Employers Need not be all a Twitter over Social Media Issues

March 31, 2010
The Bulletin Newsletter March 31, 2010 Edition

Facebook, Twitter, MySpace, blogging and the like are becoming increasingly popular, but the rules applicable to employer monitoring of such social web sites are just developing. However, one New Jersey employer's mistake is helping shed light on what an employer should and should not do.

In *Pietrylo v. Hillstone Restaurant Group*, the employer became aware that two of its employees were participating in an online chat room of MySpace known as Spec-Tator. Apparently, the employer became concerned that the employees' comments may harass or humiliate other employees and managers or adversely impact the core values of the restaurant.

In light of this concern, the defendant asked one of its employees who had an account to provide her log-in information so they could monitor the communications. The employer accessed Spec-Tator using this log-in and eventually terminated the two plaintiffs based on their chat. Following their discharge, the plaintiffs filed suit alleging, among other things, a violation of the federal Stored Communications Act (SCA), 18 U.S.C. § 2701, *et seq*.

The SCA prohibits, in relevant part, anyone from intentionally accessing without authorization a facility, through which an electronic communication service is provided or intentionally exceeding any authorization that is granted, and thereby obtaining an electronic communication. Violations may be punishable by fines and imprisonment and may be the subject of a civil action. A successful plaintiff may be entitled to receive equitable relief, actual damages (not less than $1,000), profits made by the violator, punitive damages and attorney's fees.

At trial, the employee providing the log-in information testified that she felt she had no choice in giving out her username and password, and that she would be in trouble with her employer if she did not cooperate. Evidence also showed that the employer accessed Spec-Tator not just once, but several times.

The jury concluded that the employee's purported authorization was not only coerced, but also that the employer exceeded the scope of authority since there was no evidence that a "blanket" authorization had been granted. The plaintiffs were awarded actual damages, which were fairly insignificant because they quickly found new jobs, punitive damages and attorney's fees.

So, what should employers do? First, employers should consider publishing a social media policy to protect their business interests. Such policies may prohibit employees from making untruthful, derogatory comments about the company or its management, employees, customers or products (or those of a competitor). However, the policy must not restrict employee communications about the terms and conditions of employment in a manner that would violate their employees' rights to engage in concerted activity under the National Labor Relations Act. The policy should encourage employees to address grievances directly with management rather than vent complaints publicly and to report (but not respond to) any derogatory comments they discover about the company on the Internet.

The policy may also prohibit the use of company logos and branding materials, the disclosure of any proprietary or confidential information, and the violation of copyright and trademark laws. Policies should also encourage the appropriate use of privacy settings, respectful language and honesty and contain a reminder that anonymous comments do not necessarily remain anonymous and postings may last forever.

Employees should be told that if they post commentary that may be viewed as an official statement by the company, they must include a disclaimer such as "The views and opinions expressed are my own and do not necessarily reflect the views of [the company]." Finally, while employers may wish to monitor social media sites to ensure adherence to company policies, they must do so in a lawful manner.

If you need assistance with developing a social media policy or have questions concerning monitoring employee use of such sites, please contact the author, Claudia Orr, or your Plunkett Cooney attorney.