Employers' Ongoing Challenge: Managing Employees' Social Media Use

by Francine Esposito

Social media is a powerful force that is here to stay. Government protests around the world have been organized through social media and corporate America has come to rely on the expansive low-cost publicity social media provides. Facebook alone now boasts of more than a billion active users.[1] Whether employers know it or not, employees' personal social media use is an unproductive distraction in the workplace—either through company computers that do not block access or through employees' smart phones, and that is in addition to the significant time employees spend on social media off duty. Whenever and wherever employee social media use occurs, the consequences can be devastating to employers, including when employees publicly post embarrassing comments about them; disparage their competitors; unknowingly disclose or even purposefully attempt to steal their confidential information; threaten or harass others; or engage in other undesirable conduct that affects their image and reputation.

Despite the widespread use of social media, employers have been slow to implement policies governing their employees' online activity, either because they are not convinced policies are necessary or they are unsure of the proper content. Moreover, the actions of an aggressive National Labor Relations Board (NLRB)—holding that several commonsense policy provisions (*e.g.*, prohibiting discourtesy, disparagement, and improper use of intellectual property) violate the law[2] and thwarting employers' attempts to hold employees accountable for their undesirable social media use—have left employers unsure of their rights.

Employers are justifiably perplexed and cautious, since legal developments relating to social media use continue, and employers may be liable under various laws, not only for accessing and taking action based on information employees disclose on social media, but also for failing to take action based on this information. In other words, they may be damned if they do and damned if they don't take action based on their employees' posts.

Consequences of Improper Action

Section 7 of the National Labor Relations Act (NLRA) has been employees' most effective claim against employers who take adverse action for social media use. That provision guarantees employees, whether or not they are represented by a union, the right "to engage in…concerted activities for the purpose of collective bargaining or other mutual aid or protection."[3] Protected concerted activity includes when employees collectively voice concerns regarding terms and conditions of employment, or when a single employee seeks to initiate group action or bring group complaints to his or her employer's attention. Such activity often takes the form of public complaints about wages and supervisor conduct. Unlike employees' protected concerted activity of the past, which was limited to water cooler discussions, hand billing or perhaps an ad in a newspaper, current-day employees are able to voice their views to an audience of millions with a few keystrokes.

In the wake of several rulings against employers for disciplining employees for what they viewed to be inappropriate social media use, the acting general counsel of the NLRB issued three lengthy reports applying longstanding interpretations of the NLRA to employees' new-age cyberspace activity in an effort to provide guidance to employers.[4] Indeed, no matter how critical or embarrassing to the employer, employee communications were found to be protected concerted activity, since they stemmed from employees' terms and conditions of employment and ongoing discussions with their coworkers. The NLRB found it irrelevant that employees may

have cursed or used various derogatory terms to describe their management, including crook, stupid and other terms not fit to print.[5] The NLRB viewed these comments and related sarcasm to be "quite innocuous,"[6] and not "accompanied by verbal or physical threats."[7] The general counsel's report, however, acknowledged that employees' social media posts were more likely to lose the NLRA's protections if they: were merely "individual gripes,"[8] interrupted the work of others,[9] undermined supervisory authority,[10] were threatening,[11] were "disloyal, reckless, or maliciously untrue"[12] (a standard used in 1953 for disparaging comments about an employer or its products in the context of appeals to third parties), or were "opprobrious"[13] (a 1979 standard used for public outbursts against supervisors). Unfortunately, no detailed guidance regarding the type of social media posts that would meet these older standards decades later, in today's technological world, was provided, and rulings in favor of employees deemed to have engaged in protected concerted activity continue.[14] Employee rights under the NLRA are somewhat analogous to the well-established constitutional rights of public employees to engage in speech regarding matters of public concern.[15]

In addition to the above, employers have long known they cannot discriminate against applicants or employees based on an individual's membership in a legally protected classification.[16] Social media makes these issues so much more complicated. Employer decision makers now have greater access to and knowledge of a whole other level of personal information about applicants and employees (most of whom have no concept of how to use security settings) than they would otherwise glean in the workplace, including these individuals' religion, national origin, disability or association with disabled individuals, genetic information and sexual orientation. Whether this personal information was actually considered in making adverse employment decisions will inevitably lead to litigation. When that happens, how does the decision maker prove a negative? How does one unring a bell?

Discrimination may occur during the hiring process, since many employers now search for and evaluate applicants' social media presence to determine whether the individuals would be a 'good fit' with their organization. In March 2014, the Equal Employment Opportunity Commission (EEOC) and the Federal Trade Commission (FTC), the agency enforcing the Fair Credit Reporting Act (FCRA), issued a joint publication explaining how federal discrimination laws and FCRA apply to background checks in connection with employment decisions, and specifically warned employers against using information obtained from social media to discriminate against employees.[17] It is also important to note that employers who hire third parties to check the social media presence of an applicant or employee without giving prior notice and receiving prior consent from the individual may violate FCRA.[18]

Discrimination may also occur when managers, who become aware of certain information through 'friending' their subordinates on social media, subsequently find themselves having to take adverse employment action against those individuals. Further, what constitutes actionable conduct under anti-discrimination laws is sometimes surprising. The EEOC regulations interpreting and enforcing the Genetic Information NonDiscrimination Act of 2008 (GINA),[19] the first major non-discrimination law passed after the advent of social media, suggest that an employer may violate the law when a manager purposefully returns to a social media site to obtain additional genetic information about an employee after initially stumbling upon some information inadvertently.[20]

Federal and state computer use laws may create liability for employers as well. In 2009, a New Jersey jury awarded back pay and punitive damages to employees who were discharged for their rants about their supervisors and customers on an invitation-only MySpace page.[21] The employer was found to have unlawfully coerced an employee, who had come forward to report her coworkers' conduct, to provide access to the private site, and to have surreptitiously monitored employees' postings in violation of the federal Stored Communications Act[22] and the parallel New Jersey law.[23] Reliance on these laws, to some extent, is no longer necessary. In 2014, Governor Chris Christie signed a law prohibiting employers from requiring applicants and employees to provide a user name, password or other access to their personal social media accounts, and from discriminating or retaliating against individuals for refusing to comply with an improper request, filing a complaint, participating in an investigation, or otherwise opposing violations of the law.[24] Aggrieved individuals can seek redress through the New Jersey Department of Labor. The law, however, grants employers latitude to investigate, upon receipt of specific information, employee misconduct or transfer of confidential information.

Consequences of Not Taking Proper Action

Employers are well aware of their obligation to provide a harassment-free work environment. Employees' social media use could result in actionable harassment in numerous ways, and employers may face liability if they fail to prevent or stop the conduct about which they were aware or should have been aware. As such, liability is much more likely when managers are arguably aware of the harassment due to their

social media connection with the offending employee and/or victim. Further, employers should be hesitant to take the position that employees' social media postings are off-duty issues for which they are not responsible. Employers very well may be responsible, depending upon the circumstances.[25]

Employers may face negligent hiring or retention claims[26] when an individual's social media posts demonstrate that he or she is not suited for the particular employment or possesses dangerous attributes. For instance, an employer may be liable for injuries incurred by a third party during an accident caused by a drunk tractor trailer driver whose frequent public social media posts reference his binge drinking—an issue about which the employer arguably should have been aware.

Employers may face claims of false advertising based on employees' social media posts. Indeed, FTC guidance has put employers on notice of their potential liability for their employees' online endorsements of their products or services without disclosing the material fact of their employment, even if the comments are not authorized or known by the employer.[27] As such, contrary to most employers' desire that employees avoid referencing themselves as representatives of the company, they must actually instruct employees to disclose the employment relationship under these circumstances in an effort to avoid liability.

The consequences of employers not taking proper action relating to employees' social media use is perhaps greatest when employees disclose the employer's confidential information, such as customer lists, marketing strategies or other proprietary information. Indeed, sales and marketing departments often plow full speed ahead into the realm of social media without conferring with human resources and legal departments regarding the potential legal consequences of doing so. To avoid this issue, employers must treat the information they wish to protect as confidential, implement effective policies, and educate employees on the proper use of social media. Unfortunately many employers merely rely on cookie-cutter policies obtained on the Internet, rather than thoughtfully drafting one of their own, tailored to their specific concerns. Employers should also remain vigilant in policing employees' violations of confidentiality obligations. Indeed, an employee was recently made to forfeit his settlement payout in an employment litigation since his daughter's comments about the settlement on Facebook violated his confidentiality obligations.[28]

Confidential information is often lost when employees whose responsibilities included work-related social media use attempt to take the substantive content and/or significant contacts created over a period of time using the employer's resources when they leave the company. Indeed, disputes have occurred over the ownership of Twitter and LinkedIn accounts where employers did not specifically set forth, in policies or preferably formal agreements, who owns the work-related social media accounts.[29] Further, employers may violate wage and hour laws when they fail to pay non-exempt employees for work-related social media use performed outside of work hours.

Lastly, employers forego a significant benefit in defending litigation if their counsel fails to research employees' social media use. Most plaintiffs who sue their employers put their mental state at issue by seeking damages for emotional distress allegedly caused by their employer. Social media postings are akin to diaries, which have traditionally and routinely been requested during discovery. Social media content, however, is even better, as it often includes photographs, including those of purportedly distraught former employees clearly enjoying life. Plaintiffs may also post other information relevant to their claims. As such, employers should request information regarding employees' social media use during discovery—both the identification of accounts and relevant content. Indeed, a federal court in New Jersey recently approved a jury instruction of adverse inference against a plaintiff who intentionally destroyed relevant Facebook postings requested during discovery.[30]

Conclusion

Although employers cannot prohibit all employee social media use they consider to be undesirable, they may nonetheless take reasonable steps to protect their interests through well-thought-out policies and agreements tailored to their specific workplace, diligent and appropriate monitoring of social media, training of managers and employees regarding the pitfalls of social media use, and well-reasoned employment decisions. Most importantly, employers should confer with counsel whenever they are unsure of whether their action, or inaction, may cause liability under the constantly evolving law relating to social media use. ⚖

Francine Esposito *is a partner at Day Pitney LLP, and has practiced both labor and employment law on behalf of management for over 20 years. She regularly drafts policies and conducts seminars on social media and other employment-related issues.*

ENDNOTES

1. *See* Company Info, Facebook Newsroom, Facebook, newsroom.fb. com/company-info/ (last visited Oct. 3, 2014).
2. *See, e.g., Costco Wholesale Corp.,* 358 NLRB No. 106 (Sept. 7, 2012) *vacated by Costco Wholesale Corp. v. NLRB*, 2014 U.S. App. LEXIS 14895 (D.C. Cir. Aug. 1, 2014) (*citing NLRB v. Noel Canning*, 134 S. Ct. 2550 (U.S. 2014)); *Karl Knauz Motors*, 358 NLRB No. 164 (Sept. 28, 2012).
3. 29 U.S.C. § 157.
4. *See NLRB Operations Memorandum* OM 11-74 (Aug. 18, 2011), OM 12-31 (Jan.

14, 2012) and OM 12-59 (May 30, 2012).
5. OM 11-74 at 5.
6. *Id.* at 4.
7. *Id.* at 6.
8. *Id.* at 17.
9. *Id.* at 5, 11.
10. OM 11-74 at 11.
11. *Id.* at 6.
12. *Id.* at 9.
13. *Id.* at 4, 9.
14. *See, e.g., Hispanics United of Buffalo*, 359 NLRB No. 37 (Dec. 14, 2012) (Facebook postings regarding a colleague's *criticism* of their job performance); *Design Tech. Grp., LLC d/b/a Bettie Page Clothing*, 359 NLRB No. 96 (April 19, 2013) (Facebook postings regarding a manager's poor handling of employee safety concerns); *Three D, LLC, d/b/a Triple Play Sports Bar and Grille*, 361 NLRB No. 31 (Aug. 22, 2014) (Facebook postings criticizing the employer's payroll tax withholding practices).
15. *But see In re Tenure Hearing of Jennifer O'Brien*, Civil Case No. A-2452-11T4, 2013 N.J. Super. Unpub LEXIS 28 (N.J. Super. Ct., App. Div. Jan. 11, 2013), upholding the propriety of a discharge of a tenured teacher for facially offensive Facebook comments that were her personal expression of job dissatisfaction and which did not address a matter of public concern.
16. The New Jersey Law Against Discrimination prohibits discrimination against an employee based upon race, creed, color, national origin, nationality, ancestry, age, sex, pregnancy, familial status, marital status, domestic partnership or civil union status, affectional or sexual orientation, gender identity or expression, atypical hereditary cellular or blood trait, genetic information, liability for military service, and mental or physical disability, perceived disability, and AIDS and HIV status. N.J.S.A. 10:5-12.
17. *Background Checks: What Employers Need to Know* (March 10, 2014), available at eeoc.gov/eeoc/publications/background_checks_employers.cfm.
18. 15 U.S.C. §1681, *et. seq*.
19. Genetic Information Nondiscrimination Act of 2008, Pub. L. No. 110-233, 122 Stat. 881 (codified as amended in scattered sections of 26 U.S.C., 29 U.S.C. and 42 U.S.C.).
20. 29 C.F.R. §1635.8.
21. *Pietrylo v. Hillstone Rest. Grp.*, No. 06-5754 (FSH), 2009 U.S. Dist. LEXIS 88702 (D.N.J. Sept. 25, 2009).
22. 18 U.S.C. §§ 2701-11.
23. N.J.S.A. 2A:156A-27.
24. N.J.S.A. 34:6b-5-10.
25. *See, e.g., Espinoza v. Cnty. of Orange*, 2012 Cal. App. Unpub. LEXIS 1022 (Cal. Ct. App. Feb. 9, 2012) (affirming judgment for a plaintiff who was the subject of numerous offensive anonymous disability-related posts on a co-worker's blog).
26. *See Di Cosala v. Kay*, 91 N.J. 159, 173-174 (N.J. 1982).
27. *Guides Concerning the Use of Endorsements and Testimonials in Advertising*, 74 Fed. Reg. 53124, 53136 (Oct. 15, 2009) (codified at 16 C.F.R. § 255).
28. *Gulliver Sch., Inc. v. Snay*, 2014 Fla. App. LEXIS 2595 (Fla. Dist. Ct. App. Feb. 26, 2014).
29. *See, e.g., Eagle v. Morgan,* Civil Case No.11-4303/2013 U.S. Dist. LEXIS 34220 (E.D. Pa. March 12, 2013), for case involving a dispute between an employer and a former executive over ownership of content and access to a LinkedIn account. The court ruled in the executive's favor on several grounds, including unauthorized use of name, invasion of privacy, and misappropriation of publicity, but found the executive could not sufficiently establish damages or causation; *PhoneDog v. Kravitz*, Case No.11-03474 (MEJ) (N.D. Cal. *settlement announced* Dec. 3, 2012), *related proceedings at* 2011 U.S. Dist. LEXIS 129229 (Nov. 8, 2011) and 2012 U.S. Dist. LEXIS 10561 (Jan. 30, 2012), involving a dispute between an employer and former employee over who owned a marketing Twitter account with 17,000 followers. *See also OWS Media Group, Inc. v. Wedes*, N.Y. Sup. Ct., No. 159126/2014, *complaint filed* 9/17/14, a non-employment dispute relating to the rightful owner of the Occupy Wall Street Twitter account.
30. *See Gatto v. United Air Lines, Inc.*, Civil Case No. 10-01090, 2013 U.S. Dist. LEXIS 41909 (D.N.J. March 25, 2013), in which defendant requested access to plaintiff's Facebook account during discovery to refute personal injury claims relating to work-related injury, but plaintiff deleted the account during discovery and did not reactivate it as requested before losing data.