MINIMIZING HR RISK IN A SOCIAL MEDIA WORLD

By James Parton III
Parton Sell Rhoades

Social media – Facebook, Twitter, LinkedIn, and many more – are increasingly dominating the internet and entering the workplace. Social media add both complexity to existing HR issues and create new risks to be managed. These new challenges can extend far beyond the workplace and management's direct control. Even in the workplace, employees have independent real-time access to social media through smartphones. Simply continuing existing policies and practices is wholly inadequate in this brave new world.

The following are examples of the varied kinds of legal risk to a company from misuse of social media by employees and management:

- **Discrimination** – a manager chooses not to hire an applicant after checking his Facebook page, which makes clear he is a Muslim.
- **Harassment** – one employee posts threatening messages on another's Facebook wall or makes offensive comments on the company's Facebook page.
- **Invasion of privacy** - the employer disciplines the employee for his off-duty Facebook posts which it considers inconsistent with the employer's public image.
- **Unfair labor practice** – an employee is disciplined after complaining on Facebook about perceived unsafe or illegal workplace practices.
- **Retaliation or whistleblower claims** - the employer disciplines an employee after the employee's posts to her blog complaints about perceived violations of environmental regulations by the employer.
- **Trade secrets** – an employee or manager intentionally or unintentionally discloses confidential information in his personal Twitter feed.
- **False advertising** - an employee posts rave reviews of the employer on Yelp without revealing that she is an employee.

This article will highlight critical risks and suggest best practices for managing them.

I. RISK HOT SPOTS

These are some areas in which employers should be particularly sensitive to the potential consequences of their actions.

A. Hiring

A hiring decision, especially for smaller companies, is a huge commitment. Making the right hiring choice is difficult because of limited sources of information.

Almost every employer who has made hiring decisions has felt the desire to run a Google search on an applicant, check for a Facebook page, or otherwise use the internet to determine if there is something "out there" which she would "like to know" about the applicant.

The employer should know not to ask whether an applicant has a disability, is in a same sex relationship, his age, or her religion. However, accessing the applicant's Facebook page will likely put the employer in possession of this kind of information. Regardless of whether it serves any role in rejecting an application, discovery of the employer's practice of checking applicant social media sites could provide a basis for a future claim of discrimination in hiring.

B. Unfair Labor Practices

The National Labor Relations Act (NLRA) gives union and nonunion employees the right "to engage in concerted activities for the purpose of collective bargaining or other mutual aid or protection." Actions by an employer which might deter employees from exercising their rights are illegal. If the employer's business has a substantial effect on interstate commerce (with some exceptions), the employer is subject to the NLRA whether or not there is a union or any organizing activity occurring. In the context of social media, the National Labor Relations Board ("NLRB") has interpreted the NLRA in ways which may be surprising to many employers.

For example, an employer was ruled to have violated the NLRA by terminating five employees for profanity laced Facebook posts which began with one employee's post that a coworker said they not do enough to help customers and asked "My fellow coworkers how do u feel?"

The NLRB also held that a provision in the Costco employee handbook prohibiting employees from electronically posting statements that "damage the Company, defame any individual or damage any person's reputation" violated the NLRA. The NLRB recently held that a rule encouraging "courtesy" in communications with customers and other employees violated the NLRA, but upheld the employee's discharge for a Facebook post which ridiculed a customer.

The Office of the General Counsel has concluded that many employers have problems with overly broad social media policies that appear to restrict employee concerted action rights. These include policies which prohibited:

- employees from revealing personal information regarding coworkers, company clients, partners, or customers without their consent.
- the use of the Employer's logos and photographs of the Employer's store, brand, or product, without written authorization.
- use of any social media that may violate the rights and reasonable expectations as to privacy or confidentiality of any person.

- communications or posts that constitute embarrassment, harassment or defamation of the employer or of any employee, officer, board member, representative, or staff member.

- statements that lack truthfulness or that might damage the reputation or goodwill of the employer, its staff, or employees.

According to the NLRB, these policies were not sufficiently narrow and specific to exclude conduct protected by the NLRA while banning improper conduct that is not protected. However, rules that clarify and restrict their scope by including examples of clearly illegal or unprotected conduct, such that they could not reasonably be construed to cover protected activity, are not unlawful.

The Office of the General Counsel determined one of the policies it reviewed to be in full compliance with the NLRA and attached a copy to its latest report. NLRB, Operations Memorandum 12-59 ("OM 12-59"), available at http://www.nlrb.gov/publications/operations-management-memos.

California law prohibits all employers from restricting or disciplining employee discussions of wages and working conditions. Even if the business is not subject to the NLRA, any attempt to punish or prevent posts concerning these issues subjects the employer to damages and penalties.

C. Social Media Harassment

Under California law, all employers have a duty to take immediate and appropriate action when it knows or should have known of illegal harassment of an employee. Employers with 5 or more employees are also obligated to take "all reasonable steps necessary to prevent discrimination and harassment from occurring." The extent of an employer's obligation when the harassment occurs off-duty through social media posts is unclear.

For company-sponsored sites, they are likely similar to the workplace itself. Company-sponsored social media sites may include intranet forums or external sites such as a company Facebook page. For example, the Supreme Court of New Jersey held Continental Airlines could be liable for harassment of a female pilot which included vulgar and pornographic posts to the airline's online bulletin board accessible to all pilots. The court likened the bulletin board to a company lounge. It also ruled that, even if the bulletin board were considered separate from the workplace, harassing posts could still be considered as evidence of a hostile work environment.

Legal liability may also result from how an employer responds to posts on an employee's personal social media site. In a recent unpublished (i.e. not citable as legal precedent) decision, the California Court of Appeal affirmed an $820,000 judgment against a company based in mostly on harassing blog posts made on another employee's personal blog as well as harassing conduct in the workplace. Management was aware of the posts and the probable culprits, but made inadequate efforts to prevent them from

continuing. The court ruled that the employer's failure to take immediate and appropriate corrective action once it learned of the posts and the likelihood of other employees' participation supported the large award.

What is the extent of an employer's duty? If an employer sponsors a social media site, it is likely to be considered to have knowledge of what is posted there. along with knowledge comes the duty to act. Therefore, an employer should make a practice of regularly checking posts on its sponsored sites and responding appropriately where necessary.

It would be a mistake for management to monitor employee's posts to other sites. Monitoring may raise privacy concerns. Beyond that, however, what the employer does not know about off-duty conduct is unlikely to hurt it. If a complaint is made, a response is required. Otherwise, it does most employers little good, and potentially much harm, to go looking.

D. Privacy

Employers must also be mindful of privacy laws. Reports of employers demanding email and social media passwords from applicants as part of the application process has resulted in a new California law banning the practice. Effective January 1, 2013, it will be illegal to require or request usernames, passwords, or other information about social media sites from employees or applicants or to access social media in the presence of the employer. The law includes an exception if it is relevant to an investigation into workplace misconduct or employee violation of applicable laws and regulations.

Monitoring employee social media posts which are not posted confidentially may still be legal. However, the employer who later disciplines or terminates an employee based on posts by employee (or his "friends") about his private life may face liability for invasion of privacy and wrongful termination. For purposes of unemployment insurance, California regulations state that "If there is no injury or potential injury to the employer's interests, the employer cannot reasonably impose the employer's standards of behavior on an employee during his or her off-duty time." It may be considered an invasion of privacy to discipline an employee for off-duty conduct discovered through checking an unrestricted social media post, if the employer cannot demonstrate an actual or potential injury to its interests resulting from the post.

The manner by which the employer monitors employee social media posts may also expose the employer to civil and criminal penalties. The Electronic Communications Privacy Act of 1986 bars intentional interception or access to electronic communications without authorization unless it is likely to further legitimate business interests.

Some employers use third parties to conduct social media searches on job applicants. The results of those searches may be treated as subject to the federal Fair Credit Reporting Act and the California Investigative Consumer Reporting Agencies Act. Advance consent from the job applicant is required under these acts, and a rejected applicant is entitled to a copy of any consumer report used to make the hiring decision.

E. False Advertising

Another risk arises when employees post laudatory statements about their employer's products or services without identifying themselves as employees. The posts may be on a company sponsored site, such as a company Facebook page, or on sites such as Yelp. The Federal Trade Commission has stated that a failure to identify the endorser as an employee may be illegal. For example, if a hostess at a restaurant posts enthusiastic reviews of the restaurant on Yelp, knowledge that the endorser is an employee would probably affect the weight and credibility of her endorsement. If she does not so identify herself, she has violated FTC Guidelines.

Depending on the involvement of management in encouraging or failing to prevent such endorsements, the FTC may investigate and impose substantial sanctions. For example, a PR firm used employees to post reviews as ordinary consumers. After an FTC investigation, the PR firm agreed to a Consent Decree lasting 20 years and imposing reporting and compliance provisions for both the agency and owner.

This use of social media is also potentially a violation of California's False Advertising law (Bus. & Prof. Code §17500) and Unfair Business Practices law (Bus. & Prof. Code §17200). Public disseminated advertising which contains a statement that is false or misleading, or which the company should have known was untrue, or misleading, is a violation. California courts have held that statements by employees may constitute advertising.

II. BEST PRACTICES

Develop a limited social media policy. Employers should consider adopting a carefully limited policy outlining expectations for acceptable use of social media by employees.

Ensure that policies are not overly broad. Policies besides a social media policy – such as standards of conduct, use of company logos, nondisclosure of confidential information and internet usage at work – should also be reviewed carefully to determine if they could be interpreted as restricting concerted action rights under the NLRA.

Update other policies. Employers should update their existing policies to make clear that its policies against harassment in the workplace and workplace violence, standards of conduct, confidentiality, etc. apply to employees' online conduct. Care should be taken to avoid inadvertently violating the NLRA.

Dispel unwarranted expectations of privacy. Employers are wise to adopt a policy concerning the use of company-supplied computers, smartphones, etc. that states clearly that their contents and all communications and posts made using them should not be considered private and may be accessed by management.

Establish clear procedures for complaints and reporting. Employers should include internet harassment in their policies concerning employee reports or complaints

about harassment or discrimination.

Incorporate social media activities into employment and non-disclosure contracts. All such contracts should be reviewed and, where necessary, revised to make specific reference to social media posts and activities.

Consistently monitor any employer-supported social media. If your company sponsors any social networking platform, it may be responsible for failures to take action in response to posts made in violation of policy or law. Employers should consider assigning a person to monitoring such sites on a scheduled basis.

Distinguish between on-duty and off-duty social media use. Absent an articulable employer interest, employers should take extra care before taking any adverse employment action based on an employee's off-duty use of social media.

Respect employee privacy concerns. Employers should not attempt to access employees' restricted content without permission of the employee. Obtaining that permission in writing, and without coercion, is recommended.

Be careful with "protected" information that may be obtained online. Employers who wish to check the internet regarding job applicants may wish to consider having it done, and filtered, by persons other than decision makers. Employers should have a clear written statement of the purpose for such searches that is limited to job-related information from which hiring decisions may legally be made. Employers who do an online search for one candidate, should do one for all. Selective use of social media searches may lead to a claim of bias.

Be aware of whistleblower protections. Taking action in response to an employee's internet posts on matters of public concern or statutorily protected rights can result in a "whistleblower" or retaliation claim.

Respond promptly and appropriately to notice of potential online harassment. Mindful of other restrictions (e.g. "concerted action"), employers who learn of offensive or threatening posts about an individual or identifiable class of employees must not look the other way. An immediate response appropriate to those circumstances, often beginning with an investigation, should be undertaken.

Maintain consistency. Employers should endeavor to apply their social network rules and impose discipline uniformly and consistently. While situations differ, employers should be mindful of their past responses to similar situations. Taking the time to investigate, think through appropriate responses, and carefully document the basis for any deviation from previous disciplinary action can prevent future discrimination claims.