

Holland & Knight

Social Media Risks to Corporate Communicators

By Timothy J. Conner, Jennifer A. Mansfield And Charles D. Tobin¹

Social media have opened up exciting and vast new platforms for corporate marketing. Active engagement with company executives, commentary on products and services, news about corporate development -- a quick tweet or Facebook posting can reach billions of consumers at almost no cost to the company.

But social media can actually cost a company millions in liability with just one careless communication. All communicators in the new media environment, and especially corporate communicators, need to be on guard for the legal risks that have been developing as fast as the technology. The risks crop up in a variety of legal areas.

Release of Confidential Information

New media present new means for a company's employees, through wrongdoing or inadvertence, to release confidential or sensitive information. Once information is released through social media, it can be nearly impossible to pull it back. The improper release of confidential information can lead to unwanted publicity and legal exposure.

For example, in October of this year, a vendor for Lawrence (Kansas) Memorial Hospital's on-line bill pay service experienced a computer glitch that exposed the financial information of more than 8,000 patients, triggering a federal investigation. The hospital faces potential exposure of up to \$25,000 in fines from the U.S. Office of Civil Rights, the federal agency that oversees patient privacy and confidentiality. The hospital also issued letters to all of the 8,000 plus patients and offered them a one-year subscription to a credit monitoring service.

In another example, Wisconsin nurses posted confidential patient X-rays on Facebook, which instigated an FBI investigation for potential violations of the Health Insurance Portability and Accessibility Act ("HIPAA"). Civil penalties can be as high as \$1,500,000 for all violations in a calendar year. The U.S. Department of Health and Human Services is considering implementing regulations in early 2012 that would allow individuals to receive a percentage of fines levied or monetary settlements reached with the government. And, although there is no private cause of action for HIPAA violations, Missouri has allowed them to form the basis for state law claims of negligence per se, and under North Carolina law, a HIPAA violation may be actionable as an intentional infliction of emotional distress. Litigation in this area surely will increase.

Intellectual Property Infringement

The widespread access to photographs, literature and other creative works on the Internet also has led to a proliferation of intellectual property claims. Many people have the mistaken impression that if they find a photograph or video on the internet, it's okay to reuse it. A company may encounter risk through two primary sources: employees posting on behalf of the company and individual users posting on the company's website.

¹ Mr. Conner and Ms. Mansfield are with the National Media Practice Team of Holland & Knight LLP and are resident in the firm's Jacksonville, FL office. Mr. Tobin is the chair of the firm's practice team and is resident in the firm's Washington D.C. office.

For example, the website unclebarky.com reported that it took down photos it posted of reporter and news anchor Kim Fischer after the photographer threatened a copyright infringement lawsuit. In November 2011, Singapore Press Holdings sued Yahoo! in the Singapore High Court for allegedly reproducing 23 articles from its newspapers over a 12-month period.

Maremont v. Susan Fredman Design Group, Ltd. is a more unusual case, where a U.S. federal court held that the plaintiff stated a claim for false endorsement under the Lanham Act, 15 U.S.C. § 1125(a)(1)(A). The plaintiff in that case, a popular interior designer with large social media followings, was severely injured in an accident. While Maremont was still in the hospital, employees of Susan Fredman Design Group, where she worked, posted to Facebook and Twitter under Maremont's accounts, which showed Maremont's photo next to the posts. Although Maremont asked her employer to stop posting under her name, the posts continued until Maremont eventually changed her passwords. In a March 2011 opinion, the court held that Maremont's allegations of "Defendants' deceptive use of her name and likeness" stated a claim for false endorsement, which is misuse of a trademark, and denied the defendant's motion to dismiss. Later, in December 2011, the court denied summary judgment, opening the door for the plaintiff to prove actual damages under the Lanham Act claim.

Of course, the Internet is not a "public domain" smorgasbord, where everyone is free to graze on others' artistic content. The copyright to images and literature on the Internet presumptively remains the property of the creator or their assignee. Companies therefore need to be careful before lifting material off of the internet and using it for themselves.

Defamation and Privacy Claims

Section 230 of the federal Communications Decency Act, 47 U.S.C. § 230, protects companies from liability when someone *outside of the company* posts injurious material on the company's website. The company itself, however, may be liable *when an employee posts* defamatory or invasive material. The law does not protect the company when, in the eyes of the law, it is the publisher of the wrongful statement.

For this reason, a Minnesota court held that an invasion of privacy claim could result from a healthcare worker posting test results diagnosing a sexually transmitted disease on a publicly accessible social network, even though the information remained on the Web for just 24 hours. Likewise, the parents of a murder victim sued the individual and the employer when an emergency medical worker posted photographs of the victim's body on Facebook.

Government Regulations to Protect Consumers and Children

Government regulations concerning advertising or communicating to others via social media also impose restrictions. For instance, regulations on advertising under the federal Food, Drug, and Cosmetics Act apply equally to social media sites and print advertising. In 2010, the Food and Drug Administration issued a warning letter to Novartis for four violations relating to information "shared" about the drug Tasigna on Facebook.

Likewise, Securities and Exchange Commission regulations regarding communications about stocks and other investments apply to information posted on social media. In 2007, the CEO of Whole Foods Market engaged in "sock puppet" activities -- creating a false person and posting criticisms of competitors while praising Whole Foods -- that led to an SEC investigation of the company. Although the SEC eventually found no violations of regulations, the company went through a gauntlet of bad publicity and undoubtedly incurred extensive costs to defend the multi-year SEC investigation.

The Federal Trade Commission in 2009 also implemented regulations that now require on-line product reviewers to disclose connections between advertisers and their endorsers that might materially affect the weight or credibility of the endorsement. The FTC has aggressively enforced this provision with respect to bloggers. For example, in 2010, the FTC approved a final order settling charges that Reverb Communications, Inc., and its owner, Tracie Snitker, engaged in deceptive advertising by posing as ordinary consumers posting game reviews at the online iTunes store, without disclosing that the reviews came from paid employees working on behalf of the developers. And earlier this year, the FTC finalized an order settling charges that Legacy Learning Systems Inc. and its owner, Lester Gabriel Smith, deceptively advertised the "Learn and

Master Guitar” program through online affiliate marketers who falsely posed as ordinary consumers or independent reviewers without clearly disclosing they were paid substantial commissions for every sale they generated. Under the final order, Smith and Legacy Learning will pay \$250,000, and maintain a system to review and monitor their affiliate marketers’ representations and disclosures.

The government has also become proactive in protecting children on the web. If a company’s website targets children under thirteen years of age, or the company should know that children under thirteen are attracted to the website, then the company must comply with the Children’s Online Privacy Protection Act (COPPA), 15 U.S.C. §§ 6501-06. Under COPPA, companies with websites must obtain verifiable parental consent when they collect personally identifiable information for their own use, or when they collect such information that will be publicly posted.

Labor and Employment Claims

In 2010, CareerBuilder.com and Jobsite released studies showing that employers used social media to support their recruitment efforts and to research job candidates. But sometimes employers will receive information via social media that they cannot lawfully consider when hiring, such as race or religion. If the employer receives that information anyway, it must take steps to ensure that it does not base hiring decisions on the protected status.

For example, under the antidiscrimination provisions of Title VII of the Civil Rights Act of 1964, 42 U.S.C. § 2000e *et seq.*, an employer cannot take religion into account in making employment decisions. But in *Gaskill v. University of Kentucky* a federal court found direct evidence that an applicant was denied employment precisely because of his religious beliefs. In that case, Gaskill was a professor considered the lead candidate to head the University’s new observatory, when a search committee member found an on-line article he authored titled “Modern Astronomy, the Bible, and Creation,” causing concerns about whether to hire a “creationist.” A key document was an email from the chair of the search committee complaining to the head of the astronomy department that Gaskill will be denied the job “because of his religious beliefs” and that “no objective observer could possibly believe” the decision was based on anything other than religion, because Gaskill was “so superbly qualified [and] so breathtakingly above the other applicants in background and experience.” The federal district court denied cross motions for summary judgment, soon after which the University paid Gaskill \$125,000 as part of a settlement agreement in which it denied any wrongdoing.

Social media posts on company sites also provide fertile fodder for disparate treatment claims. A mid-level manager’s discriminatory animus or statements could support a discrimination claim against the company. In *Blakey v. Continental Airlines, Inc.*, a court held that the airline could be liable for harassing remarks employees allegedly made on the airline’s internet forum for crew members. While employers should not be held liable for non-work social media sites that they do not know about, even for private Facebook or Twitter posts, employers are potentially liable when they learn about harassing posts but do nothing to stop the conduct.

Workplace use of social media also can bring federal labor law claims. Even in right-to-work states, the law protects employees’ discussions of the “terms and conditions of employment.” For this reason, a National Labor Relations Board administrative law judge recently determined that a New York nonprofit organization violated federal law when it fired five employees for their Facebook posts reacting to a co-worker’s criticism of their performance. The judge held that the employees have a right to discuss the terms and conditions of their employment, and the Facebook posts were “concerted” activity, and therefore protected under the Act.

Some NLRB administrative decisions and complaints have declared certain firings over social media posts to be protected activity, while others have found that the firings were lawful. Before firing an employee over his or her social media posts, the company should analyze the posts for protected content -- such as gripes about the boss or how much employees are paid -- and whether the posts are between coworkers. If the posts are about the terms and conditions of employment, or are shared with coworkers, they may be protected by law.

Protecting the Company from the Risks of Social Media

Companies of course want to continue to push information out over the Internet and interact with customers through social media. That makes perfect business sense. But the company can and should also take reasonable steps to protect itself while taking advantage of these wonderful new forms of communication. For example:

- The company's website should always contain the most up-to-date terms of use and privacy policies.
- Companies should implement clear policies that address which employees can use social media in the workplace, what types of materials they may post, and that the company expects all employees to safeguard proprietary and private information at all times.
- Appropriate internet use on company time should become a regular part of new-employee training, and should be reinforced through company in-services and written internal communications.
- Company managers should be trained in employee privacy rights, laws against discriminatory communications in the workplace, federal labor relations laws, and other legal issues protecting employee communications.
- Company policies should be implemented setting out what information can be considered when hiring and whether or when an internet search will be conducted on candidates.
- Employees should be trained to obtain clearance from the copyright holder for the use of material found on the Internet. The company also should implement the procedures under the Digital Millennium Copyright Act (DMCA), 17 U.S.C. § 512, so that the company is protected when it follows the "safe harbor" provisions of the law.
- All companies should secure insurance to cover as many of these risks as possible.

With proper training and risk management, social media provide a low-cost and reasonably safe environment for companies to expand their businesses and engage their consumers.

