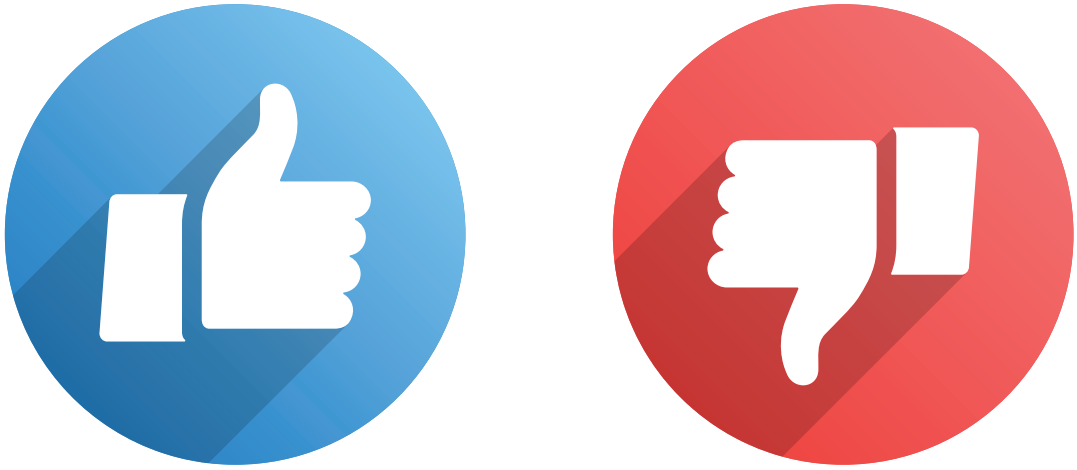

Things to 'Like' and 'Unlike' About Social Media

What Every Employer Needs to Know

by Melissa A. Salimbene and Lindsay Dischley

MELISSA A. SALIMBENE *is a member of the firm at Chiesa, Shahinian & Giantomasi in West Orange, where she practices employment law and commercial litigation.*

LINDSAY A. DISCHLEY *is counsel at Chiesa, Shahinian & Giantomasi in West Orange, where she practices employment law and commercial litigation.*

THE SURGE IN SOCIAL MEDIA use in recent years has permanently changed the way people communicate and interact, in the workplace and elsewhere. Everyone from Generation Z to the Baby Boomer generation is documenting their life on social media and using it as a resource for information. Businesses are also using social media for numerous purposes, including recruiting, customer service, marketing, public relations, and intra-company communications. According to a 2018 report by the University of Massachusetts-Dartmouth, of Fortune 500 companies: 53 percent have blogs; 91 percent have Twitter accounts; 89 percent have Facebook pages; 79 percent have YouTube accounts; 98 percent use LinkedIn; and 63 percent use Instagram.[1]

While social media has brought innumerable benefits to the workplace, these benefits are accompanied by legal challenges. Thus, in order to optimize the value of social media and limit the legal risks, it is crucial that businesses comply with applicable laws when they: 1) use social media when recruiting new talent and making hiring decisions; 2) monitor employees' social media activities; 3) discipline employees based upon such activity; and 4) face legal disputes over ownership of social media accounts used to market the company.

How Can Employers Use Social Media During the Hiring Process?

There are many benefits to using social media in recruiting and hiring. Professional social networking sites, such as LinkedIn, are easy and cost-effective platforms to locate and connect with new talent. These sites also increase visibility by permitting companies to not only advertise open positions online through formal job postings, but also through informal company or employee posts stating "we're hiring."

Employers can also obtain valuable insight into job candidates through a social media review that would not otherwise typically be available in the traditional hiring process, including: exaggeration of qualifications; evidence of violence, illegal drug use or other unlawful activities; sexually explicit activity; a poor work ethic; poor grammar, spelling, or communication skills; or discriminatory tendencies. With seemingly endless information about individuals freely available, it is quite tempting for employers to conduct such reviews when making hiring decisions. In fact, most employers are doing so. According to a 2017 Career Builder survey, 70 percent of employers use social media to screen candidates before hiring, and 54 percent of those employers have discovered content that caused them to not hire a candidate.[2]

The survey also revealed that employers are not just looking for negative content. In fact, 60 percent of employers who conduct social media searches look for information that supports a candidate's qualifications for the job.

There are even circumstances where an employer could incur liability for failing to conduct social media reviews as part of its screening procedures. For example, if a new hire sexually harasses a co-worker and, had the employer conducted a social media search it would have discovered numerous sexually charged posts by the new hire, the harassed co-worker may have a claim against the employer for negligent hiring.

As beneficial and important as social media searches may be, employers must proceed with caution to ensure compliance with applicable laws. The New Jersey Social Media Privacy Law[3] prohibits employers from requiring or requesting an applicant or employee disclose usernames or passwords, or provide access to private social media accounts; however, the law expressly provides that an employer is not prohibited from: 1) accessing or utilizing information obtained in the public domain, such as information contained on non-private, social media pages; or 2) implementing a policy pertaining to employer access to company-issued electronic devices or accounts employees use for business.[4] An employer who violates this law may be assessed civil penalties; there is no private cause of action under the law.[5]

Although employers are not required to obtain consent before reviewing publically available information on social media accounts, employers using third parties to conduct background checks that include a social media search must comply with the Fair Credit Reporting Act (FCRA),[6] which requires an applicant's consent before a third party conducts a background check.

When making hiring decisions based on social media research, businesses must also consider federal, state and local anti-discrimination statutes. These laws prohibit an employer from making employment decisions—including hiring decisions—based upon an individual's protected characteristics. Social media searches may reveal candidates' protected characteristics, such as religion, age, marital and familial status, sexual orientation, gender identity and disability through photos, posts and affiliations that would not otherwise be evident in a face-to-face interview. An employer could be accused of discrimination in a failure to hire lawsuit if, after reviewing a candidate's social media pages revealing protected characteristics, the candidate is not offered the job.

To reduce the risks associated with investigating job candidates on social media, employers should: 1) be consistent by conducting social media searches for all applicants or none; 2) establish written search procedures that state who will conduct the search, when it will be conducted, what sites will be searched, and what information will be sought; 3) provide training for staff to ensure consistency in the process; 4) insulate decision makers from impermissible considerations by having the searches performed by other designated individuals, if possible a human resources professional or third-party vendor who will know what information may be considered in making hiring decisions; 5) conduct the search after a face-to-face interview so the employer is less likely to be accused of relying on protected characteristics in selecting candidates for an interview; 6) search only publicly available information; 7) document the search by printing or saving screenshots of anything causing concern (such documentation will protect the company if the content is unavailable when a hiring decision is challenged); and 8) check the facts, focus on the candidate's own posts, and give the candidate a chance to respond to worrisome social media content.

How Can Employers Monitor Their Employees' Social Media Use?

Businesses are also monitoring social media to assess current employee conduct and truthfulness. A common story heard is when an employee calls out sick and then posts pictures from the beach on social media with the caption "best sick day ever!" A 2017 Career Builder survey revealed that 43 percent of employers surveyed caught an employee lying about being sick by checking social media.[7] Monitoring employees' social media activities can also prevent scams and virus attacks that can damage the company's network; prevent disclosure of confidential information; protect the company's reputation; prevent false advertising claims that could result if an employee were to endorse its employer's services or products without disclosing that he or she is an employee of the business; and protect against potential liability for harassment claims as an increasing number of such claims are arising out of social media.

Employers monitoring social media activity of current employees must also be mindful of federal and state laws that afford employees certain protections, such as First Amendment free speech protections for government employees and privacy laws including the Wiretap Act,[8] the Stored Communications Act,[9] the Electronic Communications Protection Act,[10] and common law invasion of privacy laws. In general, these privacy laws prohibit intentionally accessing, without authorization, stored electronic communications. Although enacted long before social media existed, courts have interpreted these laws to mean, among other things, that employers may not improperly access an employee's private social media page; however, as with the New Jersey Social Media Privacy Law, anything publically available or otherwise legally obtained is fair game and may be accessed by employers.

For example, in *Pietrylo v. Hillstone Rest. Grp.*,[11] an employer was found liable under the Stored Communications Act and Wire Tap Act because a manager forced an employee to provide the password to a private MySpace.com page used by employees to complain about work conditions, and the manager later terminated several employees who posted on the page. On the other hand, in *Ehling v. Monmouth-Ocean Hosp. Serv. Corp.*,[12] the court granted summary judgment dismissing a lawsuit against an employer that terminated a plaintiff's employment due to content she posted on her private Facebook page. The court determined the employer did not violate the Stored Communications Act because it did not improperly gain access to the Facebook posts; rather, the plaintiff's coworker and Facebook 'friend' took screenshots of the posts and voluntarily, without prompting, emailed them to management.

What Social Media Conduct Can Employers Discipline?

The most effective way for employers to manage employees' social media conduct is through a written policy setting forth the parameters for appropriate social media use related to the workplace. These parameters must be carefully drafted to best protect employers, including from harassment and discrimination lawsuits, the disclosure of confidential information, and reputational damage, while also ensuring employees' rights are protected, including their rights under the National Labor Relations Act (NLRA).[13]

In recent years, the National Labor Relations Board (NLRB) has examined social media policies and disciplinary actions stemming from purported violations of such policies to ensure employers are not infringing upon employees'

rights under Section 7 of the NLRA.[14] Section 7 protects employee rights to take "concerted" action for their "mutual aid or protection" regarding "terms and conditions" of employment. Examples of protected conduct include bringing group complaints to management or initiating or engaging in discussions with other employees regarding terms or conditions of employment.

The NLRB will first determine whether a social media policy explicitly or implicitly restricts Section 7 activity. The sheer maintenance of a workplace policy that restricts Section 7 activity may constitute a violation of the NLRA even if no disciplinary action has been taken pursuant to the policy. While an employer could face an unfair labor practice charge and a policy may be found unenforceable even if the employer is not unionized, the NLRB will look to see if the rule or policy was promulgated in response to union activity as part of its analysis.

If disciplinary action has been taken for a purported violation of a social media policy, the NLRB will determine whether the employee engaged in Section 7 activity. If the employee's conduct was part of a discussion with other employees regarding terms and conditions of employment, the NLRB will likely find the discipline improper.

General counsel memos discussing the results of NLRB investigations related to social media cases provide guidance as to how a social media policy can be narrowly tailored and enforced in a way that will not infringe on Section 7 rights.[15] The key is to clearly define what constitutes appropriate and inappropriate social media conduct and to provide specific examples. In doing so, employers must be mindful that Section 7 has been interpreted to allow employees to express extreme viewpoints (including disparaging, confrontational or harsh communications containing vulgar language and profanity) so long as the comments are not threatening. Notably, employers cannot bar employees from posting false or misleading statements otherwise protected by Section 7 unless the employee acts with a malicious motive, meaning the employee knowingly publishes false statements or publishes statements with reckless disregard for the truth.

Additionally, a policy restricting employees from posting images of the employer/company will not be enforceable. Such a policy would unlawfully preclude an employee from posting images of picket signs depicting the company's name in connection with a protest involving terms and conditions of employment. Similarly, a policy requiring employees to obtain prior approval before using the employer's name, discussing the employer, or identifying themselves as employees will be unenforceable, as will a policy that requires an employee to discuss work concerns with an employer before posting about it on social media.

The NLRB is focused on protecting Section 7 rights, so employers may generally prohibit 'inappropriate' social media conduct related to the workplace with no connection to terms and conditions of employment or concerted activity.

A social media policy may also prohibit employees from disclosing the company's confidential and proprietary information so long as 'confidential information' is clearly defined. In fact, directing employees not to divulge private information, trade secrets, or other confidential information can be imperative, particularly where employers maintain confidential health information. In defining confidential information, the company should cross-reference its policy on confidential information and/or provide examples of the information that may not be disclosed (*i.e.*, customer lists, ingredients, recipes, know-how or proprietary systems, processes or procedures) so employees understand the prohibition does not apply to disclosures about working conditions.

An enforceable policy should also prohibit employees from social media conduct that violates laws prohibiting discrimination and harassment in the workplace, and the policy should cross-reference the company's anti-discrimination and anti-harassment policies.

As a catch all, a social media policy should explicitly state that it is not prohibiting employees' Section 7 activities; however, this carve out is not a failsafe to ensuring compliance with the NLRA. In *Chipotle Services LLC d/b/a Chipotle Mexican Grill and Pennsylvania Workers Organizing Committees*,[16] the NLRB found that Chipotle's *Social Media Code of Conduct* violated the NLRA even though it expressly stated it did not restrict any activity protected by the NLRA or other laws, finding this was not sufficient to cure the unlawful provisions within the policy. For example, the policy prohibited employees from posting confidential information without defining 'confidential' and statements that contained false information, without clarifying the statements had to be maliciously false.

In addition to putting employees on notice of appropriate and inappropriate conduct, a policy should define 'social media' and any restrictions on the use of social media during company time or on company equipment. Employers may institute a blanket prohibition on social media activities during work time, but work time does not include breaks, lunch or before or after an employee's shift. Employers may also limit social media activities that violate company policy during non-work time. The policy should also advise that employees have no expectation of privacy in company-issued equipment and the company reserves the right to monitor such use. Again, employers may always monitor public postings.

The policy should further state that

employees are accountable for content they post regardless of whether it is posted while in the office, at home or on the employee's own time; outline disciplinary measures for violations of the policy; and identify the individual(s) at the company to contact with questions or to report violations of the policy.

Employees should be required to sign an acknowledgment form stating they received the policy, reviewed it and understand it. Once the policy is implemented, employers must apply the policy consistently and impose discipline, if necessary.

Social media policies are not one-size-fits-all, and should be custom tailored to each company's needs; however, a social media policy can be vital to protect any company from liability, including harassment and discrimination lawsuits. As such policies advise employees exactly what they can and cannot do on social media, employees will also be less susceptible to making mistakes on social media, including accidentally disclosing confidential information. Such policies can also be effective in identifying and responding to social media mistakes should they occur.

How Can Employers Protect Their Social Media Accounts?

Company-specific social media pages are a quick, easy, inexpensive and effective way for businesses to reach the masses and disseminate information about the company's products and services, and to attain a loyal following. Consequently, social media accounts are becoming increasingly more valuable to businesses.

Employers need to ensure the company—and not an individual employee—owns all company social media accounts. Social media ownership disputes are becoming more frequent, especially where businesses hire employees to set up and run the company's social media accounts. For example, in *PhoneDog v. Kravitz*,[17] PhoneDog hired Kravitz as a product reviewer. Kravitz communicated with customers through a Twitter account he created with the handle PhoneDog_Noah, which amassed 20,000 followers. When Kravitz left for a competitor, he took the account with him, modified the handle, and began sending tweets for his new employer. PhoneDog sued, claiming ownership of the account. Although the case settled before the court ruled on the issues, it demonstrates the types of disputes that may arise.

In order to prevent such ownership disputes, employers should: 1) implement policies that clearly state the company owns all social media accounts; 2) require that no company usernames/profiles be created without express permission from the company; 3) specify that content created by employees on the company's social media pages is work-for-hire, created as part of their job duties, and the sole property of the company; 4) register social media accounts in the company's name and prohibit employees from conducting business through personal social media accounts; 5) if a company account is already in an employee's name, determine if the site's terms of service offer the opportunity to terminate or transfer ownership of the account to the company; 6) state in employee agreements that social media accounts are the property of the company, or, if it is an at-will employee, have written agreements that state the company owns social media accounts; and 7) if not previously addressed, resolve transfer of social media accounts in separation agreements and releases and condition the payment of severance on an employee relinquishing any ownership right in social media to the employer.

Whether employers 'like' or 'unlike' it, social media is here to stay. Therefore, as the laws and forms of social media evolve, it is imperative for employers to remain informed of their rights to protect and promote the company while not chilling their employees' rights. ⚖

Endnotes

1. https://www.umassd.edu/cmr/socialmediaresearch/2018fortune500/.
2. https://www.careerbuilder.com/advice/social-media-survey-2017.
3. N.J.S.A. § 34:6B-5 *et. seq*.
4. N.J.S.A. § 34:6B-10.
5. N.J.S.A. § 34:6B-18.
6. 15 U.S.C. § 1681 *et. seq*.
7. http://press.careerbuilder.com/2017-11-16-Increased-Number-of-Workers-Calling-In-Sick-When-They-Arent-Finds-CareerBuilders-Annual-Survey.
8. 18 U.S.C § 2511.
9. 18 U.S.C. § 2701 *et seq*.
10. 18 U.S.C. § 2510 *et seq*.
11. CIV06-5754 (FSH), 2008 WL 6085437 (D.N.J. July 25, 2008).
12. 961 F. Supp. 2d 659, 661 (D.N.J. 2013).
13. 29 U.S.C. § 151, *et seq*.
14. 29 U.S.C. § 157.
15. Memorandum OM 11-74, Office of the General Counsel (Aug. 18, 2011); Memorandum OM 12-31, Office of the General Counsel (Jan. 24, 2012); Memorandum OM 12-59, Office of the General Counsel (May 30, 2012).
16. 04-CA-147314 and 04-CA-149551, 364 NLRB No. 72 (Aug. 18, 2016).
17. *PhoneDog v. Kravitz*, No. 11-03474 (N.D. Cal. Nov. 8, 2011).