BUSINESS LAW NEWS

The State Bar of California • Issue 4 2011

10 Social Media Must Haves For Your Corporate Compliance And Ethics Program

Michelle Sherman

Companies would be legally remiss not to add a social media component to their corporate compliance and ethics program. Agencies such as FINRA, the FTC, and the NLRB are bringing complaints against companies arising from their social media activity or employee related activity, thus highlighting the need for companies to demonstrate that they are exercising due diligence to promote ethical conduct and prevent criminal conduct in the context of social media activity.[1] The following list is a starting point; however, there may be additional items that a social media attorney would recommend a company include in its policy depending on the nature of its business.

Michelle Sherman

Michelle Sherman is the editor and author to the Social Media Law Update blog at the law firm of Sheppard Mullin Richter & Hampton, where she is Special Counsel in the Business Litigation and Government Contracts practice groups. Ms. Sherman also advises businesses on social media and Internet legal issues.

1. Adopt a Social Media Policy

The majority of companies realize that they need to have a social media policy for a variety of reasons, but only about a third of them have a written policy. There are at least three good reasons for a company to have a social media policy. First, companies with a social media policy can take advantage of a "safe harbor" offered by the FTC in connection with its amended guidelines for online endorsements and testimonials ("Endorsement Guidelines").[2] In notes to its "Guide Concerning The Use of Endorsements and Testimonials," the FTC recognized that a business cannot realistically oversee all of the social media posts by its employees and ensure that they do not violate the Endorsement Guidelines.[3] The FTC has stated that the employer should not be held liable in this situation if: (1) the employer has a social media policy concerning the "social media participation" of its employees; and (2) the established company policy adequately covered the "rogue" employee's conduct. Second, a social media policy (coupled with a confidentiality agreement and computer use policy) is a good way for companies to show that they are taking reasonable measures to protect their trade secrets by addressing the risks of employees posting about new products or other proprietary information on social networking sites such as LinkedIn or Facebook. Third, a social media policy is a good way to protect the company's brand. Many employees do not appreciate the risks of social media, and that their social media activity may hurt the brand of the company due to embarrassing and thoughtless posts in which employees are associated with their employer.[4]

For the companies that have adopted a social media policy any time before August 2011, when the NLRB issued a report discussing social media activity by employees and company policies to regulate this activity, there is a good chance that these company policies are overbroad. In the August 18, 2011 report, the Acting General Counsel for the NLRB reported on the outcome of investigations into 14 cases involving the use of social media and employer's social media policies. The NLRB Report stated that employers had the most problems with overbroad policies.[5]

Social media policies adopted prior to August 2011 need to be reviewed, and most likely revised, to ensure that protected activity under Section 7 of the National Labor Relations Act is not being chilled or prohibited. A policy that tells employees they cannot "disparage the company" or "criticize co-workers" without carving out online conversations between employees concerning work conditions, benefits, or

The State Bar of California
180 Howard Street
San Francisco, CA 94105
(415) 538-2341
www.calbar.ca.gov

compensation is overbroad. Section 7 provides in pertinent part that: "[e]mployees shall have the right to self-organization, to form, join, or assist labor organizations, to bargain collectively through representatives of their own choosing, and to engage in other concerted activities for the purpose of collective bargaining or other mutual aid or protection."[6] In practice, this means that employers cannot chill or penalize communications between employees concerning work conditions, terms and conditions of employment (salary, benefits), managers, and management.

The financial incentive for making sure your policy, as well as its application to your employees' social media activity, is done correctly is underscored by a September 2, 2011 administrative law judge (ALJ) opinion. In *Hispanics United of Buffalo, Inc.,* the ALJ ordered the non-profit Hispanics United of Buffalo, Inc. ("HUB") to rehire and provide back pay to five employees who were fired over Facebook posts in which they complained about criticisms of their job performance by another HUB employee.[7]

A social media policy can tell employees "to do" the following when it comes to any social media activity in which they are associated with the company: (1) Maintain high privacy settings; (2) Protect confidential and proprietary information; (3) Respect the privacy of other people; and (4) Abide by all laws and regulations. Some "Don'ts" in a social media policy may include: (1) Do not provide online recommendations for current employees of the company; (2) Do not endorse the company's products or services without having your post approved in advance by the marketing department; and (3) Be clear your views are your own, and that you are not speaking on behalf of the company.

2. Implement Your Social Media Policy With an Effective Training Program

Notwithstanding the exponential growth of people using Facebook and other social networking sites, people are still relatively uninformed about the risks of social media and seem genuinely surprised to learn later that prospective employers are researching candidates on the Internet. And, more significantly for companies, parties in litigation are being ordered to produce their Facebook activity when there has been some showing that it is relevant or may lead to the discovery of admissible evidence.[8] Accordingly, it is important for companies to communicate their social media policy to employees. An effective training program should emphasize areas of particular concern for your company which may include, for example, protecting the privacy interests of your customers, complying with FINRA/SEC social media guidelines, antitrust compliance, not disclosing confidential or proprietary information, and brand protection.

3. Update Your E-Discovery Approach

Social media activity by companies should be thought of as an extension of "electronically stored information" ("ESI") and the discovery rules that apply when a company is in a legal dispute that would trigger a duty to preserve company emails and electronic documents. When the Federal Rules of Civil Procedure were amended in 2006 to include ESI, the term was "intended to be read expansively to include all current and future electronic storage mediums."[9] It does not matter how brief the storage period, courts will treat the information as discoverable. Accordingly, even storage in the "cloud" or on a social networking site will be treated as discoverable ESI. To summarize the e-discovery rules, there is a duty to preserve relevant or potentially relevant information once litigation is pending or reasonably anticipated as long as it is in your custody or control. For the party filing the legal action, the litigation hold and "do not destroy" notice should be triggered before the complaint is filed. "A duty to preserve evidence arises when there is knowledge of a potential claim."[10]

Companies that wait until they are in litigation to adopt a document retention policy have been sanctioned by the court, and they receive stiffer penalties when there is evidence that discoverable documents have been destroyed in the meantime. A study in 2010 found that courts are increasingly imposing strong sanctions against attorneys and their clients for failing to comply with the e-discovery rules.[11] In the 401 cases in which sanctions were sought, the study found that sanctions were awarded in over half of them.[12] Some of the sanctions were especially severe and included case dismissals, adverse jury instructions, and large monetary sanctions.[13] Five million dollar sanctions were ordered in five cases, and $1 million or more in four others.[14] Defendants were sanctioned for e-discovery violations nearly three times more often than plaintiffs,[15] and the number one reason for imposing sanctions was failure to preserve electronic evidence.[16] Thus, it may be fiscally negligent for companies not to address social media activity in their e-discovery policies and procedures.

4. Update Your Document Retention Policy

If your company is using social networking sites for business purposes, then your document retention policy should be updated to capture social media activity, including posts on how the company is doing financially, online advertising, and

communications with consumers. The time periods used for offline communications based on the nature of their content are a good model for what retention periods should be used for social media activity.[17] Further, if your company is in a regulated industry, it may be subject to guidelines for document retention. If your company is in one of those industries, a good bright line rule is to capture the same online communications that you are required to maintain if they were offline communications.[18]

5. Update Your Sarbanes-Oxley Act Compliance Program

Section 409 of the Sarbanes-Oxley Act of 2002 ("SOX") provides in pertinent part that: "Each issuer reporting under section 13(a) or 15(d) shall disclose to the public on a rapid and current basis such additional information concerning material changes in the financial condition or operations of the issuer … as the Commission determines, by rule, is necessary or useful for the protection of investors and in the public interest." The public policy intent behind Section 409 is reflected in the Regulation Fair Disclosure ("Regulation FD")[19] and how it is applied by the SEC.[20] Regulation FD mandates that all publicly traded companies disclose material information to all investors at the same time. Section 409 also resulted in the SEC substantially increasing the disclosure requirements under Form 8-K. Form 8-K is "the 'current report' companies must file with the SEC to announce major events that shareholders should know about."[21]

With many companies now posting their financial statements on their website or through links on their Facebook fan page or Twitter account, it is important for companies to update their internal procedures for disclosures to the public to ensure that the reports filed with the SEC are consistent with statements made on their social media networking sites and vice versa. There needs to be coordination between the finance department, public relations, the legal department, and the department responsible for maintaining the social media sites to ensure that press releases concerning material changes in the financial condition or operations of the company are also reflected on social media sites. "Material changes" may include, for example, events that would require a company to issue a Form 8-K or Regulation FD disclosure. At the same time, it is important that updates on the social media sites do not precede the announcement through the traditional published press release and SEC reports. Further, do not disclose material information on Twitter or Facebook that is not available elsewhere.

To underscore the importance of updating information on company sponsored sites, it is worth considering Credit Suisse and the fine of $4.5 million that was imposed on it by FINRA. In its May 26, 2011 press release, FINRA notes that "[a]lthough Credit Suisse knew of these inaccuracies, it did not . . . *correct the information on the website where the information was displayed* (emphasis added)." Credit Suisse is reported in the FINRA press release as not admitting or denying the charges but consenting to the entry of FINRA's findings. The Credit Suisse fine was based on conduct dating back to 2006, suggesting that companies should consider auditing their website and social media sites to make sure that information posted there is not outdated, incorrect, or misleading.

6. Audit the Social Media Activity of Potential Targets for Mergers and Acquisitions

Before acquiring a company, conduct an audit to identify the potential risk of your company being financially responsible for pre-acquisition violations of FINRA, SEC regulations, or SOX on the target company's respective websites or social media accounts.

7. Establish an Internal Procedure for When and How the Internet Can Be Used to Make Employment Decisions.

In a January 2010 survey commissioned by Microsoft, 70 percent of the 275 U.S. recruiters, human resources professionals, and hiring managers who responded said they have rejected candidates based on information found online.[22] Thirty-five percent of those employers said they rejected applicants based on membership in certain groups.[23] Making an employment decision based on group membership may violate federal or state law where membership is related to a protected class. Protected factors include, for example: (1) Race, color, national origin, religion, and gender under Title VII of the Civil Rights Act of 1964; and (2) Sexual orientation, marital status, pregnancy, cancer, political affiliation, genetic characteristics, and gender identity under California law. Most states have their own list of protected factors, which should be considered depending on where your company has employees. This year, the University of Kentucky paid $125,000 to settle a religious discrimination case that included evidence of the University's Physics and Astronomy Department search committee making inquiries into the leading candidate's religious beliefs after a committee member found through an Internet search that the candidate, Dr. C. Martin Gaskell, had a personal website with an article entitled "*Modern Astronomy, the Bible, and Creation.*"

Thus, it makes sense for companies to implement an internal policy along the following lines: (1) HR department training on interview skills and managing employees should

include the ways in which information taken from social media and Internet searches can possibly give rise to allegations of employment discrimination; (2) Internet searches should only be allowed for candidates who are being brought into the office for interviews having been pre-screened; and (3) Internet searches of job applicants or employees should be done by people who are removed from making employment decisions so they can filter out information that are protected factors before the search results are forwarded to company employees who are giving performance reviews or making recommendations on hiring, promotions, or downsizing.

If a company decides to use an outside vendor for social media background checks, the company should still have an internal policy for what managers can and cannot do when making employment decisions. It is not uncommon for companies to be unaware of the extent to which their employees are using the Internet to interview people and make employment decisions.

Further, outside vendors are required to comply with the Fair Credit Reporting Act ("FCRA") in providing background checks using the Internet,[24] in addition to being subject to corresponding state laws as applicable. The FCRA requires, among other things, that: (1) the employer get written permission to obtain a report on the applicant or employee; (2) if the employer decides to take adverse action based on the report such as rejecting the candidate or passing an employee over for a promotion, then the employer must issue a "pre-adverse action disclosure" to the applicant or employee with a copy of the report and a summary of the person's rights under the FCRA; and (3) the employer must provide the affected person with notice that he or she has a right to dispute the accuracy of the report with the consumer reporting agency.[25]

One outside vendor for social media background checks, Social Intelligence Corporation, has been asked to respond to questions raised by U.S. Senators Richard Blumenthal (D-Conn) and Al Franken (D-Minn) in a letter dated September 19, 2011.[26] In their letter, the Senators ask Social Intelligence to state what steps it is taking to ensure that information gathered from social networks is accurate; whether the company is respecting the guidelines for how the websites and their users want the content used; and whether the company is protecting consumers' right to online privacy.

In light of the Senators' letter, companies may want to consider how much weight to give information from a social media background check. In addition, companies may want to ask outside vendors for written assurances that no laws have been violated in gathering the information (*e.g.* FCRA, privacy, copyright, or other intellectual property laws).

8. Take Reasonable Measures to Protect Your Trade Secrets.

Update your confidentiality agreements and computer use policies with employees, and use a broad definition of "trade secrets" as reflected in the Economic Espionage Act.[27] Clearly communicate what are the company's trade secrets and the ways in which use of them is restricted. One of the essential elements for a misappropriation of trade secrets case is that the company has taken reasonable measures to protect its trade secrets, which would include, in the social media era, a social media policy with training for employees so they are not inadvertently disclosing the company's trade secrets. In the unfortunate situation of having to pursue a misappropriation of trade secrets case, have your litigation counsel consider a civil claim for violation of the Computer Fraud and Abuse Act as well since most misappropriation cases these days include the downloading of information from computer databases in excess of the person's authorized access to the company's computers.[28]

9. Incorporate Privacy Protections Into Your Business Practices.

Verizon reports in its 2011 Data Breach Investigations Report that 509 million records were compromised by data breaches from 2008-2010. [29] This report also states that the attacks are usually not highly sophisticated, and, further, that "almost all breaches are avoidable (or at least in hindsight) without difficult or expensive corrective action."[30] Accordingly, there are steps companies can and should be taking to protect their data, including, for example, installing and maintaining a firewall to protect data, encrypting transmission of cardholder data and sensitive information across public networks, using and regularly updating anti-virus software, implementing strong access control measures, locking out users after a few failed attempts to enter their password, and restricting access to data by business need-to-know.

Because data breaches do occur, companies should also incorporate privacy protections into their business practices. Companies should collect only a reasonable amount of information and no more, have sound retention practices for consumer information (not an unduly long period of time), and take steps to ensure data accuracy (so misinformation is not reported on consumers).

10. Review the FTC Guidelines for Online Endorsements With Employees

In order to benefit from the "safe harbor" provided by the FTC for companies with a few "rogue" employees who violate the Endorsement Guidelines, companies need to communicate their social media policy to employees. While unintentional in most instances and posted with the best of intentions, employees continue to post positive reviews without disclosing that they work for the PR company promoting the product or the company that is selling it. Employees need to understand that they cannot post reviews for the company's products (or the products of its competitors) without disclosing their relationship with the employer company. Further, when companies learn of reviews that employees have posted in violation of the FTC Endorsement Guidelines, they need to take steps to remove them.

Conclusion

While there is not a perfect overlap between the laws that govern offline conduct and social media activity, these laws do provide a useful starting point for what companies should include in their corporate compliance and ethics programs. As described above, the case law and regulations continue to develop in this area, and companies are expected to stay current or be held legally liable through sanctions, damages, or injunctive relief. ■

Endnotes

1 U.S. Sentencing Guidelines Manual, § 8B2.1 (2010) (providing that to have an effective compliance and ethics program an organization "must exercise due diligence to prevent and detect criminal conduct" and "promote an organizational culture that encourages ethical conduct" and compliance with the law), *available at* http://www.ussc.gov/Guidelines/2010_guidelines/index.cfm.

2 FTC, Guides Concerning The Use of Endorsements and Testimonials In Advertising, 16 C.F.R. § 255 (2009).

3 *Id.* at 48 (the FTC "is not aware of any instance in which an enforcement action was brought against a company for the actions of a single 'rogue' employee who violated established company policy that adequately covered the conduct in question").

4 *See, e.g.*, David Bauder, *Octavia Nasr fired by CNN – the editor tweeted admiration for Grand Ayatollah Mohammed Hussein Fadlallah*, WashingtonPost.com, July 8, 2010; Stephanie Clifford, *Video Prank at Domino's Taints Brand*, New York Times, April 15, 2009.

5 https://www.nlrb.gov/news/acting-general-counsel-releases-report-social-media-cases.

6 29 U.S.C. § 157.

7 *Hispanics United of Buffalo, Inc.*, Case No. 3-CA-27872 (NLRB Div. of Judges Sept. 2, 2011).

8 *EEOC v. Simply Storage Mgmt.*, 2010 WL 3446105, at *3 (S.D. Ind. May 11, 2010).

9 Notes of the Advisory Committee to the 2006 Amendments to Fed. R. Civ. P. 34.

10 *Micron Tech v. Rambus,* 255 F.R.D. 135 (D. Del. 2009).

11 Dan H. Willoughby, Jr., Rose Hunter Jones, Gregory R. Antine, *Sanctions for E-Discovery Violations: By The Numbers*, 60 Duke L.J. 789 (2010).

12 *Id.* at 789.

13 *Id.* at 803-04.

14 *Id.* at 814.

15 *Id.* at 803.

16 *Id.* at 789.

17 *See, e.g.,* FINRA Regulatory Notice 11-39 (August 2011) (citing Reporting Requirements for Brokers or Dealers under the Securities Exchange Act of 1934, SEC Rel. No. 34-38245 (Feb. 51997) ("The SEC has stated that the content of an electronic communication determines how it must be preserved.").

18 *See, e.g.,* FINRA Regulatory Notice 10-06 (January 2010); Regulatory Notice 11-39 (August 2011).

19 17 C.F.R. §§ 243.100 – 243.103.

20 SEC, *Commission Guidance On The Use Of Company Web Sites* (August 7, 2008), *available at* http://www.sec.gov/rules/interp/2008/34-58288.pdf.

21 http://www.sec.gov/answers/form8k.htm.

22 Cross-tab Transforming Market Research, *Online Reputation In A Connected World*, at 3 (January 2010), *available at* http://ilookbothways.com/2010/07/08/microsoft-online-reputation-in-a-connected-world/.

23 *Id.*

24 FTC letter to Renee Jackson, Nixon Peabody LLP, Counsel for Social Intelligence Corporation (May 9, 2011).

25 15 U.S.C. § 1681 et seq.

26 Letter from Senators Richard Blumenthal (D-CT) and Senator Al Franken (D-MN) to Max Drucker, CEO and President of Social Intelligence Corporation (September 19, 2011).

27 18 U.S.C. § 1839.

28 18 U.S.C. § 1030(g).

29 www.verizonbusiness.com/resurces/reports/rp_data-breach-investigations-report-2011_en_xg.pdf.

30 *Id.* at 3.