of knowing an individual's personal statistics. Sometimes it was even difficult to know the applicant's gender if the name was gender-neutral, like Pat, Terry or even Sam. This lack of knowledge about personal statistics allowed employers to screen applicants without the danger of being accused of making a hiring decision based on a personal, law-protected attribute.

Today's computer-savvy employers are routinely searching the internet for information regarding applicants. With the click of a mouse, employers are instantaneously bombarded with pictures of applicants and their families and friends, thereby disclosing, at the very least, that applicant's gender, color, visible disabilities and possibly race. Those same photographs could also disclose religious affiliations of the applicant and his or her family if religious garb is worn or the picture is taken at a place of worship. Pictures can even disclose other group affiliations or memberships in labor unions. Potential employers who search these sites also may have access to whatever personal information is written on the site — anything from information about the applicant's children and their activities, to the applicant's medical problems or involvement in programs such as Alcoholics Anonymous. Without actively searching on the internet, the potential employer would never be privy to such personal non-work-related information about an applicant. And once this information is learned, it cannot be "unlearned." So, from just a few minutes on a social networking site, an employer can learn a wide array of information about an applicant that could result in a claim that such information was used improperly in making the hiring decisions.

Employers should be equally cautious about the use of social networking during the interviewing stage. They should refrain from posing questions to employees about information learned from a social networking site that they

would not otherwise pose. For example, if an employer typically would not ask questions about union affiliation during an interview, it would not be appropriate to ask such questions based on something seen on a social networking site. Similarly, interviewers should be cautious about tweeting about prospective candidates after the interview. Depending upon what is written, that candidate may have a potential claim against the employer if she or he is not hired.

Despite all of this, it is not practical to assume employers will stop "Googling" their applicants or searching for other information on the web. It's human nature to be curious, after all. But when doing so, employers should ask themselves whether the information they are seeking is relevant to the job for which they are hiring. When weighing the pros and cons of searching social networking sites for information regarding applicants, employers are in a much better position to defend a failure to hire claim when they can honestly say they didn't have access to the applicant's personal information. For employers who make an informed decision to continue researching information about applicants on social networking sites, the company should consider having a policy in place that expressly states that the company is an equal opportunity employer and that any irrelevant personal information that is learned through an internet search will not be used in making hiring decisions. As always, if an employer can show that the most qualified candidate for the job was chosen, he should be able to successfully defend himself against failure to hire claims.

Monitoring and Controlling Current Employees' Use of Social Networking Sites

As you would expect, employee and employer viewpoints differ on whether and when it is appropriate to monitor what employees post on their social networking sites. In a recent workplace survey, 60 percent of business executives surveyed said the employer has a right to know how employees portray themselves and their organizations on social networking sites. On the other hand, while 74 percent of the employees surveyed understood that what they say about their employers online can damage their employer's reputation, 63 percent of those employees still believed that employers should not be permitted to monitor their social networking sites.[2]

So, what should an employer do? First and foremost, there is no question that an employer has the right to prohibit or restrict the personal use of company computers, computer networks, company-issued BlackBerrys® and other equipment. Employees should understand that they should have no expectation of privacy when using company owned or issued equipment and networks. This is true even when the employees are using the company's equipment to access their personal sites or when they are using such equipment "off the clock."

To Tweet or Not to Tweet: Social Media in Professional Sports

Like many employers, the professional sports industry has grappled with how to respond to the widespread use of social media sites such as Twitter and Facebook. In the past year alone, the San Diego Chargers fined a player $2,500 for complaining on Twitter about the food at training camp; the Kansas City Chiefs suspended Larry Johnson for posting anti-gay remarks on his Twitter site and pro-tennis' anti-corruption unit began an investigation into whether players were passing inside information on their Twitter sites in violation of tennis' anti-corruption rules.

The concern over players' use of social media has led both the National Football League (NFL) and the National Basketball Association (NBA) to adopt sweeping new Twitter policies. The NFL policy bars Twittering 90 minutes before games and continues the ban until post-game interviews have been completed. The NBA's policy prohibits any use of cell phones, personal digital assistants (PDAs) and other devices, which provide access to sites such as Facebook and Twitter 45 minutes before the game and continuing until the players have fulfilled their post-game media obligations. Additionally, at least four NBA teams have adopted even stricter bans that bar use of these sites during meetings, practices and other "team time."

While the stated reasons for these new rules are that players should be focusing on their jobs and not with communicating with their fans, it is also clear that these policies are enacted to ensure that the league's broadcast partners, who pay huge rights fees to the league, are given the first opportunity to broadcast breaking news stories to the public. Whatever the reason, the prohibitions contained in these policies raise serious questions about the rights of employers to regulate "off-field" behavior and whether enforcement of such policies by the courts violates a players First Amendment rights. Whether it is arbitrators under the league's collective bargaining agreements and/or the courts, when a player can tweet or post on Facebook and what the player can say on those sites are issues that will almost certainly be litigated in the coming months.

The more difficult question to answer is whether employers should monitor social networking when employees are off duty and not using company equipment. And if employers do monitor employee activity, what should they do with the information they find? This is a difficult question and does not have one simple answer. An employer's decision whether to monitor employees use of social networks when they are not working is based upon a number of factors, many of which are unique to the employer and business.

For example, what if an employer employs social workers to counsel clients on drug and alcohol prevention and has a policy in place to remind employees that because of their role, they are agents of their employer at all times, and they must conduct themselves accordingly both in the workplace and in public. That same employer, through a social networking site, finds pictures of its social workers drinking and carrying on at a local bar. What should that employer do with that information?

By now, everyone has heard about the Domino's Pizza employees who posted a video on YouTube showing them making pizza under less-than-hygienic conditions and making fun of customers. By the time Domino's was able to remove the video, it had been viewed more than one million times and the damage was done.

A company has the right to protect its legitimate business interests even if that includes implementing a policy that regulates an employee's use of social networks on non-working time. So, for the employer of the social workers, protecting its reputation in the community is a legitimate business interest and one that the employer has a right to protect. Similarly, a business-owner like Dominos, which could suffer devastating repercussions from negative postings about the company, has a right to prohibit employees from using social networking sites in a manner that is detrimental to the employer.

As you can imagine, there is very little case law on this subject. However, as the use of social networking continues to grow, we are beginning to see some court decisions. For example, a state court in New Jersey held that although an employer has no duty to monitor employee comments made on an electronic bulletin board, they do have a duty to prevent employee harassment in settings related to the workplace if they know or have reason to know such harassment is taking place.[3] In another case, a California appellate court upheld a decision that employers may have a defamation claim against former employees based upon information posted on blogs.[4]

Should Employers Search Social Media Sites? Negligent Hiring Claims

When deciding whether to hire an employee, search engines like Google and Bing can be useful screening tools for employers. Unfortunately, however, there are pitfalls to the "use all the tools approach."

In determining whether an employer has used due care in its hiring process, the courts will consider the totality of the circumstances. Where the employee is likely to have routine and regular conduct with the public, more screening is needed than when such contact with the public is likely to be minimal. For example, where the applicant will be working alone with patients at a nursing home, greater background scrutiny is needed than for the applicant for a payroll administrator position at that same nursing home, as in the 1999 *Barry v Manor Care, Inc.* case. Hence, there are situations where doing too little pre-employment screening may expose an employer to negligent hiring claims. There are also situations, however, where doing more screening than the circumstances call for may actually increase the risk of liability. A recent case highlights this conundrum. A FedEx employee allegedly raped an 8-year-old girl while on a computer-repair call to the child's household. Fed-Ex had a policy of doing background checks, but it was alleged they performed those checks negligently and thereby failed to discover the employee's violent past. As counsel for the family noted, while the employer may not have had a duty to do background checks, "when you take it on as a matter of corporate policy, then you have a duty to do so properly."

Applying this reasoning to social media sites, consider this scenario. The employer, by policy or practice, regularly examines Facebook and LinkedIn as part of its pre-employment screening protocol. In the case of applicant Jones, however, it either fails to engage in that review at all or does so negligently. Once hired, Jones commits a violent act against a coworker. The coworker files suit against the employer arguing that had the employer followed its own pre-employment protocol, it would have uncovered facts that would have led to the applicant's rejection. As such, even if the "totality of the circumstances" did not require the examination of these social media sites, the employer had assumed a duty of care to do so, suggesting that "no good deed goes unpunished."

This cautionary tale is not meant to suggest that less is always better, as clearly there are jobs for which detailed pre-employment screening is needed to avoid negligent hiring claims. The tale does suggest, however, that more is not always better either. If examination of a social media site is not necessary under the circumstances, don't do it, as such pre-employment screening could expose the employer to a negligent hiring claim that otherwise would not have been viable.

As this area of the law continues to develop, employers must make the difficult decision whether they will monitor the social networking postings of their employees. For employers who are not comfortable monitoring their employees' activities outside of work, they might want to consider purchasing a service which can monitor all social media for content involving the company. By doing this, employers could insulate themselves from claims concerning overly broad monitoring of their employees' postings and still protect the company. Another way to protect the company is by implementing a policy regarding social networking.

Employees should **understand** that they should have **no expectation of privacy** when using **company owned** or issued **equipment** and networks.

A Carefully Crafted Policy Is an Employer's Best Protection

All employers whose employees have access to the internet at work or outside of work should consider implementing a social networking policy. In drafting a policy, the first thing an employer should consider is the goal of the policy. Does the employer want to limit all personal use of company equipment or place restrictions on that use? How far does the employer want to go with regard to monitoring employees' personal postings, etc?

Zero tolerance has been an employer catch phrase for a number of years. With the Supreme Court's landmark decisions in *Harris, Faragher and Ellerth*,[5] employers recognized that sexual harassment of any kind cannot be tolerated in the workplace. While zero tolerance policies in the context of sexual harassment, as well and gender, racial, disability and other types of discrimination are acceptable, and even advisable, this may not be the case with policies concerning electronic media. Employees who are at a workstation with internet access inevitably will access non-work-related websites at some point during the work week. It would be difficult for an employer to implement a policy of zero tolerance for personal use of electronic media and even more difficult and time-consuming to monitor. This, however, does not negate the possibility of an employer blocking certain sites from company computers or doing away with internet access altogether if it is not necessary for the business.

Many employers are taking less drastic measures and implementing reasonable policies with restrictions on social networking. These policies may be incorporated into other existing policies such as an electronic media policy or drafted as a stand-alone policy. The policies should be in writing and distributed to every employee either in an employee handbook or by some other means that ensures every employee receives it. Regardless of the format, here are some points all policies should include:

- An affirmative statement regarding the use of company equipment. Regardless of the stance that the employer takes with regard to personal use of company equipment, it is critical that employers have clear guidelines concerning the use of social networking sites. At a minimum, the policy should explain that employees should have no expectation of privacy with regard to their use of company equipment including, but not limited to, computers, phones, cell phones and PDAs. The policy should also clearly state whether employees may use company equipment for personal reasons and detail the restrictions or prohibitions of such use.
- A statement addressing social networking both at work and at home. It should explain that employees who engage in social networking, whether on or off the job, must abide by the employer's policies and procedures concerning harassment, intellectual property and confidential information and/or trade secrets.
- A statement addressing the use of the company's name, logo, uniform or other distinct means of identifying the company, including using company email addresses on personal social networking sites. Additionally, the policy should address the use of customer or client names or related information.
- A requirement for employees who identify themselves on personal sites as employees of the company (either in writing or visually by showing a uniform or logo) to include a disclaimer stating that the views expressed are those of the employee and do not reflect the views of the employer.
- A statement prohibiting all uses of social media that disclose proprietary or confidential information such as trade secrets and inventions, customer lists, financial information, business plans, etc.
- A statement prohibiting employees from tweeting, texting or engaging in other types of external social networking during company meetings (although it should go without saying).
- An explanation of the consequences of violating the policy, such as disciplinary action up to and including discharge.
- A "point person" to whom employees can go with questions or concerns.

Employers should also take into consideration use of company-sponsored blogs, websites, etc. when drafting the policy. If a company uses social networking tools for business purposes, the employer must consider such uses when drafting the policy. Obviously many, if not all, employees should have access to online networking sponsored by the company.

In the wake of company-sponsored networks, employers need to be cautious with regard to employee use of company networks from a timekeeping perspective. For example, because the internet is available at all times, employers need to make sure that hourly nonexempt employees are not accessing company-sponsored sites and performing work "off the clock." The best way to ensure that is to incorporate language into an existing policy prohibiting working "off the clock." The language should explicitly state that hourly nonexempt employees must record all time accurately and should not be performing work outside of the workplace or off work time, including working on company-sponsored online networks, without authorization from the company. Without such a policy, nonexempt employees could potentially claim that by having a blog or site available, the employer was encouraging employees to use the site and that they are entitled to payment of wages for time outside of work spent on the company-sponsored site. The Fair Labor Standards Act requires an employer to pay an employee for any work that the employer suffers or permits. Without a clear policy prohibiting "off the clock" work, an employer would have the burden of proving that the employee is not entitled to the wages he is claiming.

ACC Extras on…Social Networking

ACC Docket

- *Online Social Networking and Your Career: Are You Staying Ahead of the Game? (July 2008).* In-house counsel should be aware of social networking sites to join them. Find out about this type of online social networking and explore some of its potential benefits. *www.acc.com/docket/soc_netwk&car_jul08*

Quick Reference

- *A Checklist for Social Media Legal Notices and Policies (November 2009).* A non-exhaustive list of provisions to consider in preparing a policy, agreement or legal notice for use with members and others that connect with associations through an online social networking site, or in connection with a more formal terms of service or legal notice for a page, site or blog on a social networking site. *www.acc.com/quickref/soc_medchklist_nov09*
- *The Legal Aspects of Online Social Networks: An Overview for Associations (October 2009).* A non-exhaustive list of legal tips and issues to consider in connection with using social networking sites or social media either to create/manage content, or to send or sponsor content. *www.acc.com/qickref/assoc/socialnetwks_oct09*

Sample Form & Policy

- *Social Media and Social Networking Policies and Procedures (June 2007).* A model set of social media policies and procedures that discusses creating and managing content, leaving comments, confidentiality and privacy, potential conflicts and red flags. *www.acc.com/forms/soc_media_jun07*

Leading Practice Profile

- *Social Networking for Companies: Leading Practices in Leveraging Social Media for Business, Creating Social Networking Policies and Using Social Media in Hiring (September 2009).* Examine the use of social networking in companies, and the law department's role in crafting effective social networking and electronic usage policies, mitigating risks and addressing social networking in the recruiting and hiring process. *www.acc.com/soc_ntwk/companies_sep09*

Education

- *Don't Be a Party Pooper, Let Your Business Be Social. Just Watch What It Does! (October 2009).* This presentation defines and explains the significant social networks and who is participating in them, the various ways that corporations are playing and profiting, the new economies created, and the legal risks and business risks your company may face if it participates. *www.acc.com/socialbiz_oct09*
- *Nuts and Bolts of Employment Screening: I-9s, Background Checks and Medical Exams (December 2007).* This ACC program material is a substantive overview of the laws that every employer needs to know and what the company must do prior to a candidate starting work. *www.acc.com/empl/screen_dec07*

ACC has more material on this subject on our website. Visit *www.acc.com,* where you can browse our resources by practice area or use our search to find documents by keyword.

Once a policy is in place and distributed to employees, it is advisable to hold a training session so the employer can explain the policy to the employees and give them an opportunity to ask questions. Often such sessions bring to light potential issues that the employer did not consider when drafting the policy, allowing the employer to revisit those issues after the meeting. Employee training sessions also give employees an opportunity to vent their concerns in a controlled atmosphere and allow the employer to address the concerns before they get blown out of proportion. During the training session, employers should remind employees of the potential negative consequences of what they post. Specifically, employees should be reminded that whenever they are engaging in social networking, their postings may be broadcasted to an infinite number of viewers and therefore, they should choose their words wisely.

In general, employees should refrain from making any references to their employer or its customers on personal sites. If employees do make references to the employer, they should make it clear, through a disclaimer or other means, that the employer does not sanction the views expressed. Finally, employees should be reminded that if their postings violate any of the employer's policies such as the policy against harassment, disclosing confidential information or trade secrets, etc., even if during personal time, the employee will be subject to disciplinary action.

Employers who recognize the extent to which social networking and other types of electronic media is being used both in and outside of the workplace, and who are willing to implement reasonable policies concerning social networking, will be able to use social networking to their advantage while, at the same time, protecting themselves from its negative implications.

Have a comment on this article? Email editorinchief@acc.com.

NOTES

1. Employee applications should be reviewed by an experienced person. For example, either an appropriately trained human resources specialist or an employment attorney, before being used in order to avoid unnecessary employment-related claims.
2. Deloitte LLP, Survey Results, *2009 Ethics & Workplace Survey: Social networking and reputational risk in the workplace* (2009).
3. *Blakey v. Cont'l Airlines, Inc.* 751 A.2d 538 (NJ 2000).
4. *Varian Med. Sys., v. Delfino,* 6 Cal.Rptr.3d 325 (Cal.Ct. App.2003).
5. *Harris v. Forklift Sys. Inc.,* 510 US 17 (1993); *Faragher v. City of Boca Raton,* 524 US 775 (1998); *Burlington Indus., v. Ellerth*, 524 US 742 (1998).