The Legal and Effective Business Use of Social Media in the Workplace

Theodora R. Lee

Theodora R. Lee is a senior shareholder/partner with Littler Mendelson, P.C., San Francisco. She specializes in representing employers in all aspects of employment and labor relations law, including class action litigation; wrongful termination and employment discrimination litigation; National Labor Relations Board matters, including representation cases, unfair labor practice proceedings, grievance arbitrations; Title VII/FEHA proceedings, including race, sex, religious, and age harassment and discrimination; unfair competition proceedings; and state and federal wage and hour litigation. She was named as a Leading Law Firm Rainmaker by the Minority Corporate Counsel Association in 2010 and a Northern California Super Lawyer in 2011 and 2012. She is a graduate of Spelman College and the University of Texas School of Law.

INTRODUCTION

In today's marketplace, businesses cannot survive without the Internet. The Internet allows companies to expand sales and to develop and maintain relationships with customers, and allows employees to communicate with each other concerning all aspects of the business. Along with all of the advantages of the Internet, there have also been disadvantages, especially in the workplace. This article addresses what social networking and social media mean in the workplace, discusses issues that employers might encounter, offers tips for employers to guard against issues relating to social networking both on and off duty hours, and concludes with a checklist of steps an employer can take to prevent issues before they arise.

SOCIAL NETWORKING AND SOCIAL MEDIA

The terms "social networking" and "social media" are often used interchangeably to refer to information that is exchanged from person to person over the Internet. In short, "social media has converted the Internet from a read-only encyclopedia into an interactive, second-by-second communication forum with the world as the audience." Gevertz & Greenwood, *Crafting an Effective Social Media Policy for Healthcare Employees*, 22 Health Law 28 (Aug. 2010). Some highly visible forms of social media that are regularly used include Twitter, Facebook, MySpace, LinkedIn, and YouTube. In addition, many websites offer a forum for blogging. Although the Internet is the vehicle for most forms of social media, other burgeoning technologies include text messaging and smart phones with the capability to share media, such as Apple's iPhone.

EMPLOYMENT ISSUES CONCERNING SOCIAL NETWORKING AND SOCIAL MEDIA

Over the last several years, social media use has risen dramatically. For example, one study indicates that in June 2010 there were more than 92 million unique visitors on Twitter—a 109-percent increase from the previous year. Press Release, *Indonesia, Brazil and Venezuela Lead Global Surge in Twitter Usage* (Aug. 11, 2010), available at http://www.comscore.com. With the increased use of social media overall, employers may assume that social media usage during work hours has also increased. Another study suggests that 61 percent of employees in the United States accessed their Facebook accounts during working hours an average of 15 minutes per day. See Nucleus Research Study, *Facebook: Measuring the Cost to Business of Social Networking* (July 2009), available at http://nucleusresearch.com.

With the staggering growth of social media, companies and their legal counsel have been presented with novel ways in which employees may bring claims against their employers. Companies and their counsel must learn new laws that impact employer-employee relations as a result of the increased use of social media and must develop new policies that address social networking and social media usage in the workplace.

Examples of potential misconduct associated with the use of social networking in the workplace include:

- Breach of employee privacy;
- Disclosure of company trade secrets and confidential information;
- Employee gripe sessions;
- Harassment and Title VII issues;
- Defamation;
- Misuse of intellectual property;
- Excessive use of social media during working hours;
- Pornography and obscenity;
- Union organizing;
- Unauthorized and deceptive endorsements; and
- Violations of other employment policies.

In addition to the case law addressing these activities, federal and state statutes affect the use of social networking and help define the parameters of acceptable use. Relevant federal statutes include the National Labor Relations Act (29 USC §§151–169); the Federal Trade Commission Act (15 USC §§41–58); the Stored Communications Act (18 USC §§2701–2712); the Wiretap Act (18 USC §§2510–2522, 2701–2712), and the Fair Credit Reporting Act (15 USC §§1681–1681x).

Accessing Employees' Social Networking Websites

Access Using Employee Passwords

Although employers may want access to social websites where employees may be communicating, employers must be careful not to pressure employees into providing passwords or other authorizations for access to restricted social media websites because doing so may violate the Stored Communications Act and other federal and state laws.

On September 27, 2012, Governor Brown signed two bills that increase privacy protections for social media users in California. Assembly Bill 1844, to be codified at Lab C §980, prohibits employers from demanding user names, passwords, or any other information related to social media accounts from employees and job applicants. Further, employers are banned from discharging or disciplining employees who refuse to divulge such information. The prohibition does not apply to passwords or other information used to access employer-issued electronic devices. The new law also stipulates that nothing in its language is intended to infringe on employers' existing rights and obligations to investigate workplace misconduct. Proponents of the bill intended AB 1844 to be a common-sense measure that would bring clarity to a murky area of employment law and would stop business practices that impede employment. A similar bill, SB 1349, to be codified at Ed C §§99120–99122, establishes a similar privacy policy for postsecondary education students with respect to their use of social media. Although the bill prohibits public and private institutions from requiring students, prospective students, and student groups to disclose user names, passwords, or other information about their use of social media, it stipulates that this prohibition does not affect the institution's right to investigate or punish student misconduct. Senate Bill 1349 was intended to stop what was perceived to be a growing trend of colleges and universities delving into student social media accounts, particularly social media accounts of student athletes.

This recent action by the California state legislature followed at least one previous court decision holding that an employee who was pressured by her employer into divulging her password had not given effective authorization to her employer to access her MySpace account. See *Pietrylo v Hillstone Restaurant Group* (D NJ, Sept. 25, 2009, No. 06–5754 (FSH)) 2009 US Dist Lexis 88702, *8 (unpublished opinion). See also *Pietrylo v Hillstone Restaurant Group* (D NJ, July 24, 2008, No. 06–5754 (FSH)) 2008 US Dist Lexis 108834 (unpublished opinion). In the *Pietrylo* case, an employee of a restaurant created a webpage on MySpace called the "Spec-Tator," where employees could vent about their workplace. The webpage could be accessed only if the user was invited and if the user had a (password-protected) MySpace account. On more than one occasion, managers from the restaurant accessed the webpage by requesting a password from another employee. The employee who gave her password to the managers believed that she had to do so; she "felt that [she] probably would have gotten in trouble" otherwise. 2009 US Dist. Lexis 88702 at *8. Two employees were terminated for comments made on the webpage. The employees brought suit claiming, among other things, violations of the Stored Communications Act. See 18 USC §2701(c)(2). The defendants argued that if access to Spec-Tator was authorized "by a user of that service with respect to a

communication of or intended for that user," there should be no violation. The plaintiff argued that the defendants did not have proper authorization and that there had been an invasion of privacy. The case went to trial, and the jury found that the company's managers unlawfully accessed the webpage on five occasions. The court ruled that once the managers were aware that the other employee had reservations about giving them her password, the managers should have known that they were not authorized to continue accessing the webpage. 2009 US Dist Lexis 88702 at *10.

Access Under False Pretenses

Employers must also refrain from entering restricted websites under false pretenses to gain access, because doing so may violate federal laws such as the Stored Communications Act or the Railway Labor Act. In *Konop v Hawaiian Airlines, Inc.* (9th Cir 2002) 302 F3d 868, the plaintiff airline pilot established a website where he posted information that was critical of the airline's management and its proposal for wage concessions in the existing collective bargaining agreement. As part of the website, he set up passwords and required visitors to log in with a username. He also created a list of people who were eligible to view the contents of the website, specifically excluding company management. The company vice president asked one of the other employees who were eligible to view the website for permission to use his name to access it because the company was concerned about untruthful allegations that the plaintiff was making on the site. The plaintiff filed suit against the company claiming, in part, that the company viewed his website without authority and under false pretenses. He alleged that after the company vice president gained access to the website, the vice president disclosed the website's contents to a rival union faction. The plaintiff also contended that he was subjected to intimidation and threats of defamation lawsuits later, partly because of the information provided to the incumbent union by the vice president.

The airline company argued that there were no violations of law because the other employee had voluntarily provided his information to the company's vice president to access the plaintiff's website. The court held, however, that because there was no evidence that the other employee ever actually viewed the website, the vice president might not be an authorized "user" under the Stored Communications Act. See 18 USC §2701(c)(2) ("user" is a person who *uses* service and is authorized to do so). The plaintiff argued that because the other employee never used the website, he was not a "user" at the time he gave the vice president access. 302 F3d at 880. The court also held that the vice president may have violated the Railway Labor Act (45 USC §§151–188) because he accessed the plaintiff's website under false pretenses and provided the information he discovered on the website to the plaintiff's incumbent union. The court reversed and remanded the case to the lower court to address whether the company violated the Stored Communications Act and the Railway Labor Act.

Risk of Legal Action

Accessing an employee's social networking website may expose the employer to legal action. In an unreported case, the United Food and Commercial Workers Local 1500 filed charges with the NLRB regional office in Brooklyn, claiming that an employer's social media policy was impermissibly vague and overbroad and violated its employees' rights under Section 7 of the National Labor Relations Act (NLRA) (29 USC §§151–169; see 29 USC §157). The policy prohibited employees from disclosing confidential information, either externally or to fellow employees, and from discrediting the employer's services or products on social networking sites such as Facebook and Twitter. See Law360, *Union Targets Stop & Shop Over Facebook Policy* (Mar. 30, 2012).

Facebook's Position

Facebook, Inc. has vowed to try to end certain employers' practice of asking current and prospective employees for access to their social media accounts, joining a growing outcry that the practice is an invasion of personal privacy and a gateway to legal liability. According to Facebook's Chief Privacy Officer, Erin Egan, requests for access to individuals' Facebook profiles or private information "undermine the privacy expectations and the security of both the user and the user's friends," violate Facebook's terms of use, and "potentially expose the employer who seeks this access to unanticipated legal liability." Law360, *Facebook Wants Employers Out Of Workers' Profiles* (Mar. 23, 2012), available at http://www.mintz.com/media/pnc/0/media.2880.pdf. Facebook's position is, of course, consistent with the new California legislation discussed above.

Access to Public Websites

In contrast to private websites, employers desiring to access public websites will likely not violate privacy laws. In *Moreno v Hanford Sentinel* (2009) 172 CA4th 1125, 91 CR3d 858, the plaintiff wrote an article called "An Ode to Coalinga" that made a

number of negative comments about the inhabitants of Coalinga, where the plaintiff had grown up. The plaintiff posted the article on her MySpace page and "made her article available to any person with a computer and thus opened it to the public eye." 172 CA4th at 1130. A high school principal in Coalinga downloaded the article and submitted it to a local paper, which published it with the plaintiff's name. As a result, the plaintiff's family was harassed. The plaintiff filed suit alleging, among other things, invasion of privacy. The court held that the plaintiff's claim failed because she had no expectation of privacy once she posted her article on MySpace and made it available for anyone with Internet access.

Monitoring Employees' Off-Duty Social Media Activity

An employer is unlikely to have any duty to monitor an employee's off-duty social media activity. In *Maypark v Securitas Sec. Servs. USA, Inc.* (Wis App 2009) 775 NW2d 270, a security guard who worked for the defendant took photo badges of female employees from a work site, ejaculated on them, and posted them on an adult website from his home. When the employer found out, it fired the security guard immediately. A group of female employees sued the company for negligently training and supervising the security guard. The appeals court reversed judgment for the female employees, instead finding in favor of the company. The court held that "employers have no duty to supervise employees' private conduct or to persistently scan the world wide web to ferret out potential employee misconduct." 775 NW2d at 276.

If, however, an employer has knowledge that employees are using a work-related forum, such as an electronic bulletin board, to harass another employee, the employer may have exposure if it fails to take effective measures to stop the harassment. In *Blakey v Continental Airlines, Inc.* (NJ 2000) 751 A2d 538, a female pilot brought claims of discrimination and retaliation against the airline. During the litigation, the airline's employees used an on-line computer bulletin board to post negative comments about the plaintiff. The plaintiff claimed that the comments were false and defamatory and insisted that the airline was responsible for preventing the conduct because it was aware of the posts. The court discussed whether an electronic bulletin board, not physically in the workplace, is nonetheless so closely related to the workplace that it should be regarded as part of the workplace. On remand, the lower court was instructed to determine whether the relationship between the electronic bulletin board and the airline established a connection to the workplace sufficient to impose liability on the airline. If such a connection exists, an employer who has notice that its employees are engaging in a forum that is harassing to another employee has a duty to remedy the harassment.

If an employer has knowledge that employees are using a work-related forum, such as an electronic bulletin board, to harass another employee, the employer may have exposure if it fails to take effective measures to stop the harassment.

Monitoring Personal E-Mail Sent on Company Computers or E-Mail Systems

An employer can monitor personal e-mail sent using a company network if the company has a clear policy to that effect and can demonstrate that the employee in question was aware of the policy. In *Scott v Beth Israel Med. Ctr., Inc.* (NY Sup Ct 2007) 847 NYS2d 436, the plaintiff sued his employer, alleging breach of his employment contract on the grounds that he was entitled to severance pay when he was terminated without cause. The plaintiff sent e-mails to his attorney over the hospital's network using his work e-mail address. The hospital had a clearly written policy stating that employees had no expectation of privacy in e-mail sent through the hospital's network, prohibiting personal use of the network, and providing that the hospital owned all communications on it. The policy language provided as follows (847 NYS2d at 439):

> 1. All Medical Center computer systems, telephone systems, voice mail systems, facsimile equipment, electronic mail systems, Internet access systems, related technology systems, and the wired or wireless networks that connect them are the property of the Medical Center and should be used for business purposes only.
>
> 2. All information and documents created, received, saved or sent on the Medical Center's computer or communications systems are the property of the Medical Center.
>
> 3. Employees have no personal privacy right in any material created, received, saved or sent using Medical Center communication or computer systems. The Medical Center reserves the right to access and disclose such material at any time without prior notice.

Although the plaintiff was communicating with his attorney, the court held that the plaintiff had waived the attorney-client privilege because he had constructive knowledge of the policy, the policy

prohibited personal use of the network, the hospital reserved the right to monitor e-mail, and the computer staff had access to the plaintiff's e-mail stored on the hospital's server.

An employer will likely be prohibited from monitoring an employee's e-mail sent through a company computer from a personal e-mail account, unless the employer has a clear policy prohibiting employees from doing so and employees are aware of the policy. In *Stengart v Loving Care Agency, Inc.* (NJ 2010) 990 A2d 650, the plaintiff sent personal e-mails to her attorney using her personal password-protected web-based e-mail account on a company computer. The plaintiff filed a discrimination suit against the company and the company's computer forensic expert discovered e-mails between the plaintiff and her attorney. The plaintiff demanded the return of all e-mails but the company refused, arguing that the plaintiff had waived the attorney-client privilege. The court held in favor of the plaintiff because there was confusion over which version of the company's e-mail policies applied, it was unclear whether the plaintiff had ever received the e-mail policy, the e-mail policy did not address accessing personal e-mail accounts on company equipment at all, and public policy dictated that such communications be protected. Moreover, by reading arguably privileged e-mails and failing to promptly notify the employee and by using the contents of at least one e-mail in responding to interrogatories, the employer's counsel violated state court rules. See NJ Court Rule 4.4(b); See ABA Model Rules of Prof Cond 4.4.

Monitoring Text Messages

In today's business environment, text messaging has risen dramatically with the increased use of cell phones and other personal communication devices. According to one poll, 65.2 percent of Americans use text as a way to communicate. comScore MobiLens May 2010 Mobile Subscriber Market Share Report (3-month average ending May 2010 versus 3-month average ending February 2010 with age 13 and over), available at http://www.comscore.com/Press_Events/Press_Releases. Text messaging has permeated the workplace, and employers are faced with more issues concerning text messaging and privacy implications.

An employer likely can monitor employee text messages when there are clearly defined legitimate business reasons for doing so. In *City of Ontario v Quon* (2010) ___ US ___, 177 L Ed 2d 216, 130 S Ct 2619, the plaintiff and other police officers sued the city, claiming that their Fourth Amendment and privacy rights were violated when the city reviewed the plaintiff's text messages. The plaintiff, along with the other officers, had been given pagers with monthly character limits. Before receiving the pagers, the city made the employees, including the plaintiff, sign a computer usage, Internet, and e-mail policy. The policy did not specifically mention text messaging, although the city made clear that text messages were to be treated like e-mail. When the plaintiff and other officers exceeded the monthly character limits for several months, the police chief conducted an audit to find out whether the character limit was too low. The city asked the service provider to furnish transcripts of the messages. After review, it was determined that many of the plaintiff's messages were not work-related, but contained sexually explicit content. The court ultimately held that there was no violation of the Fourth Amendment because, in searching the text messages, the city had a legitimate intent that was reasonable (*i.e.*, it was an audit, not a criminal investigation).

An employer likely can monitor employee text messages when there are clearly defined legitimate business reasons for doing so.

The Court also indicated in dicta that employers wishing to monitor company cell phones must create a reasonable expectation with their employees that their communications may be monitored. A company should make sure that its policy is clear and specific and that the policy is communicated to, and acknowledged by, the employees. See 177 L Ed 2d at 227. See, *e.g., Simmons v Southwestern Bell Tel. Co.* (WD Okla 1978) 452 F Supp 392, 394, aff'd (10th Cir 1979) 611 F2d 342 (plaintiff did not have "reasonable expectation of privacy" in his personal conversations on work telephones when he knew that his telephone conversations could be, and were being, monitored).

How to Handle Blogging—Anonymous or Not

Many times an employee or former employee vents about his or her employer by blogging on the Internet. Sometimes the employer knows the identity of the blogger; other times it does not. Regardless, the employer needs to be careful about how it addresses bloggers because the blogging activity may involve issues of privacy and issues under the National Labor Relations Act.

For example, an NLRB administrative law judge (ALJ) has ruled that an employer's social media

policy that prohibited employees from discussing work-related legal matters without express permission from the company's legal department violated federal labor laws. The ALJ, however, upheld the company's ban on posting photographs of uniformed employees. Although the policy's provision concerning discussion of legal matters did not restrict the employees' Section 7 rights expressly, the ALJ ruled that it could be reasonably construed to prevent the employees from discussing working conditions and other terms and conditions of employment, particularly when the discussions concerned potential legal actions by employees. See Law360, *NLRB Judge Slams Security Co.'s Ban On Social Media Talk* (Apr. 2, 2012).

NLRB GENERAL COUNSEL'S POSITION

The NLRB Office of General Counsel has taken the position that many provisions often seen in employers' social media policies violate the NLRA. See NLRB Assoc. Gen. Counsel Memo OM 12–31 (Jan. 24, 2012) (Jan. 2012 Report), available at http://mynlrb.nlrb.gov/link/document.aspx/09031d45807d6567. See also NLRB Assoc. Gen. Counsel Memo OM 12–59 (May 30, 2012) (May 2012 Report), available at http://www.nlrb.gov/news/acting-general-counsel-releases-report-employer-social-media-policies; NLRB Assoc. Gen. Counsel Memo OM 11–74 (Aug. 18, 2011), available at http://mynlrb.nlrb.gov/link/document.aspx/09031d458056e743. The May 2012 Report includes an example of a social media policy that was approved by the NLRB's General Counsel.

No Defamation/Nondisparagement

According to the General Counsel, a broad nondisparagement policy is a *per se* violation of the NLRA because such a policy could inhibit employees from making negative comments about the terms and conditions of their employment. The General Counsel stated that the following policy prohibition was overbroad and hence illegal: "[m]aking disparaging comments about the company through any media, including online blogs, other electronic media or through the media." Jan. 2012 Report, at 4. The General Counsel reached the same conclusion with respect to a policy that prohibited "discriminatory, defamatory, or harassing web entries about specific employees, work environment, or work-related issues on social media sites." Jan. 2012 Report, at 16.

However, by including nondisparagement policy language within a list of other forms of unprotected conduct, an employer's nondisparagement policy will comply with the NLRA. In the Jan. 2012 Report, at 16, the General Counsel gave its stamp of approval on a policy that:

> prohibited the use of social media to post or display comments about coworkers or supervisors or the employer that are vulgar, obscene, threatening, intimidating, harassing, or a violation of the employer's workplace policies against discrimination, harassment, or hostility on account of age, race, religion, sex, ethnicity, nationality, disability, or other protected class, status, or characteristic.

Discussions of Work-Related Concerns

One policy discussed in the General Counsel's Jan. 2012 Report required employees to discuss with their manager or supervisor first any work-related concerns, and provided that any failure to comply could result in corrective action, including termination. The General Counsel concluded that this policy violated the NLRA because of the threat of discipline. Jan. 2012 Report, at 15. Employers can avoid this potential pitfall by urging, but not mandating, that employees use internal channels, rather than social media, to resolve workplace concerns.

Confidentiality

According to the General Counsel, a confidentiality policy is illegal if it would impinge on employees' ability to discuss their wages and working conditions with others inside or outside the organization. Consistent with that reasoning, the General Counsel's May 2012 and Jan. 2012 Reports each disapproved confidentiality provisions in employers' social media policies. The General Counsel stated that (May 2012 Report, at 4):

> [R]ules prohibiting the communication of confidential information without exempting Section 7 activity inhibit this right because employees would reasonably interpret such prohibitions to include information concerning terms and conditions of employment.

In contrast, the General Counsel approved a policy provision that "prohibited employees from using or disclosing confidential and/or proprietary information, including personal health information about customers or patients" as well as "'embargoed information,' such as launch and release dates and pending reorganizations." Jan. 2012 Report, at 17.

Logos, Trademarks

A social media policy that prohibits employee use of a company's tradenames, trademarks, or service marks outside the course of business without prior approval of the company's legal department is

unlawful. The General Counsel takes the position that employees have the right under the NLRA to use the company's name and logo (Jan. 2012 Report, at 14)

> while engaging in protected concerted activity, such as in electronic or paper leaflets, cartoons, or picket signs in connection with a protest involving the terms and conditions of employment.

The General Counsel reasoned that such protected use of a company's name and logo does not "remotely implicate[]" the company's interests protected by trademark law. Jan. 2012 Report, at 14.

Employee Disclaimers

Social media policies commonly mandate that employees must include a disclaimer in any social media content that relates to the employer. For example, in one of the cases discussed in the General Counsel's Jan. 2012 Report, the employer's social media policy required that employees "expressly state that their comments are their personal opinions and do not necessarily reflect the Employer's opinions." The General Counsel opined that this policy requirement violated the NLRA because it "would significantly burden the exercise of employees' Section 7 rights to discuss working conditions and criticize the Employer's labor policies." Jan. 2012 Report, at 15.

However, the General Counsel did approve an employee disclaimer requirement in the section of a social media policy addressing product promotions. The General Counsel explained that, in context, this provision could not be read to interfere with Section 7 rights because the policy focused on product promotions and endorsements and was intended to avoid potential liability for unfair and deceptive trade practices under guidance issued by the Federal Trade Commission. See also May 2012 Report, at 15.

Communications With the Media

Social media policies often tell employees not to discuss with the media their social media content related to the company. The General Counsel's Jan. 2012 Report, at 14, found that a rule prohibiting employees from communicating with the media or requiring prior authorization was unlawfully overbroad. However, a company media policy that seeks merely to ensure a consistent and controlled company message and limits employee contact with the media only to that extent should not be interpreted to restrict Section 7 communications. In other words, it appears that employers should still be able to craft a provision on media relations in a social media policy that complies with the NLRA.

"Unprofessional" Content

In several reported cases, the General Counsel took issue with policy terms that were undefined, vague, or subjective. These terms included prohibitions on insubordination or other disrespectful conduct, inappropriate conversation, unprofessional communication that could negatively impact the employer's reputation or interfere with the employer's mission, and unprofessional or inappropriate communication regarding members of the employer's community, as well as a requirement that social media activity occur in an honest, professional, and appropriate manner. See, *e.g.*, Jan. 2012 Report, at 9. Employers can achieve the intended objectives of this disfavored language by using terms that are defined in the social media policy or other policies or by providing examples of prohibited conduct along with examples of conduct that is protected by the NLRA.

Employee's Self-Identification

Some policies prohibit employees from identifying their affiliation with the organization when engaging in social media activity unless there is a legitimate business reason for doing so. The General Counsel has taken the position that this type of policy violates the NLRA because "personal profile pages serve an important function in enabling employees to use online social networks to find and communicate with their fellow employees at their own or other locations." Jan. 2012 Report, at 15. Telling employees not to mention their employer by name in a personal profile is akin to telling them not to do the same at a cocktail party.

Securities Blackouts

Among the few policy provisions with which the General Counsel did not take issue was one that stated that the employer might "request employees to confine their social networking to matters unrelated to the company if necessary to ensure compliance with securities regulations and other laws." Jan. 2012 Report, at 17. The General Counsel reasoned that "employees reasonably would interpret the rule to address only those communications that could implicate security regulations," as distinct from the terms and conditions of their employment. Jan. 2012 Report, at 17.

Concerted Employee Action

The Acting General Counsel continues to take the view that employees using social media to engage in concerted complaints about their employment are protected by the National Labor Relations Act, while

employees who are merely airing individual gripes lack statutory protection.

[T]he NLRB seems to be telling employers that they must have a thick skin when it comes to social media posts by employees that the employer deems inappropriate if those posts involve protected concerted activity.

In one case, an employee working for a chain of home improvement stores, upset that a supervisor reprimanded her in front of a company manager, updated her Facebook status with a comment that included an expletive and the name of the employer. Several individuals, including one co-worker, indicated on the Facebook page that they "liked" the comment, but when the employee later added an online comment that the company did not appreciate its employees, her co-workers did not respond to the posting. The employee was fired due to her Facebook comments. The NLRB concluded that the home improvement company employee was not protected by the NLRA, observing that she (Jan. 2012 Report, at 35)

> had no particular audience in mind when she made that post, the post contained no language suggesting that she sought to initiate or induce coworkers to engage in group action, and the post did not grow out of a prior discussion about terms and conditions of employment with her coworkers.

NLRB General Counsel's 2011 Memorandum on Social Media Cases

On August 18, 2011, the General Counsel of the NLRB issued a lengthy memorandum to all Regional Directors summarizing the NLRB's resolution of "social media cases." Notably, in all of the summarized cases, the employees posted on their own Facebook page, on their own time, and using their own equipment. These cases have three common themes. First, the subject matter of each of the posts at issue related to the terms and conditions of employment, the exercise of rights conferred by the NLRA, or other matters traditionally considered "protected activity" under NLRB precedent. Second, in each of these situations, the General Counsel concluded that employees were collaborating, otherwise known as "concerted activity." Last, in each of the cases, the offending Facebook post was either the culmination of an on-going dispute with the employer or the continuation of a preexisting conversation among employees.

In each of the cases, the offending Facebook posts included offensive comments, such as "swearing and/or sarcasm," use of a "short-hand expletive," or references to management personnel as an "asshole" and a "scumbag." Nonetheless, in each case, the General Counsel concluded that the employer's termination violated the NLRA. Thus, the NLRB seems to be telling employers that they must have a thick skin when it comes to social media posts by employees that the employer deems inappropriate if those posts involve protected concerted activity. See NLRB Assoc. Gen. Counsel Memo OM 11–74 (Aug. 18, 2011), available at http://mynlrb.nlrb.gov/link/document.aspx/09031d458056e743.

The Memorandum also identified social media policy provisions that the General Counsel deemed overbroad and in violation of the NLRA. These provisions included the following commonly used policies:

1. *Inappropriate Discussions*: Prohibition against "inappropriate discussions about the company, management, and/or coworkers."

2. *Defamation*: Prohibition on any social media post that "constitutes embarrassment, harassment or defamation of the [company] or of any [company] employee, officer, board member, representative, or staff member."

3. *Disparagement*: Prohibition against "employees making disparaging comments when discussing the company or the employee's superiors, coworkers and/or competitors."

4. *Privacy*: Prohibition on "revealing, including through the use of photographs, personal information regarding coworkers, company clients, partners, or customers without their consent."

5. *Confidentiality*: Prohibition on "disclosing inappropriate or sensitive information about the Employer."

6. *Contact Information*: Prohibition on "using the company name, address, or [related] information on [employees'] personal profiles."

7. *Logo*: Prohibition on using "the Employer's logos and photographs of the Employer's store, brand, or product, without written authorization."

8. *Photographs*: Prohibition against "employees posting pictures of themselves in any media . . . which depict the Company in any way, including a company uniform [or] corporate logo."

In finding these rules unlawful, the General Counsel emphasized not only their overbreadth, but also that "the rule[s] contained no limiting language to inform employees that [the rules] did not apply to

Section 7 activity." This suggests that a policy will not violate the NLRA as long as the policy contains a disclaimer that explicitly informs employees that the policy will not be construed or applied in a manner that improperly interferes with employees' rights under Section 7 of the NLRA (29 USC §157).

An employer should make clear to its employees that any comment, however slight, about a company product on any social media, requires disclosure of the employer-employee affiliation.

ANONYMOUS BLOGGERS

When handling an anonymous blogger who posts negative information about the company, an employer may or may not be entitled to identification of the blogger. See *Krinsky v Doe 6* (2008) 159 CA4th 1154, 1178, 72 CR3d 231 (refusing to enforce subpoena to identify anonymous blogger whose "rude and childish posts [were] intemperate, insulting, and often disgusting"; they were not actionable because they fell into area protected by First Amendment and were merely "crude, satirical hyperbole"). But see *Cohen v Google, Inc.* (NY Sup Ct 2009) 887 NYS2d 424 (finding that Google and Blogger.com were required to provide account data and enforce subpoena to identify blogger of "Skanks of NYC" blog because references to plaintiff were factual, and if proven false, could support defamation claim).

COMMENTS ABOUT COMPANY PRODUCTS ON SOCIAL MEDIA WEBSITE

An employer should make clear to its employees that any comment, however slight, about a company product on any social media, requires disclosure of the employer-employee affiliation. Often, employees may post reviews about their company's products or services on social media websites. Unfortunately, many times, the employee does not discuss his or her affiliation with the company, which can run afoul of Federal Trade Commission regulations. In a recent settlement, a public relations firm agreed to settle FTC charges that it advertised its clients' gaming applications deceptively by having its employees pose as ordinary customers and post reviews on a website concerning particular games without disclosing that they worked for the company. The FTC noted that the employees should have disclosed their affiliation with the company because these "facts would have been relevant to consumers who were evaluating the endorsement and deciding whether to buy the gaming applications." Press Release, Public Relations Firm to Settle FTC Charges that It Advertised Clients' Gaming Apps Through Misleading Online Endorsements, Aug. 18, 2010, available at http://www.ftc.gov/opa/2010/08/reverb.shtm.

CHECKLIST FOR PREVENTING SOCIAL MEDIA ISSUES

Although there are many potential social networking landmines that an employer must navigate, there are several relatively easy steps that every employer can take to decrease potential liability.

- Make sure that new hires are properly trained on the importance of social media.
    - Prepare a policy or addendum to the employee handbook that discusses the importance of social media and the impact that it has on the workplace and organization. Reinforce the importance of reporting concerns and clarifying questions with supervisors and management before posting something that may be inappropriate or that violates the law.
    - Prepare additional policies that address specific concerns such as personal emails and texts from company computers, use of company email or other technology to send personal messages, protection of trade secrets, and promotion of company products on social media websites.
    - Make sure that any policy is acknowledged by the new hire in writing and maintain copies in the personnel file.
- Create clear social media policies that leave little room for ambiguity and ensure that every employee acknowledges those policies.
- If an employer wishes to gain access to restricted social media websites, consider the following:
    - Try to obtain voluntary consent from an employee to access the website by asking the employee if he or she is willing to execute a consent form. It is important that the employee understand that he or she is providing the employer with the password. Consider having the employee's signature witnessed.
    - Ask if the reporting employee is willing to provide a screen shot of the social media site.

  - Make sure the employee understands that he or she will not be punished or retaliated against in any way if the employee is not willing to provide a password or voluntary consent, or revokes the consent at a later time.

- If an employer wishes to safeguard its ability to review personal e-mails or text messages, consider the following:
  - Prepare a policy that notifies the employee that the employer may review any communication sent over the company network, regardless of whether it is over the company e-mail or text messaging system or it involves a personal account using a company device.
  - In the policy, notify the employee that his or her communications are subject to review even after the employee leaves, regardless of whether they concern business or personal communications.
  - Make sure that the policy covers personal accounts that are accessed during work hours from company systems.
  - Make sure that the policy expressly covers text messages and other forms of communication on personal handheld devices supplied by the employer.
  - Make sure that the employee clearly and expressly acknowledges receipt and his or her understanding of the policy.
- If an employer discovers blogs that negatively affect the employment relationship, do not immediately file suit but consider potential alternatives.
  - Investigate the social media website that posted the blog to determine whether the blog violates the website's terms of use. Request that the blog be taken down.
  - Prepare a provision in the employer's electronic policy statement that prohibits employees from anonymous postings about the company and requires employees to disclose their identity when they are communicating on a blog about the employer.
  - Prepare a demand letter and request that the negative posting be taken off the website, particularly if the posting is by a former employee who may be engaging in defamation.
  - Simply ignore the posting, because, like the news, today's headlines are easily forgotten within a few days. Allow for a cooling off period and gauge the likelihood that negative comments may tarnish the company image or sales.
- Before taking action against an employee for off-duty conduct that involves use of social media, check the relevant state statutes to determine whether such conduct is protected. For example, many state statutes protect employees for off-duty conduct such as political activity, consumption of lawful products, or other conduct. See, *e.g.*, Lab C §96(k) (Labor Commissioner will take assignments of claims for wages lost resulting from demotion, suspension, or discharge from employment for lawful conduct occurring during nonworking hours away from employer's premises).
- If the employer has taken action against an employee for violating one of its policies on social media or use of the company network, be very careful about monitoring Internet usage or technology because it can be seen as retaliatory after a complaint is filed. In *Zakrzewska v The New School* (SD NY 2008) 543 F Supp 2d 185, 187, the court allowed the plaintiff to amend her complaint to allege that she was retaliated against after complaining of discrimination because her employer engaged in covert monitoring of her personal Internet use at work. The court indicated that such retaliation could dissuade a reasonable employee from making a complaint about discrimination.
- Once litigation begins, consider sending out a preservation letter to opposing counsel directing the employee to preserve all communications on any company device such as a smart phone, portable laptop, personal handheld device, or iPad.
- When entering into settlement negotiations, consider postings that need to be removed on social media websites. As part of the settlement, consider including in the agreement provisions that require the employee to cooperate with the employer to remove negative comments from websites, to agree not to post negative comments in the future, and to provide a list and location of all social media websites on which the employee has posted negative communications.