New Jersey Law Journal



# A Guide to the Pitfalls and Perils of Social Media in the Workplace

This article will aid attorneys when counseling employers regarding the permissible and prudent use of social media.

By **Maja M. Obradovic and Jemi Goulian Lucey** | February 01, 2019


The use of social media by employees for both personal and work-related activities is commonplace, but can pose significant risks for employers. This article will aid attorneys when counseling employers regarding the permissible and prudent use of social media.

## Monitoring Social Media Accounts

Social media can be an invaluable resource for employers in screening potential employees beyond the traditional interview setting. The majority of employers use social media to "cyber-vet" job applicants, however there are pitfalls associated with this practice. Information readily available on job applicants' social media profiles can

reveal protected characteristics which cannot be considered in an employer's hiring decision (race, marital status, health). Ultimately, accessing candidates' personal information may suggest an improper motive in a failure-to-hire situation.

Employers can avoid this by having HR or a third-party vendor conduct the social media screening and not share any inappropriate information with the hiring manager. If the ultimate hiring decision is based on legally considerable social media content, this should be documented and the posts archived.

Employers may often have legitimate business reasons to examine employee use of social media: to monitor productivity, protect confidentiality, ensure that an employer's reputation or brand is not defamed, or protect other employees from online harassment or cyber-bullying. Employees, on the other hand, have an interest in preserving some degree of privacy in their social media activity.

A best practice to harmonize these interests is to shape employees' expectations of privacy by adopting robust Authorized Use Policies (AUPs), however the "dos and don'ts" of AUPs have been a moving target. Employers should be particularly mindful of the following limitations:

1. *Common Law and Statutory Limitations on Social Media Access*

Employers must balance their legitimate reasons for monitoring employee social media accounts against the employees' reasonable expectation of privacy. The foundation for this lies in the Fourth Amendment as to public employees, but was later used as a template for analyzing employee privacy issues in the private sector.

Enacted in 2013, N.J.S.A. 34:6B-6 prohibits employers from requiring current or prospective employees to "provide or disclose any user name or password, or in any way provide the employer access to, a personal account through an electronic communications device." New Jersey courts had previously relied upon the federal Stored Communications Act (SCA) to protect employees' personal accounts, which imposes civil and criminal liability upon anyone who intentionally accesses an

electronic communication facility without appropriate authorization. In *Pietrylo v. Hillstone,* the U.S. District Court for the District of New Jersey held that two restaurant managers violated the SCA when they pressured an employee into providing them with her MySpace password to access a private chat room in which employees criticized their employer.

While the SCA was enacted before the advent of the internet, and courts have urged Congress to update the statute to address technological innovations, Congress has yet to act. As a result, courts have employed highly technical analyses to shoehorn activity on social media within the SCA definition of "electronic communications." Employing this methodology, New Jersey courts have recently held that the SCA covers non-public Facebook wall posts and Twitter accounts.

Employers must therefore first examine whether they have the right to access their employees' social media accounts. The statutory prohibition does not restrict employers from accessing social media profiles to the extent they are in the public domain as a result of a profile's privacy settings.

Additionally, an important exception under New Jersey law is an employer's right to conduct an investigation into an employee's

> (1) ... work-related misconduct based on the receipt of specific information about activity on a personal account by an employee; or (2) of an employee's action based upon the receipt of specific information about the unauthorized transfer of an employee's proprietary information, confidential information or financial data to a personal account by an employee.

This allows employers to seek even privacy-protected information if directly relevant to an investigation. A common law right to privacy also exists.

2. *NLRB Protections and "Concerted Activity"*

During the Obama administration, the National Labor Relations Board (NLRB) expanded the categories of protected employee speech by invalidating a number of employers' AUPs or finding that actions taken against employees in response to their social media posts were unlawful. Importantly, NLRB rules apply to both unionized and non-unionized employees.

A fundamental concept that underlines the NLRB's rulings are that they protect employees' "concerted activity." Under the National Labor Relations Act (NLRA), activity is "concerted" if it is addressed to or can reach at least one other person (typically a co-worker) and is aimed at organizing, inciting action of employees to protest their work conditions, or protecting themselves. There is no need for an agreement to act. The NLRB has interpreted even "liking" another employee's post as sufficient to qualify as concerted activity.

Conversely, if the subject comments are purely a private gripe, they are not protected. A post that merely complains about the "tyranny" of the employer and calls the manager names is not protected as it expresses an employee's frustration but does not contain language aimed at inducing group action. The NLRB has previously protected employees' speech even when a significant part of such speech is not aimed at "concerted activity."

Given that NLRB members are political appointees, political forces often change the landscape. The Trump-era NLRB, in its first major decision in *The Boeing Company* case, announced a more employer-friendly test when assessing facially neutral policies, which calls for an analysis of: (1) the nature and extent of the impact of the policy upon an NLRA right; and (2) the legitimate justification for the policy.

3. *First Amendment Protections*

A public employer's right to discipline employees for violating its AUP requires analysis as to whether such adverse action would survive a First Amendment challenge. The Fourth Circuit, in *Liverman v. City of Petersburg,* held that the police department's

policy containing a blanket prohibition against any social media posting that reflected negatively upon the department was unconstitutionally overbroad under the First Amendment, and that disciplinary action taken against officers who violated the policy was impermissible. The court held that government may not prohibit speech on the grounds that it expresses a critical viewpoint.

Whether or not an employee's speech falls within First Amendment protection requires application of the U.S. Supreme Court's *Pickering* balancing test, which weighs the employer's administrative interest against the employee's right of free speech. Some examples of speech that is not protected include advocating for illegal activity, inciting violence and defamation.

## Characteristics of Strong AUPs

In issuing an AUP, employees must be clearly informed that the employer will be monitoring their use of the employer's electronic devices, including computers and company-issued cell phones, for internet and electronic communications generally, and social media use. Courts generally uphold such policies.

An employer should specify its ability to monitor those electronic devices, even if they are password protected, or if they are used off-hours or off-premises. Employers should specify that company-issued electronic devices be used solely for work-related purposes. Employers should prohibit the transmittal and downloading of material that is discriminatory, harassing, offensive or otherwise unlawful. The employer should advise that any unauthorized use may result in discipline, including suspension and termination of the employee.

## Addressing Employee Misuse of Social Media

Employee behavior that affects an employer's ability to operate efficiently, and an employee engaging in conduct that is unprofessional and hurtful to either other employees, clients, or patrons of the institution, is sanctionable. A school in Paterson, New Jersey, terminated a first-grade teacher who made derogatory comments on

Facebook about her students. The Appellate Division agreed that "in a public school setting thoughtless words can destroy the partnership between home and school that is essential to the mission of the schools." The efficient operation of the school outweighed the teacher's right to free speech.

Additional examples of impermissible social media activity can be distilled through NLRB cases. For example, advocating insubordination is not protected and can justify termination. Similarly, crude and insensitive jokes can be actionable.

## Can the Employer be Liable for Employee Misuse?

Employers need to protect themselves against incurring liability for an employee's misuse of social media. Courts tend to focus on two areas to determine employer liability: (1) whether the social media forum is related closely to the employer such that it can create employer liability; and (2) whether the employer was aware of, or should have been aware of, the misuse.

In *Blakey v. Cont'l Airlines*, the New Jersey Supreme Court ruled that while employers do not have an affirmative duty to monitor private communications of employees, an employer must take action if it becomes aware of discriminatory or harassing posts on social media. An employer has a duty to redress such illegal conduct or can be liable just as if the conduct was occurring in the workplace.

Actively monitoring employees' social media activity can create a duty on the part of the employer to take action. In *Doe v. XYC Corporation*, a mother sued her husband's employer for negligence after he used a company computer to post his step-daughter's nude photos on a child pornography website. The court held the employer was on notice and breached its duty to exercise reasonable care by not attempting to stop the father's actions.

It is essential that all anti-harassment, -discrimination and -retaliation policies clearly state that inappropriate behavior through social media is unacceptable and may be the subject of discipline. Employers should train against harassment and discrimination on

social media and take action if it becomes aware of impermissible use.

## Conclusion

Social media has profoundly changed our cultural landscape both within and beyond the workplace, and employers must adapt to these changes by implementing protective and proactive policies related to the hiring and oversight of their employees. Attorneys who counsel employers are the first line of defense against the associated risks, and should provide guidance accordingly.

**Maja M. Obradovic** *and* **Jemi Goulian Lucey** *are counsel in the Litigation Department of Greenbaum, Rowe, Smith & Davis, in Woodbridge. Obradovic serves as co-chair of the Employment Law Practice Group. Lucey is a member of the Employment Law Practice Group and co-chair of the Higher Education Practice Group.*