McAfee & Taft
A PROFESSIONAL CORPORATION

The Legal Pitfalls of Online Social Media

McAfee & Taft Law Alert - August 13, 2009

By Ryan Lobato and Dara Wanzer

Across the spectrum, individuals and organizations are waking up to the various perils of online social media. Last week, the U.S. Marine Corps banned access to online social networking through the Marine Corps Enterprise Network on the basis that such access presents an unacceptable security risk.[1] Similarly, the National Football League® has recently banned its players from using Twitter®.[2] Tony La Russa, famed baseball manager, recently settled a lawsuit with Twitter® over a (now deleted) fake Twitter® profile page.[3] Even lawyers and judges are coming under scrutiny for their online social networking activities.[4] Perceived anonymity or impersonal communication may lead people to do or say things that they would not say or do in person.

The simple fact is that with the increasing popularity of online social media channels such as Facebook®, Twitter® and LinkedIn®, corporate and private individuals are starting to realize their legal vulnerability. For example, an employer might publicly praise an employee through LinkedIn®, a professional social networking site, by giving the employee a positive "Recommendation." If the employee's performance subsequently declined, resulting in a termination of employment, the "Recommendation" might later be brought into court as evidence in a claim of wrongful termination, perhaps providing just enough evidence for the suit to survive a motion for summary judgment.[5] Alternately, Facebook® users might create unauthorized "pages" or register a fictitious Facebook® username associating themselves with the company. While many such uses are innocent, they nevertheless have the potential to infringe company trademarks and copyrights, or associate the company with discriminatory or harassing content.

Other risks of online social media include identity theft and impersonation. While Facebook® typically removes fake or impersonating accounts under its comparatively conservative abuse policy,[6] Twitter® explicitly allows so-called parody accounts to exist if it is "obvious that the profile is fake."[7] Illustratively, a quick search of Twitter® users will reveal a number of parody

accounts for Sarah Palin, Barack Obama and a variety of Disney® characters. Unchecked, such impersonating accounts may engage in a number of questionable or illegal acts, including trademark infringement, tarnishment, trade libel, disparagement, brand hijacking, dilution and other such harms. Alternately, the user may be attempting to engage in Tweet-squatting, or reserving the user name in bad faith or for profit.

But the legal issues involved with online social networking do not end there. While there is no case law on point, it is possible that old Tweets™ or Facebook® status updates might constitute "reasonably accessible" Electronically Stored Information (ESI) for purposes of discovery under Federal Rule of Civil Procedure,[8] and consequently past Tweets™ may become increasingly significant. Further, trade secrets may be inadvertently revealed or otherwise misappropriated, inventions disclosed, accounts divulged, client lists released, operating manuals shared, or other sensitive and/or confidential information transmitted to the world in the blink of an eye – and often unintentionally. Finally, social media is also becoming an avenue for counterfeiting, alerting readers to websites or real-world locations where counterfeit goods such as fake watches and purses may be purchased.

While it is true that there are significant pitfalls with online social media, it is difficult to underestimate the marketing potential that these channels of communication hold. Consequently, companies should consider the following steps:

- Create an account on Facebook®, Twitter®, LinkedIn® and any other online social networking site, even if only to reserve the account name. Ideally, the company should develop an online social media advertising campaign[9] to further market the corporate brand. Advertising consultants and social media strategists are available to help.
- Decide if employee use of online social media will be permitted during company time, including break time. Make the same decision for off-company-time using company issued technology such as BlackBerrys® or laptops. Incorporate this decision into a formal corporate e-mail and internet usage policy. If no such policy exists, develop and implement one.
- Periodically monitor employee use of online social media to ensure it falls within corporate policy. Employers may adopt a monitoring policy for a variety of reasons. A company may adopt a policy to protect the company from injury to its reputation, or for workplace productivity reasons. The company may adopt a policy simply because they want to be alerted to suspicious activity. However, employers do not have carte blanche to monitor employees. Employees are entitled to a certain amount of privacy in the workplace, and an employer must balance its employees' reasonable expectation of privacy with legitimate business purpose and scope.
- Note, however, that surreptitious monitoring of employees is generally not an appropriate policy. Employees generally feel less violated when they are aware of what will be happening, and continuation of employment with knowledge of a monitoring policy generally equates to employees' implied consent to the policy.
- Regardless of the policy, employees should not be representing the corporate brand without the appropriate permission or authority to do so.
- Develop and implement a strategy for policing use of company marks on online social networking sites like Facebook® and Twitter®. If a fake account is discovered, action should be taken immediately.

In sum, while certain risks exist, online social networking holds tremendous opportunity for those "in the know." With a little foresight and vigilance, many of the dangers can be avoided. By observing the above measures, one can feel comfortable moving forward and confident in the protection and expansion of business and private interests. Should you need further assistance or have follow-on questions please feel free to contact us.

- McAfee & Taft Intellectual Property Group
- McAfee & Taft Labor & Employment Group

---

[1] Thomas Claburn, *Marine Corps Bans Social Media On Military Network*, InformationWeek, August 7, 2009, (last visited Aug. 7, 2009).

[2] Tony Bradley, *Social Network Policies: Pentagon vs. NFL*, PC World, August 5, 2009, (last visited Aug. 7, 2009).

[3] *Twitter, La Russa Settle Suit*, Associated Press, June 6, 2009
(last visited Aug. 7, 2009)

[4] Molly McDonough, *Facebooking Judge Catches Lawyer in Lie, Sees Ethical Breaches #ABAChicago*, ABA Journal, (last visited Aug. 7, 2009).

[5] Example drawn from Phil Jones and Lauren Mutti, *Beware of Good Deeds: Employer "Recommendations" on Social Networking Websites*, July 17, 2009, (last visited Aug. 7, 2009).

[6] Facebook reporting Frequently Asked Questions, (last visited Aug. 7, 2009).

[7] Twitter® Impersonation Policy, (last visited Aug. 7, 2009).

[8] Specifically, Fed. R. Civ. P. § 26(b)(2)(B). Example drawn from David Jacoby and Judith S. Roth, *'OMG! Ur TM, © Being Infringed @Twitter!'*, Law360, available online at **http://ip.law360.com/articles/112468,** (last visited Aug. 7, 2009).

[9] The Twitter® 101 for Business guide is available online at http://business.twitter.com/twitter101/?f12e0df8, (last visited Aug. 7, 2009).

OKLAHOMA CITY
TENTH FLOOR
TWO LEADERSHIP SQUARE
OKLAHOMA CITY, OK 73102-7103
(405) 235-9621 office • (405) 235-0439 fax

TULSA
500 ONEOK PLAZA
100 WEST 5TH STREET
TULSA, OK 74103
(918) 587-0000 office • (918) 599-9317 fax