

Reproduced with permission from Privacy & Security Law Report, 10 PVLR 1163, 08/15/2011. Copyright © 2011 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>

Getting It Right: Five Must-Have Provisions for Your Social Media Policy



BY MELISSA J. KRASNOW

Prevalence of Social Media Policies

According to a recent survey¹ of technology, federal government, financial services, health care, education and other organizations, 68 percent of respondents have social media policies. In a 2009 survey² by Manpower, 29 percent of companies in the Americas had a social media policy. Companies that do not have social media policies likely are preparing them or at a minimum considering them.

Melissa J. Krasnow, a partner in the Corporate Group of Dorsey & Whitney LLP in Minneapolis, is a Certified Information Privacy Professional and serves on the International Association of Privacy Professionals Publication Advisory Board.

Common Provisions of Social Media Policies

Certain provisions are common in social media policies. Based on a review of company social media policies, including the publicly available policies of six public companies (i.e., Best Buy, Coca-Cola, IBM, Intel, Nordstrom and Wells Fargo),³ these provisions include: (1) use common sense and do not be misleading, (2) do not disclose confidential or proprietary information, (3) do not disclose material nonpublic information, (4) comply with company policies and applicable law and (5) identify yourself and fully disclose your affiliation when you communicate about the company.

Use Common Sense and Do Not Be Misleading

A number of policies advised employees to use common sense and exercise judgment when using social

¹See nCircle 2011 Social Media Security Trends Survey, March 2011, at http://www.ncircle.com/index.php?s=resources_surveys_Survey-SocialMedia-2011.

²See "Social Networks vs. Management? Harness the Power of Social Media, Manpower, January 2010, at https://candidate.manpower.com/wps/wcm/connect/97091280420bb140a9bbeda17e379a88/MANP_285779_WHITE_1up.pdf?MOD=AJPERES

³See Best Buy Social Media Policy, last updated April 13, 2011 at <http://forums.bestbuy.com/t5/Welcome-News/Best-Buy-Social-Media-Policy/td-p/20492>; Coca-Cola Online Social Media Principles, Dec. 15, 2009 at <http://www.thecocacolacompany.com/socialmedia/>; IBM Social Computing Guidelines, 2010 at <http://www.ibm.com/blogs/zz/en/guidelines.html>; Intel Social Media Guidelines, last update March 2010, at <http://www.intel.com/content/www/us/en/legal/intel-social-media-guidelines.html>; Nordstrom Social Networking Guidelines, Feb. 25, 2011 at <http://shop.nordstrom.com/c/social-networking-guidelines> and Wells Fargo Blogs and Social Media Community Guidelines at <http://blog.wellsfargo.com/community-guidelines.html>.

media, and said that individuals were responsible for their postings. Negative communications about the company or other companies (such as competitors or vendors or their products and services) or certain individuals (such as customers), should be avoided, according to numerous policies. Many policies also advised not to use social media in a false or misleading way. The Federal Trade Commission's 2009 Guides Concerning the Use of Endorsements and Testimonials in Advertising⁴ (the FTC Guides), which prohibit making false or unsubstantiated statements, is a basis for this provision. See 16 C.F.R. Part 255.

A virtual world example of being misleading that occurs with frequency is being an impostor. It is neither difficult nor uncommon for a person to establish an account at a social media website and claim to be someone else (e.g., an executive officer of a company) or claim that the account is on behalf of a company. Impersonating another through an account at a social media website typically violates the terms of use of the website.⁵ See the Facebook Statement of Rights and Responsibilities and the Twitter Impersonation Policy.

Do Not Disclose Confidential or Proprietary Information

A key concern of companies is that the use of social media increases the risk of disclosing confidential or proprietary information, even unintentionally. As a result, many policies contain a provision broadly prohibiting this on behalf of the company and often specifying what confidential or proprietary information is. Some companies add financial or other sensitive information to confidential or proprietary information. In addition to company confidential information, the prohibition often extends to the confidential information of the company's competitors, business partners, customers and employees. Finally, policies may provide examples for illustrative purposes.

Do Not Disclose Material Nonpublic Information

For public companies, there is the additional category of material nonpublic information. A company or a person acting on behalf of the company that intentionally or unintentionally selectively discloses material nonpublic information must make simultaneous or prompt public disclosure of that information. See the Security and Exchange Commission's Rule 100 of Regulation FD.⁶ Public disclosure of material nonpublic information can be made by (1) furnishing or filing a report on the SEC's Form 8-K or (2) disseminating the information through another method of disclosure reasonably designed to provide broad, non-exclusionary distribution of the information to the public.⁷ See Rule 101(e) of Regulation FD. Other company policies that cover

material nonpublic information (e.g., insider trading policy and disclosure policy) should be reviewed to make sure they are consistent and integrated with a policy covering social media. Such other policies also may be cross-referenced in a policy covering social media.

Comply with Company Policies and Applicable Law

This provision is important because other company policies should be reviewed in preparing a social media policy. Does another policy cover aspects of social media and could such policy be amended and updated instead of preparing a stand-alone social media policy? The answer will depend on the situation of the particular company.

For example, many companies have an electronic communications policy to address appropriate uses of the company's computer system and to reduce employee expectations of privacy and a company's risk. Often, an electronic communications policy is amended to address the use of social media.

However, if a company does not have an electronic communications policy, the following provisions can be included in a social media policy where the company: (1) expressly reserves the right to access and monitor the use of the company's computer network, equipment and communications systems and the contents of files and communications created, stored, sent or received on the systems; (2) notes that the computer network, equipment and communications systems are company property and; (3) states that there should be no expectation of privacy in anything created, stored, sent or received through the company's computer network, equipment, communications systems or the internet. Court cases considering employers' right to monitor or review material sent or received on a company computer are fact-specific and consider, among other things, the language of the policy at issue and the extent to which it has been used or enforced in the past.⁸ See, for example, *City of Ontario v. Quon*, 130 S. Ct. 2619 (2010) and *Stengart v. Loving Care Agency, Inc.*, 990 A.2d 650 (N.J. 2010).

An electronic communications policy also often addresses the extent of personal use of the company's computer network, equipment, and communications systems. Many policies limit personal use or keep personal use to a minimum. Such a policy should be reasonable and enforceable and enforced consistently.

Regardless of which approach is taken, a policy covering social media should be drafted to be consistent and integrated with other company policies (e.g., electronic communications policy, code of ethics, code of conduct, record retention policy, privacy policy, employee handbook, insider trading policy and disclosure policy, etc.). In addition to company policies, if company agreement provisions could be implicated (e.g., confidentiality provisions), they should be reviewed as well. If there is any inconsistency between the policy covering social media and another company policy or agreement, the one that will govern should be noted. In

⁴ The FTC Guides Concerning the Use of Endorsements and Testimonials in Advertising are at <http://ftc.gov/os/2009/10/091005revisedendorsementguides.pdf>.

⁵ The Facebook Statement of Rights and Responsibilities is at <http://www.facebook.com/terms.php>. The Twitter Impersonation Policy is at <http://support.twitter.com/entries/18366-impersonation-policy>.

⁶ Rule 100 of Regulation FD is at <http://www.sec.gov/divisions/corpfin/guidance/regfd-interp.htm>.

⁷ Rule 101(e) of Regulation FD is at <http://taft.law.uc.edu/CCL/regFD/FD101.html>.

⁸ The U.S. Supreme Court's 2010 decision in *City of Ontario v. Quon* is at <http://www.supremecourt.gov/opinions/09pdf/08-1332.pdf>. The New Jersey Supreme Court's 2010 decision in *Stengart v. Loving Care Agency* is at <http://pdfserver.amlaw.com/nj/Stengart-A16-09.pdf>.

addition, policies often include a provision about complying with applicable law (e.g., intellectual property law).

Identify Yourself and Fully Disclose Your Affiliation When You Communicate about the Company

The FTC Guides require full disclosure of a material connection between an advertiser and an endorser that might materially affect the weight or credibility of the endorsement. See 16 C.F.R. § 255.5.⁹ Employees of a company who make comments about the company or its products or services, particularly in a positive manner, must fully disclose that they are employees of the company. The FTC issued Frequently Asked Questions for the FTC Guides in June 2010,¹⁰ which address material connections, among other things. In addition, the Word of Mouth Marketing Association, an organization dedicated to advancing and advocating credible word of mouth marketing (WOMMA), issued the WOMMA Guide to Disclosure in Social Media Marketing in the wake of the FTC Guides in February 2010.¹¹ This WOMMA Guide describes disclosure practices regarding material connections.

It is important to note that the FTC has enforced the requirement to fully disclose a material connection under the FTC Guides. See *In the Matter of Reverb Communications, Inc.*, FTC File No. 092 3199, Nov. 26, 2010; *In the Matter of Legacy Learning Systems, Inc.* FTC File No. 102 3055, June 10, 2011; and *Closing Letter, AnnTaylor Stores Corporation*, FTC File No. 102-3147, April 20, 2010.¹² For example, in *Reverb Communications*, a public relations agency hired by video game application (including mobile gaming application) developers settled charges of engaging in deceptive advertising where its employees posed as ordinary consumers, posted game reviews at the online iTunes store and failed to disclose that the reviews came from paid employees working on behalf of the developers.

The FTC approved a final order settling charges that, among other things, (i) prohibits the public relations

agency from misrepresenting that the user or endorser is an independent, ordinary consumer, and from making endorsement or user claims about a product or service unless they disclose any relevant connections that they have with the seller or the product or service and (ii) requires the public relations agency to remove any previously posted endorsements that misrepresent the authors as independent users or ordinary consumers and that fail to disclose a connection between the public relations agency and the seller of a product or service.

David Vladeck, director of the Bureau of Consumer Protection of the FTC, said in May 19 testimony to the Senate Committee on Commerce, Science, and Transportation: “The *Reverb* settlement demonstrates that the FTC’s well-settled truth-in-advertising principles apply to new forms of mobile marketing . . . as in the offline world, companies must be able to substantiate claims made about their products. Developers may not make misrepresentations or unsubstantiated claims about their mobile apps, whether those claims are in banner ads, on a mobile website, in an app, or in app store descriptions. FTC staff is working to identify other violations of these well-established principles in the mobile context.”¹³

A number of policies also require that employees expressly state when they are communicating for themselves and not on behalf of the company and when their views are their own and do not necessarily represent those of the company. Best Buy’s Chief Ethics Officer recently blogged about the following interesting real-life situation: “Among the do’s and don’ts described in [Best Buy’s Social Media] Policy: [(1)] **Always disclose your affiliation to Best Buy** when talking about topics related to your job . . . [(2)] **Make it clear it’s YOUR opinion** that is being expressed, not necessarily Best Buy’s official point of view on the matter. . . [(3)] **Protect yourself, our customers and the company** by never disclosing personal information, customer data or proprietary company secrets. . . [and (4)] **Act ethically and responsibly at all times**, embodying the very best of our company values. Despite these ethical guidelines, we occasionally encounter situations where an employee shares more than is appropriate while using the social media du jour. For example, a customer recently vented her frustration on one of our vendor’s tech support websites, explaining in detail how the television manufactured by Vendor X did not operate properly. Unfortunately, the post also included this phrase: “I am a Best Buy employee and should have known better!”¹⁴

⁹ 16 C.F.R. § 255.5 is at <http://op.bna.com/pl.nsf/r?Open=byul-8kmkls>.

¹⁰ The FAQs are at <http://business.ftc.gov/documents/bus71-ftcs-revised-endorsement-guideswhat-people-are-asking.pdf>.

¹¹ The WOMMA Guide to Disclosure in Social Media Marketing is at <http://womma.org/ethics/disclosure/>.

¹² *In the Matter of Reverb Communications, Inc.*, FTC File No. 092 3199, Nov. 26, 2010, is at <http://www.ftc.gov/os/caselist/0923199/index.shtm>; *In the Matter of Legacy Learning Systems, Inc.*, FTC File No. 102 3055, June 10, 2011, is at <http://www.ftc.gov/os/caselist/1023055/index.shtm>; *Closing Letter, AnnTaylor Stores Corporation*, FTC File No. 102-3147, April 20, 2010 is at <http://www.ftc.gov/os/closings/100420anntaylorclosingletter.pdf>.

¹³ See FTC statement on Consumer Privacy and Protection in the Mobile Marketplace before the Senate Committee on Commerce, Science, and Transportation, at <http://www.ftc.gov/os/testimony/110519mobilemarketplace.pdf>

¹⁴ The blog post is at <http://www.kathleenedmond.com/2011/07/15/is-she-a-customer-or-an-employee/>.