Mitigating the Legal Risks of Using Social Media

by Sharon D. Nelson, Esq., and John W. Simek

During a 2010 conference, counsel from Coca-Cola and Sprint enthusiastically referred to their "social media ninjas," or those employees who are charged with using social media on the organization's behalf. They were clearly true believers who have invested a lot in social media and, more importantly, are enjoying the payoff.

The rise of social media has provided incredible marketing, recruiting, and customer relations benefits. Tech-savvy employers utilize these technologies to advertise employment opportunities and connect with existing and potential customers. The allure of riches to be gleaned from social media has been so great that many organizations have jumped on the bandwagon without considering where they want to go and how they should get there. They see the riches, but often fail to evaluate the risks.

Identifying Social Media Risks

The downside of social media: Its use may give rise to potential legal liability and adversely affect brand or organization reputation. Thoughtful use of social media and the development of a coherent and practical social media policy are essential. Organizations need to bring together management, IT, human resources, business development, records management, and legal personnel to formulate a good policy, one that will limit risks and maximize benefits..

Adverse Publicity

A few years ago, musician Dave Carroll looked out the window of a United Airlines plane to see baggage handlers allegedly tossing his $3,500 Taylor guitar like a basketball. It arrived at his destination in two pieces. Conventional attempts to resolve the matter failed, so he created a catchy little tune called "United Breaks Guitars" and posted it on YouTube. More than 8 million hits later, and with the media all over the story, United buckled and donated $3,000, at Carroll's suggestion, to the Thelonius Monk Institute of Jazz.

United, badly stung by adverse publicity, began to get the message and set about learning how to leverage social media. Now, United routinely responds to social media complaints. Individuals have "tweeted" about a problem only to be contacted by United to resolve the matter. United clearly took to heart the U.S. Marine Corp unofficial mantra: "Improvise, Adapt, and Overcome."

Most organizations that embrace social media do so because these sites provide a closer, more personal interaction between the marketer and the target audience. This allows customers to feel more involved in the community of customers, while also giving companies better and faster customer opinions about a particular product or service. But, as the Dave Carroll story shows, customers can employ social media to air their grievances, which often demands a response to quiet the waters.

Misleading Advertising

Another risk comes from the Federal Trade Commission's (FTC) Act (15 U.S.C § 41 et seq., 1914) on unfair or deceptive acts or practices that broadly covers advertising claims, marketing and promotional activities, and sales practices in general. Just like traditional advertising, this means that all social media ads must be truthful and not misleading; advertisers must have evidence to back up their claims, and advertisements cannot be unfair.

Unvetted Postings

The informal nature of social media advertising and the fact that it is not generally closely monitored can produce a higher risk of legal liability for the company. In particular, the traditional and serious vetting processes for advertising and press releases are almost nonexistent because social media marketing is a daily torrent. Moreover, blog posts and comments on online communities are usually not screened before they appear. Damaging content can spread globally in hours before someone notices and removes it.

Undisclosed Endorsee Connections

In addition, the FTC has released its endorsement and testimonial guidelines applicable to social media advertisements entitled "Guides Concerning the Use of Endorsements and Testimonials in Advertising." Specifically, the guidelines provide that if there is any material connection between an organization and an online poster, the connection must be disclosed by the individual. Hence, an employee who favorably blogs or comments on the organization or its products may be deemed an endorser under the guidelines, thereby subject to the disclosure guidelines. Failure to disclose the connection can, in some circumstances, result in the imposition of liability on the company regardless of whether the company approved (or even knew of) the post.

Illegal Employment Practices

The use of social media by employees for business- and non-business-related purposes is an area fraught with legal pitfalls and requires careful consideration on the part of management and legal counsel. Employers have always done some background checking on prospective employees; however, while social media sites afford more background information than ever, their use may result in unwitting violations of privacy, equal protection, or fair financial practice statutes.

Discriminating Against a Protected Characteristic. Certainly, an employer can and should verify a potential applicant's employment history if it is readily available on a social networking site (e.g., LinkedIn), and any information that implicates unlawful conduct can serve as the basis for retracting a job offer or terminating an employee.

Aside from that, employers must tread carefully. Employers who screen applicants using these sites may be providing a rejected applicant with a basis for claiming that the employer's decision was based on a protected characteristic (e.g., race, gender, and sexual orientation) that was readily apparent on the applicant's profile. Although the applicant will have to prove the employer's decision was based upon the characteristic in making the adverse employment decision, an admission that the employer examined the individual's social media pages can make it easier for the complaint to survive a summary judgment motion and embroil the employer in costly litigation.

Violating the Fair Credit Reporting Act. In addition, employers that choose to screen blogs and social networking profiles must also comply with the Fair Credit Reporting Act (FCRA), which requires an applicant's (or employee's) consent before an employer may engage a consumer reporting agency to produce a consumer report on that individual. Although the FCRA permits the use of consumer reports that contain information gleaned from social media, the employer must disclose that the information resulted in the adverse employment decision.

Violating Expectation of Privacy. Employers who access an employee's social media sites, especially those with privacy settings, will likely face allegations that they visited these sites without express permission (i.e., the employer violated the employee's expectation of privacy). Organizations do not have unfettered access to these accounts; any enhanced privacy controls must be scrupulously respected. These controls will not only increase an employee's common law claim to privacy, but attempting to circumvent these controls can violate federal law in addition to the social networking site's terms of service.

Making Unauthorized Access. Specifically, a federal cause of action might exist under the Computer Fraud and Abuse Act, in which an employer, in accessing an employer's social media profiles, exceeds authorized access in obtaining data from the website's computer system, and the Electronic Communications Privacy Act, in which an employer engages in unauthorized access of electronically stored data or electronic communications.

Violating State and Federal Laws. Even if an organization lawfully accesses information on an employee's social media pages, some of that information might be afforded protection under various state and federal laws. For instance, certain communications are protected because they constitute protected complaints of discrimination or whistle blowing. For example, comments about compensation or workplace safety could fall under the protections of the National Labor Relations Act (NLRA).

Moreover, certain states, such as California, Colorado, and New York, have enacted "lifestyle" laws that prohibit an employer from taking adverse employee actions based on lawful, off-work conduct. In these states, companies cannot fire or discipline an employee if they discover information pertaining to questionable, but legal, off-duty conduct on an employee's social media page.

Some of these provisions do contain an exception for material conflicts of interest, such that an employer could lawfully take action if the employee's conduct harms the employer, even if the conduct is otherwise lawful. Courts, however, have yet to provide clear-cut legal guidelines on this issue:

- In *State v. Wal-Mart Stores*, two employees were terminated by Wal-Mart for dating, while one of the employees was married to another person. In upholding the organization's decision to terminate the employees, the court held that dating was not considered to be a "recreational activity" and, therefore, was not protected by New York's lifestyle discrimination statute. Shortly thereafter, the New York courts took a more expansive view of "recreational activities" protected under the statute.

- In *Pasch v. Katz Media Corp.* the court expanded the definition of recreational activity to include cohabitation. The court has since returned to a less expansive definition of recreational activity, choosing instead to follow the holding in the *Wal-Mart* case.
- Recently, the National Labor Relations Board (NLRB) filed a complaint against the American Medical Response (AMS), a Connecticut ambulatory service company. In the complaint, the NLRB claimed the termination of an employee for posting negative comments about her supervisor to her Facebook page, which drew many supportive comments from some of her co-workers, violated the NLRA. Specifically, the NLRB argued that the employee's actions were protected and that the organization's policy prohibiting disparaging comments was itself a violation of the NLRA. Ultimately, the employer reached a settlement with the NLRB and agreed to rewrite its social media policy prohibiting negative remarks in cyberspace. As a settlement, the outcome is not binding on employers, but it should certainly suggest caution. This case provides a clear statement that social media policies are going to be a new focus of NLRB enforcement actions.

Mitigating Social Media Risks

Monitor Employee Activity
Given these potential pitfalls, an organization might choose to forego monitoring employee activity on social media sites. This is a bad idea. Failing to take action on employee comments that might be considered discriminatory or harassing, especially if brought to the organization's attention, could also land the organization in hot water.

- In *Blakely v. Continental Airlines,* a female pilot filed a complaint alleging a hostile work environment and defamation against the employer airline after derogatory comments about her were posted on another pilot's electronic bulletin. The court ultimately denied the airline's motion for summary judgment as to the hostile work environment claim, holding that Continental had a duty to take effective measures to prevent the harassment when it knew, or at least had reason to know, that the conduct was occurring in a workplace-related setting.
- In *Simonetti v. Delta Air Line, Inc.* a female flight attendant filed suit on the basis of sexual discrimination after the airlines discovered "inappropriate" photographs of the employee in her Delta uniform posted on her blog. Simonetti claimed the airlines did not punish male flight attendants who maintained blogs containing similar content. Although the case was not adjudicated because Delta filed for bankruptcy shortly after the lawsuit was filed, it still stands as a stark reminder that failing to monitor social media activity can lead to costly lawsuits.

An organization that fails to scrupulously monitor its employees' usage of social media risks missing a post that reveals the organization's proprietary or confidential information. Without question, social media has dramatically increased the possibility of sharing such information, especially since the informal nature of posting to these sites makes it very easy to inadvertently disclose too much.

A single tweet saying, for instance, that the employee has been working on a new invention for Company X could have severe repercussions. Since it's so easy to also post photos and videos to social media sites, this means an employee could inadvertently reveal a wealth of information about the culture of the organization, who works there, what products are in use, and even details about customers.

Crowdsourcing, defined as the act of outsourcing tasks traditionally performed by an employee or contractor to an undefined, large group of people or community (a crowd) through an open call, has further compounded the problem. Crowdsourcing can make it very difficult, if not impossible, for an organization to retain any expectation of confidentiality in the work product being "crowdsourced."

Finally, monitoring social media can prevent a few ill-advised tweets or blog postings from tarnishing an organization's image. Domino's learned firsthand the power of social media after two of its employees posted videos of themselves doing a number of unspeakable things to the pizzas they were making. The resulting avalanche of views was a public relations nightmare.

When searching for Dominos, the YouTube video popped up prominently, only compounding the problem. Making matters worse, Domino's waited nearly two days to respond, by which time close to 1 million people had already viewed the videos, and blogs, forums, and Twitter were inundated with discussions of the incident. Even though the employees were fired and an apology was issued, the damage to the organization was done. Consumer perception of the brand soured.

Similarly, companies that maintain a Facebook page can learn from the Nestle incident in which a Nestle employee posted a comment on the organization's Facebook page requesting that those who commented on the page not use altered versions of Nestlé's logo for their profile pictures, saying their comments would be deleted. Site visitors reacted poorly. Unfortunately, the employee lost his cool and went on the offensive, responding to individual posters in a tone that was at times sarcastic or antagonistic. The resulting ruckus caused Nestle a major headache as it tried to engage in damage control.

Develop Clear Policy on Social Media Use

Most of the social media risks can be minimized by carefully crafting a social media policy coupled with implementing a few technological safeguards. There is no need to reinvent the wheel; IBM and Coca-Cola have posted their social media policies online, which can provide a good starting point. See the sidebar for the major elements.

Major Elements of a Social Media Policy

A well-crafted policy should:

1. Address all potential pitfalls in a clear and organization-specific manner and be consistent with other organization policies and procedures
2. Distinguish between business and personal use (on-the-job and off-the-job conduct)
3. Inform employees of the rules and regulations that state they will have a reduced or non-existent expectation of privacy on any of the organization provided computers, e-mail systems, mobile devices, and telephone or voicemail systems

4. Encompass what can be said, who can say it, and the manner in which things should be said

An organization's policy should provide a clear expectation of what an employee is permitted and forbidden to say. Addressing content that can be posted on social media sites can prevent a variety of mishaps, including:

- Preventing the inadvertent posting of confidential information and trade secrets
- Curtailing defamatory or otherwise inappropriate content
- Stopping any other unlawful or criminal information from being posted

The policy should instruct employees to:

- Avoid controversial subjects
- Use a polite and respectful tone, even when disagreeing
- Never post anything that could conceivably be construed as discrimination, harassment, or defamation

The policy should limit who has the authority to speak on the organization's behalf. To effect such a strategy, consider:

- Banning those individuals not authorized to speak for the organization from using any of its intellectual property (e.g., logos, trademarks, and copyrights) in any manner
- Forbidding the use of the organization's name in particular forms (e.g., username and screen name), but perhaps specifically allowing it as part of the employee's profile so long as the information remains current

The essence of a good policy is simple: "Don't be stupid." While many more words are perhaps advisable for the sake of clarity, that's what it all boils down to.

Provide Strong Consequences, Make Them Clear

Any good policy must have teeth. There must be a clear statement providing that any misuse of social media by employees can be grounds for discipline, up to and including termination. In addition, employees should be required to attend regular training and meetings to ensure they remain current on any new changes in the policy, as well as new developments regarding changes in the social media sites themselves. If changes in the policy are required, it might be a good idea to send an organization-wide e-mail highlighting the changes and announcing any upcoming training sessions.

Impose Technology Controls

Organizations should also consider whether or not to impose technological controls on social media usage. The key words are "try to impose" because the advent of smartphones has made control difficult, if not impossible, to achieve. Even if the organization-owned smartphones are controlled, many employees have personal smartphones, as well. Organizations have learned, to their chagrin, that their employees are adept at making end-runs around technological barriers.

Many companies do forbid the use of social media at work, generally using hardware or software to block common social media sites. For those organization-owned smartphones that are

sophisticated enough for advanced security measures to be taken, access to social media sites can also be banned.

However, most organizations are embracing the use of social media at least to some extent. Even where social media use is permitted, many companies will use hardware or software to monitor usage. Without question, social media usage can be the mother of all productivity drains. It has been the experience of Sprint and Coca-Cola, whose ardent embrace of social media was mentioned earlier, that those who abuse social media are generally known to their colleagues. Nevertheless, many employers are aghast when they are shown data gathered with specialized hardware and software tracking employee usage of social media.

Create a Media Czar Position
Finally, depending on the size of the company and the nature of its social media use, it may need a social media czar to oversee both an ever-changing social media landscape and the technology available to use and monitor it. Organizations are now beginning to create such positions.

Balance Social Media Potential Against Risks

Facebook, Twitter, YouTube, and their social media brethren have been in use for only a few years, and yet they have revolutionized business marketing and customer relations. This is very much a revolution in progress, and each year brings new technologies, new regulatory requirements, and new court decisions important to individuals who manage social media usage within their organization.

Social media sings a sweet siren song indeed, and yet it can morph in an instant into Pandora's Box. Success with social media, while limiting risk, requires constant vigilance.

About the authors:

Sharon D. Nelson, Esq., is president and John W. Simek is vice president of Sensei Enterprises Inc., a legal technology, computer forensics, and information security firm based in Fairfax, Va. Special thanks goes to Sensei paralegal Jason Foltin for his excellent research on this topic. Ms. Nelson can be contacted at snelson@senseient.com *and Mr. Simek at* jsimek@senseient.com. Phone: 703-359-0700. Website: www.senseient.com.