An ALM Website

December 22, 2011

CORPORATE COUNSEL

From the Experts: Is Your Company Tweeting its Way into Trouble?

Four Steps to Safely Engage in Social Media

Judah Lifschitz and Laura Fraher

In the October 2010 issue of Corporate Counsel, we provided five tips that corporations should follow to avoid "ETrouble," a term we coined to refer to the devastating impact emails and electronically stored information (ESI) can have in litigation. With social media use exploding nationwide, the E-Trouble threat has expanded to platforms such as Facebook, Twitter, LinkedIn, MySpace, YouTube, and Foursquare, which all allow users to create profiles and "connect" with others to meet new people; share ideas, news, entertainment, personal information, photographs, and videos; and engage in networking.

An August 2011 Nielsen Company study found that Americans spend nearly a quarter of their online time on social networking sites and blogs, a 43 percent increase from the previous year. Since social media sites have become increasingly popular for marketing and business purposes, the risk of E-Trouble has increased, and managing that risk is mission-critical for corporations operating in today's online world.

New York Congressman Anthony Weiner's fall from grace this past summer was caused by his misuse of social media. Weiner's case may be extreme—he was forced to resign over a scandal begun by a Twitter post—but the case should serve as a warning: online activities do not remain "private" and can be very damaging. Even well-educated users exercise poor judgment while utilizing social media sites.

Consider these real-life examples:

- A Domino's employee posted a video of himself preparing sandwiches on YouTube in 2009. Viewers found the preparation unsanitary and disgusting,

Judah Lifschitz

Laura Fraher

leading to a http://www.law.com/image/cc/128_pics/Judah_Lifschitz_128.jpg major public relations crisis—and brand damage.
- Later the same year, Kansas City Chiefs running back Larry Johnson used a gay slur in a Twitter post, leading the gay advocacy group GLAAD to demand a public apology and causing public embarrassment for the franchise.
- In early 2011, during the protests in Egypt that ultimately led to the fall of that nation's government, Kenneth Cole was forced to remove an offending tweet and publish an apology on his Facebook page after he posted: "Millions are in uproar in #Cairo. Rumor is they heard our new spring collection is now available online at http://bit.ly/KCairo-KC."
- Social media firm New Media Strategies was fired by Chrysler after a NMS employee tweeted in March 2011: "I find it ironic that Detroit is known as the #motorcity and yet no one here knows how to fu**ing drive."
- The following month, PETA initiated an online boycott of GoDaddy.com after its CEO posted a video of himself killing an elephant and then tweeted about it. Competitor NameCheap.com launched a campaign for customers to transfer domains from GoDaddy to Namecheap.com for a discount, with 20 percent of the proceeds going to SaveTheElephants.com

Social media sites create significant litigation risk for companies. With almost one billion users worldwide, more than three billion photos, and 180 billion status posts each month, these sites are gold mines of data that savvy lawyers use for information and leverage.

Recently, courts have allowed discovery of the content of social media sites, providing fair warning to everyone that careless posts will come back to haunt you. In *Romano v. Steelcase, Inc. (2010)*, a New York trial court rejected the plaintiff's privacy concerns and held that the plaintiff's social media profile, postings, and pictures were discoverable, because having posted that material online, the plaintiff could have no reasonable expectation of privacy. Romano is in line with other recent cases, including from federal courts in Indiana, Colorado, Nevada, and New Jersey.

Given such a range of discovery, what real-life risks does social media content pose? Here are but two examples of the kinds of troubles that can arise:

1. Starbucks Coffee Corp. was granted summary judgment in a sexual harassment, religious discrimination, and retaliation case brought by a former employee after the employee's MySpace page was admitted into evidence, displaying the following post: "Starbucks is in deep sh*t with GOD!!! I will now have 2 to turn my revenge side (GOD'S REVENGE SIDE) 2 teach da world a lesson about stepping on GOD. I thank GOD 4 pot 2 calm down

my frustrations and worries or else I will go beserk [sic] and shoot everyone. . . ." *Mai-Trang Thi Nguyen v. Starbucks Coffee* Corp. (2009).

2. In remanding a plaintiff's social security appeal, a New Jersey federal judge noted, "although the court remands the ALJ's decision for a more detailed finding, it notes that in the course of its own research, it discovered one profile on what is believed to be plaintiff's Facebook page where she appears to be smoking. . . . If accurately depicted, plaintiff's credibility is justifiably suspect." Purvis v. Commissioner of Social Security (2011). (Plaintiff claimed to be disabled due to bronchial asthma.)

To avoid this new brand of E-Trouble, follow these four steps:

1. **Develop Goals:** Understand your company's goals in engaging in social media and how best to achieve them. Make sure that your company's involvement in social media sites adds value that outweighs the risk of online engagement. Ask yourself who will be posting and approving content on behalf of the company, and who the target audience will be.
2. **Put it in Writing:** Create a written social media policy, which will serve as a basic handbook for employees communicating through social media platforms. The policy should include, at a minimum, the following ground rules:

    - Restrict use of company computers and email addresses for social media purposes and prohibit posting or blogging during business hours, unless approved for business purposes
    - Restrict use of company logos and trademarks.
    - Prohibit posting false or disparaging comments about the company, its employees, clients, customers, business partners, or affiliates.
    - Prohibit disclosing trade secrets and confidential or proprietary information.
    - Remind employees that they should neither claim nor imply that they speak on behalf of the company. Consider requiring employees to include a specific disclaimer, such as "the views expressed are those of the author and not of the company," whenever they post anything online and the company is or could be identified.
    - Remind employees that they must adhere to all legal obligations, including copyright, trademark, privacy, and other applicable laws.
    - Remind employees that common sense and good judgment are imperative, and instruct against posting inappropriate, controversial, or offensive content, including photographs and videos.
    - Warn employees that inappropriate use of social media may be considered grounds for disciplinary action, including termination.

3. Monitor the Content: Once implemented, enforce your policy. Designate an executive responsible for monitoring the online content of the company's social media pages, as well as the publicly available content of employees' social media pages. Monitor interactions between the company's pages and third-party "followers." Monitoring will help ensure that employees know the rules and follow them, and will also enable the firm to make policy adjustments as necessary, or to quickly respond to a minor issue before it potentially spirals out of control.

4. Share the Knowledge: When implementing your online social media policy, provide the following online safety tips and content guidelines to your employees:
    - Follow password safety: Create "strong" passwords, and do not use the same password for all Internet activities.
    - Keep the personal and professional separate: Employees should use separate profiles for their personal and corporate-designated pursuits on social media sites.
    - Don't over-share: Remind employees that their remarks are in the public domain, and that they must remain vigilant to guard against inadvertently embarrassing the company by making a private dispute public or inadvertently harming the company's interests by disclosing confidential information.
    - Check privacy settings: Familiarize yourself with privacy options available, and select the appropriate settings for your use of each site.
    - Verify your connections: When connecting with others, value quality over quantity. Connect only with persons with whom you are personally acquainted. Computer hackers often try to connect with users on social media sites by suggesting that they have a common connection to the user and, once connected, access personal information.
    - Don't "over-click": Social media sites often flood a user's inbox with links to "join," "like," or "accept" groups, causes, etc., and many users click on these links without thinking. These links often allow someone to access your personal information, and they are a favorite tool of hackers. They are often encoded with malware or data miners that will infect your computer.
    - Don't endanger yourself or others: Avoid posting too much personal information that can leave you vulnerable to Internet predators. Basic information such as birthdays, addresses, phone numbers, and names of family members or pets can be used by hackers to engage in identity theft.
    - Know your audience: Certain language and images are inappropriate for sharing with professional colleagues. Avoid the use of polarizing, politically incorrect, offensive, or derogatory comments on social media sites.
    - Avoid online rage: Never tweet while angry. And above all, always think twice before clicking "submit."

Judah Lifschitz is a trial attorney and co-president of Shapiro, Lifschitz & Schram, a Washington, D.C., law firm. He can be reached at lifschitz@slslaw.com. Laura Fraher is an associate at the firm. She can be reached at fraher@slslaw.com.