The Metropolitan
Corporate Counsel®

www.metrocorpcounsel.com

Volume 19, No. 8 August 2011

Social Media In The Workplace: The New Frontier

The Editor interviews ***Patrick T. Collins****, Member, Norris McLaughlin & Marcus, P.A.*

Editor: Please tell us about your background and experience.

Collins: I have been with the firm for 27 years where I chair our labor and employment group in New Jersey. I practice exclusively in that area on behalf of management.

Editor: Please tell us about your seminar on July 27, entitled Social Media and Technology in the Workplace (the Seminar).

Collins: We regularly conduct seminars for clients and other friends of the firm. At these programs, we ask for feedback about topics they would like us to cover in the future. Social media was the runaway winner. For employers, it is an unsettled area, particularly with respect to screening and background checks of job applicants, the use of social media in the workplace and protected concerted activity. How have social media sites affected these activities and what case law is out there to guide companies? Corporate policies regarding harassment, discrimination, and even bullying have been in place for a long time but may not be sufficient to cover use of social media.

Editor: What makes an employment policy with respect to social media – or unlimited Internet access – in the workplace effective?

Collins: Policies should be suited to each company's workplace. A manufacturing facility will be completely different from an office setting, the latter being more computer based. Some employers actually send employees for training about Twitter and Facebook and how social media can be used in connection with job responsibilities. It is critical for these employers to define permissible workplace behavior for these now highly educated users. An employer may be less concerned about social media in a manufacturing workplace, but all employers should pay attention to company-related activities on the Internet.

Patrick T. Collins

There is a fine line between a policy's being broad enough to cover legitimate issues and being so all-encompassing that an outside agency, such as the NLRB or a court, might determine that it infringes on employee rights. The main objective is to protect the company and its assets. Provisions that address the critical issue of confidentiality and use of technology should be specific, for example, regarding the use of camera phones in the office, and all policies must be communicated via customized training to managers and employees.

Editor: Can these policies be enforced without encroaching on First Amendment rights or unduly regulating employees' off-duty behavior?

Collins: Yes, policies can be enforced if they are written and implemented carefully. However, as with many employment-related issues, it is important to be aware of individual state laws. Some states, like New York, have a very broad statute about off-duty conduct, with generous protections against discrimination or adverse job action for employees engaged in legal behavior. The key is to be aware of the law and important protections for free speech or concerted activity, which applies equally to union and nonunion employees.

Editor: What are some examples of protected employee concerted activity? When do informal discussions among colleagues leave the realm of protected activity under the National Labor Relations Act (NLRA)?

Collins: Concerted activity is a longstanding concept within the NLRA, with Section 7 protecting employees' right to discuss the terms and conditions of their employment with coworkers or third parties. Now, instead of conversations at the lunch table, employees are talking on Facebook.

An early National Labor Relations Board (NLRB) case addressing concerted activity and social media was *American Medical Response of Connecticut, Inc. and International Brotherhood of Teamsters*, which involved an employee who complained about her supervisor on Facebook and made off-color comments in online discussions with coworkers. When the company invoked internal policy and tried to stop the activity, the NLRB stepped in, asserting (a) the activity constituted concerted activity, including the protection of the employee's right to discuss working conditions with coworkers, and (b) the company's policy was too broad. What made this case so provocative was that the online discussions took place during off hours – on Facebook and on the employee's private computer.

Editor: Does the law currently distinguish between public posts and private messages on Facebook or Twitter?

Collins: It's a good question. The real distinction in the *American Medical* case involves whether the employee would be subject to discipline if she used these same vulgarities in direct conversation with her supervisor. The fact that she was discussing work issues with coworkers sets the case on a narrower path from the NLRB's perspective on protected activity.

There was another case involving an Arizona newspaper reporter who was reprimanded for posting sarcastic comments on Twitter, remarking that there were no

Please email the interviewee at ptcollins@nmmlaw.com with questions about this interview.

homicides in Tucson – so far – on that particular Saturday night. The reporter took issue with being reprimanded, but the NLRB refused to file a complaint because the comments did not pertain to discussion of working conditions with coworkers. Thus, making inappropriate public comments was not protected activity.

The significant aspect of these cases is not the underlying law, which is nothing new, but rather their impact on drafting defensible social media and technology policies. Employers should avoid overly broad language and blanket restrictions that may encroach on employees' right to privacy. The fact that employee communications now are happening on Twitter and Facebook adds complexity but doesn't really change the legal landscape.

Editor: What are some appropriate investigation protocols and corrective actions?

Collins: Effective policies should address this issue, and there is a growing body of cases and decisions available to assist employers with understanding what constitutes private communications. For example, an employer likely should not reserve the unfettered right to search an employee's private Gmail account, even if it is being accessed on a company computer; however, a technology policy could advise employees that the company has a right to and, in fact, will monitor communications. It is appropriate to communicate expectations as to appropriate conduct with respect to social media and technology and to occasionally check to see what is happening on company property.

The Seminar focused on this issue during one of its sessions, which discussed a case involving communication between an employee and her attorney. A New Jersey court upheld the sanctity of attorney-client privilege as trumping any claim by the employer of the right to access such communication. Another case alleged that a supervisor coerced an employee to divulge a personal password to a website account and then logged on and discovered the employee's negative comments about the company. The coercion was deemed inappropriate.

Cases like this help to define boundaries for employers. For example, an employee using a company computer should understand the company's policy with respect to monitoring employee activity. If inappropriate behavior is discovered, then the employee may not have a right to privacy claim. The broader point is that an employer should maintain sound policies and train managers about their responsibilities to monitor employee activity in an appropriate manner. This poses an interesting dilemma, for example, when a supervisor becomes an employee's "friend" on Facebook.

Editor: What specific procedures and training programs do you suggest employers implement? Should training programs be tailored, for example, for managers and HR departments?

Collins: While all employees should be trained about corporate policies, there should be additional training guidelines that address responsibilities of managers in all areas of employment law. Specific emphasis should be placed on company risks associated with confidential information, which necessitates training on privacy laws and on how different states treat off-duty conduct. Managers must have a solid understanding of their company's culture and what behavior and situations the company will or will not find acceptable. If, for example, an employee simply attends a party and then posts pictures on a Facebook page, should this send an alarm? Likely not, but managers must be trained on how to be sensitive to these issues.

Social media have inspired terms like "netiquette," referring to the style of online versus face-to-face or formal written communication. Corporate policies should address emails, texts or tweets that may include informal or imprecise abbreviations, particularly since email, for example, has become a predominant method of communication – even in the legal field.

Editor: Are corporations using social media to enhance marketing efforts or boost the company's reputation? What role does blogging play?

Collins: When we were doing research for the Seminar, I was impressed by the numbers and sheer volume of corporations embracing social media for marketing efforts. Coca-Cola, for example, has 35 million Facebook friends, with 50,000 joining every day, and there are thousands of other companies on Facebook.

One area of concern for companies selling products is with comments and the possibility that they will be considered endorsements. If employees are making comments about their company's product, there are Federal Trade Commission (FTC) guidelines on revealing the connection between the employee and the employer. This is an additional area of law to consider when companies use social media as a marketing tool.

Companies and law firms also use blogs, and I refer to certain blogs regularly in my practice. In fact, our firm maintains several law blogs in which partners are actively involved. Blogs should be kept current and accurate, with proper disclaimers.

Editor: To what degree are corporations relying on social media to evaluate job candidates? Is this a good strategy for conducting background checks?

Collins: This was another Seminar topic. A January 2010 Microsoft survey reflected that nearly 80 percent of companies surveyed said that managers and recruiters consider online information during the hiring process, with 70 percent reporting that they have rejected candidates – before an interview – based upon what they viewed on social media sites.

This is another area requiring specific training. While basic employment law precludes asking direct questions about age, disabilities or other protected classifications, a picture posted on Facebook may divulge this information and present a very difficult problem. If it is discovered that a potential employer viewed a Facebook profile – which may include the candidate's birthday – and then declined employment, the candidate may be able to claim discrimination based on age. While it may be valid to question why the candidate posted this information in the first place – in truth, everyone should consider very carefully what they divulge on social media – the dilemma for employers is not resolved.

Employers still have access to information, for example, under the Fair Credit Reporting Act, and I understand the FTC just approved a background check company's request to use social media as part of its hiring process. This is a developing situation.

Editor: Once an employee is hired, how can companies monitor compliance with policies and procedures?

Collins: First, a company needs to understand how and to what extent employees are using technology and social media in the workplace. The results may be surprising, reflecting pervasive use of the Internet, blogs and smart phones. Employers should work with IT departments to develop ways to identify and monitor usage, and policies should address the company's right to monitor that activity. At the end of the day, the company must do what is necessary to protect itself.