





SOCIAL MEDIA CASES HIGHLIGHT CHALLENGES FOR BUSINESSES

By Rodger Kohn, February 2011

Facebook, LinkedIn and Twitter are fast becoming standard tools for businesses to communicate with customers and to market to potential customers. Of course, with powerful new communication tools comes the challenge for business owners not only to effectively use the tools, but also to prevent their abuse. Several recent cases highlight some of these challenges:

-  In a case out of Minnesota, an IT staffing firm sued one of its former employees for allegedly violating his non-competition, non-solicitation and confidentiality obligations through use of LinkedIn. The former employee is accused of “connecting” with contractors and customers in violation of his employment agreement.
-  Courtney Love has recently been sued for defamation for tweets about designer Dawn Simorangkir with whom she has a dispute. Love's tweets allegedly branded Simorangkir “a drug-pushing prostitute with a history of assault and battery who lost custody of her own child and capitalized on Love's fame before stealing from her.”
-  The National Labor Relations Board recently issued a complaint characterizing that an employee's complaints about her supervisor posted to her Facebook page could be considered “concerted” activity and thus protected under federal labor law.
-  The Supreme Court recently ruled on a case involving an employer's right to review personal text messages sent via an employer issued mobile phone. While the court ruled that the employer had the right to review these messages, the fact that this case went to the U.S. Supreme Court illustrates how difficult of legal issue this was.

The critical point is that businesses cannot ignore how their employees use social media both as part of their job and personally. Just like the use of company phones, email accounts and internet access, having a clear, well-constructed policy sets appropriate boundaries and communicates your expectations to your employees.

Some things to consider in preparing these policies include:

- Reemphasizing that equipment, including computers, cell phones and other mobile devices *and* the access (i.e. airtime, bandwidth) belong to the employer and are for use of the business.
- Making clear to employees that any communication made via company-owned equipment or company network access can be monitored, restricted or cancelled at your discretion. It is important for your employees to understand that nothing they do on your system or using your equipment is private to them; as the employer you may access, monitor and restrict use of equipment and access as needed for your business.
- Setting clear policies regarding personal access to and use of social media sites while employees are at work. While simply banning access is simple, it ignores the reality that, like personal use of phones and email, employees are likely to do it anyway. Instead, address the reality. A few suggestions include:
 - Setting parameters on when sites can be accessed and letting employees know that if the privilege is abused it can be revoked.

- Reminding them that use of company assets including equipment and internet access will be monitored.
- Making standard a policy that employees should not use their business email addresses to sign up for personal accounts.
- Clearly communicate your policies on confidential and business information and be sure that all your employment manuals are thorough and up to date. Remind your employees that posting about things that go on at work (*i.e.* working late on a big project for client x) violates your policy regarding non-disclosure of confidential information.
- Review and update your non-solicitation and other restrictive covenants to address how your employees may use social media to contact customers, suppliers and contractors after they no longer work for you.

There are many examples of social media policies already available on the web. One site, [Social Media Governance](#), has compiled an expansive list of sample policies. Remember, as with all business/legal tools, consider these examples through the filter of your own industry, the way you do business and your employee relations.

Hopefully your employees are not acting like Courtney Love, but learning that a critical piece of business information has been posted on Facebook or that an employee just connected to your prime competitor on LinkedIn is not a surprise you want either. With social media, setting some clear guidelines goes a long way to preventing these potential pitfalls.