SOCIAL NETWORKING POLICIES - COMING TO AN EMPLOYEE HANDBOOK NEAR YOU...

BRANDON L. SIPPLE

Over the past several years, the use of social networking has increased exponentially. Facebook, for instance, estimates that 500,000,000 people now use its site. Estimates of Twitter users range anywhere from 14,000,000 to 70,000,000. And that's not to mention the 70,000,000 blogs that can be found on the net.

Employer monitoring of employee internet use during work hours is certainly nothing new, and the practice has increased by more than 45% in the past decade. Most employers nowadays have policies regarding acceptable internet usage in the workplace. However, we are beginning to see an upsurge in the utilization of social networking use policies that are independent from an employer's general internet policy.

The major difference between social networking policies and general internet use policies is also the reason why these policies need to be very carefully crafted - they often govern an employee's off-duty conduct in addition to their on-duty conduct. Thus, there are many privacy and other concerns that come into play. Nonetheless, employers cite many reasons why these policies are necessary, among them:

- To monitor and prevent reputation damage from "bad employee" blogs and postings.
- To monitor and prevent "cyber-smearing" and slander.
- To monitor breaches of restrictive covenants.
- To monitor and address employees' disclosure of confidential information.
- To screen potential job applicants.

The common denominator is that social networking presents a real concern to employers that employees might utilize these vast cyber resources in ways that might cause harm to their companies. Perhaps the most frequent cases we hear about are those of disgruntled employees who use these electronic resources as a means to "bad mouth" and harm the reputation of their employers (see a real life example **here**). By regulating employees' usage of social networking sites, employers can help control and limit these problems from occurring.

However, employers should beware of the legal pitfalls off-duty internet usage and social networking policies may present. As an initial matter, a poorly drafted social networking policy could open up an employer to invasion of privacy claims. In addition to common law, certain federal (and state) statutes may come into play in this context. For instance, the Federal Electronic Communications Privacy Act ("ECPA") ,18 U.S.C. § 2510 et seq., prohibits the unauthorized interception of wire, oral or electronic communication. Another federal statute, the Stored Communications Act ("SCA"), 18 U.S.C. § 2701 et seq., makes it unlawful to "intentionally access a facility through which an electronic communication service is provided...and thereby obtain...access to a wire or electronic communication while it is in electronic storage in such system." Thus, an employer may face liability if they access an employee's external website (e.g. Facebook site) if the site is password protected and the

employer does so without authorization. Both the ECPA and SCA have exceptions if the employee consents to such access.

In the case of *Pietrylo v. Hillstone Restaurant Group, d/b/a/ Houston's*, a jury in Newark found that an employer violated the SCA, along with the New Jersey Wiretapping and Electronic Surveillance Control Act when it secretly monitored employees' postings on a private password-protected internet chat room. 2009 WL 3128420 (D.N.J. Sept. 25, 2009). The jury found that management "knowingly, intentionally, or purposefully," and without authorization, accessed the chat group, thus subjecting the employer to liability.

In order to avoid this type of liability, employers should adhere to certain best practices in drafting social networking policies that protect the interests of the employer while respecting the privacy of the employee. For instance:

- Policies should address confidentiality and trade secret protection and prohibit employees from disclosing information about customers, suppliers, etc.
- Policies should clearly state that employees engaging in social networking and blogging for either personal or professional reasons must refrain from disparaging the company and its employees.
- Policies should limit employees' authorization to speak on behalf of the organization.
- Policies should put employees on written notice that information exchanged on non-private social networking sites can be accessed by the company.
- Employers should ensure that employees sign written acknowledgments that they have no reasonable expectation of privacy on the organization's computers, email systems, etc.

Including these and other provisions in an effective social networking policy will help ensure that employees are put on notice of the employers' expectations in a non-invasive manner.

Naturally, a comprehensive examination of the ins and outs of social networking policies is beyond the scope of this article. Any employer who is considering adding a social networking and off-duty internet usage policy to their handbook should consult with a competent employment attorney familiar with this cutting edge subject.