EMPLOYMENT & LABOR ALERT

ROBINSON BRADSHAW & HINSON

OCTOBER 2009

Employment Policies – And Realities– in the Age of Blogs and Social Media Sites

By Julian H. Wright, Jr. and John M. Conley

Many workers log on to their LinkedIn, Facebook or MySpace pages – either at home or work – as regularly as buying a latte or reading the newspaper (maybe a bad example). Others will read – or perhaps write for – a blog, with estimates being that the blogosphere grows by one new blog every *second*. What happens when an employee's comments on a social media site or blog cast the employer in a poor light? Or perhaps divulge information – intentionally or unintentionally – the employer does not want known publicly? Can employers protect themselves from what their employees may do on the internet? Can employees have any confidence that their "private" or "anonymous" activities on the internet will not be the basis for decisions in the workplace?

Despite what employees may assume, there is virtually no privacy in cyberspace communications. Employers may legitimately research and consider employees' on-line activities in making employment decisions. Employers should not use deception or coercion when searching out employees' internet activities. The National Labor Relations Act also may limit what employers can do with information if employees are discussing wages or specific working conditions. Usually, however, employers are well within their rights to monitor social media sites and other internet activity – even if such activities are done on an employee's own time on his or her own computer – and use that information to inform nondiscriminatory and otherwise legal employment decisions.

Just as employers may impose dress codes, schedules, and other restrictions on employee activities, they may also restrict what employees say and do in cyberspace, particularly in terms of statements about the employer. An employee's gripe about new tasks at work could signal a competitor about a new project. Poking fun at a colleague or posting a funny photograph could be harassment. Legal risks abound – in areas from copyright to discrimination to libel and others – in the unfettered use of social media. The First Amendment protects free speech against *government* interference. Communication via social media or blogs is speech, but most employers are not the government. Accordingly, there are few legal limitations on employers restricting what their employees can communicate in cyberspace, particularly about the employer.

Companies, however, need not forbid all use of social media, even at work. A draconian policy could create a damaging backlash. No employer wants to be unpopular among employees, particularly the valuable, technologically savvy employees most connected to social media. To protect themselves and not unduly interfere in employees' on-line activities, employers can implement a two-pronged approach.

First, companies should adopt policies that spell out restrictions on employees' use of social media (both at work and at home) and how the employer may utilize information about its employees available on the internet. A non-exhaustive list of issues to be addressed in any potential policy includes: (i) guidelines for using company time and company equipment to access social media and blog sites; (ii) warnings about the lack of privacy in any such sites and notice of potential monitoring by the employer; (iii) notice to applicants and employees about the employer's use of information obtained from the internet in employment decisions; (iv) prohibitions against disclosing confidential information, making defamatory statements, or in any way compromising the employer's interests through social media; and (v) internal training and resources for HR staff in using internet information and enforcing the policy. When adopted, such social media policies should be communicated clearly, concisely, and frequently.

Second, as part of any policy – and after telling employees – employers can use available technology to monitor and, in some cases, block employee use of social media sites and blogs. Products are readily available that will track and report employees' web usage and also block browser access to websites the employer deems objectionable. This approach, though, has a number of obvious practical flaws.

Most importantly, an employer can track or block web use only on hardware that the company owns and controls. So employees still will be able to do whatever they want on their home computers. Even during the workday, employees may be able to access social media sites using intelligent phones. In addition, social media sites are proliferating. An employer can block every site it knows about today, only to find that employees are using new ones next week. Another problem is "proxy sites," which are websites from which you can browse other sites – internet middlemen, as it were. If the employee goes to proxy site A and then jumps to blocked website B, the employer's blocking technology will see only site A, which is not blocked. Moreover, blocking the proxy sites is not entirely practical because proxy sites themselves are proliferating. So while the technological approach can have considerable value for the employer, it is not a cure-all. Given all these problems, the bottom line for now is that technology alone cannot control social media use, and employers will have to rely on legal solutions, such as a clear, enforceable policy as described above.

Ultimately, a single, cookie-cutter social media policy will not work for every employer. Employers will need to tailor policies to their specific needs. Having a policy, however, is increasingly a business necessity in our ever-changing technological age.