Texas Wesleyan Law Review

Volume 18 | Issue 4 Article 7

7-1-2012

Drafting and Implementing an Effective Social Media Policy

Susan C. Hudson

Karla K. Roberts (Camp)

DRAFTING AND IMPLEMENTING AN EFFECTIVE SOCIAL MEDIA POLICY

By: Susan C. Hudson & Karla K. Roberts (Camp)[1]

TABLE OF CONTENTS

I. THE EMPLOYER'S NEED FOR A SOCIAL MEDIA POLICY

Social media is everywhere and used in many business and personal situations. There is no indication that social media use is declining; rather, social media use is constantly expanding into new realms and

1. About the Authors: Susan C. Hudson is Corporate Counsel for Pier 1 Imports where her practice focuses on labor and employment matters as well as oversight of an active litigation docket. Ms. Hudson obtained her Juris Doctorate from Texas Wesleyan University School of Law. Karla K. Roberts (Camp) worked as Corporate Counsel for Pier I Imports with a generalist practice in the areas of compliance and real estate. Ms. Camp received her Juris Doctorate from SMU Dedman School of Law. The Authors have prepared this Article in their individual capacities and not on behalf of their employers.

DOI: https://doi.org/10.37419/TWLR.V18.I4.6
Published by Texas A&M Law Scholarship, 2022

taking on new forms.[2] Social media launches political campaigns, international pop stars, and new businesses to heightened levels of success or failure with just a few mouse clicks. Because social media information has the ability to spread rapidly, not addressing social media or hoping it will not affect the employer's business is a dangerous practice.

Currently, few employers have a Social Media Policy ("Policy").[3] By not having a Policy, the employer and its business are left vulnerable to the whims of its employees' social media actions and cannot guide employees toward using social media to protect and further the employer's business purpose. A Policy's existence makes the employer proactive rather than reactive. Further, establishing a Policy provides employees with clear expectations about when social media can be used, for what purposes, and what level of privacy an employee should expect regarding personal use. Finally, the employer needs a Policy to promote consistent enforcement among all employees. Inconsistent actions by supervisors for similar employee actions could open the employer up to potential employment discrimination lawsuits.

Once the employer understands that it needs a Policy, the next step is deciding what type to implement. The employer must create a Policy that furthers the employer's business purposes. Regardless of whether the employer decides to ban social media or freely allow its use, the employer should always spell it out in a Policy that defines the parameters of social media use. However, before the employer establishes a Policy it should conduct a cost-benefit analysis of social media uses and benefits for the employer versus the cost and resources required to enforce such a Policy. The employer should consider the Policy's monitoring and enforcement costs and the employee productivity costs depending on the level of allowed social media use. Taking into account these considerations, this Article will instruct an employer or employer's counsel on how to best draft an effective Policy that will meet all of the employer's objectives.[4]

2. *See* Steve Myers, *Americans Spend Just a Fraction of Online Time with News Compared to Social Media*, POYNTER (Sept. 12, 2011), http://www.poynter.org/latest-news/mediawire/145736/americans-spend-just-a-fraction-of-online-time-with-news-compared-to-social-media/ (citing *State of the Media: Neilson Social Media Report Q3 2011*, NIELSEN, http://blog.nielsen.com/nielsenwire/social/ (last visited Feb. 14, 2012)) (stating that 22.5% of the time spent on the internet is devoted to social media).

3. Samuel Axon, *Most Companies Don't Have a Social Media Policy*, MASHABLE BUSINESS (Feb. 3, 2010), http://mashable.com/2010/02/03/social-networking-policy/ (noting that only 29% of businesses have social media policies).

4. This Article is intended to provide general information regarding the development of a social media policy. It should not be construed as legal advice or a legal opinion on any specific facts or situations.

https://scholarship.law.tamu.edu/txwes-lr/vol18/iss4/7
DOI: 10.37419/TWLR.V18.I4.6

II. COMPONENTS FOR AN EFFECTIVE SOCIAL MEDIA POLICY

A. *Define "Social Media"*

Defining "social media" for purposes of developing the employer's Policy is the first step in drafting the Policy. In this Article, "social media" and "social networking" are used synonymously even though we acknowledge a slight difference between the two—"social media" being the means by which to broadcast communications and "social networking" being a functional tool for sharing information.[5] Although defining "social media" sounds simple, it is actually very difficult. To date, no standard definition exists because the forums and applications change so rapidly. Though there is no standard definition, it is generally agreed that social media is a form of electronic communication that allows user-generated interaction between the media's creator and the user.[6] Some well-known examples include Facebook, Twitter, Linked-In, YouTube, and blogs. Thousands of other lesser-known platforms exist.[7] For instance, have you heard of the YourBuzz application?[8] It is an American Express application used to promote buzz about businesses and to consolidate and track customer reviews.[9] The Policy needs to cover the YourBuzz application and all other social media platforms, even if the employer has never heard of them!

Because of social media's amorphous nature and the infinite platform types, a broad and general definition of social media is preferable for the Policy. If the Policy's definition is too specific, the employer will have to update its Policy at the same pace as new social media forms are being developed—good luck with that. Typically, social media is defined by type of social media; therefore, it might be preferable for the employer to define it in the same way.[10] A Policy, which includes an illustrative list of social media platforms to define

5. Lon S. Cohen, *Is There a Difference Between Social Networking and Social Media?*, THE COHENSIDE (Mar. 3, 2009), http://cohenside.blogspot.com/2009/03/is-there-difference-between-social.html.

6. *See Social Media*, MERRIAM-WEBSTER, http://www.merriam-webster.com/dictionary/social%20media (last visited Feb. 14, 2012).

7. *See id.*

8. *Get the Buzz on Your Business*, YOURBUZZ, http://www.yourbuzz.com (last visited Feb. 14, 2012).

9. *Id.*

10. *See* SP Social Media Marketing, *Social Media Expanded Definition*, FACEBOOK, (July 3, 2011), http://www.facebook.com/note.php?note_id=136127186468030 (defines social media as "media [that] can take many different forms, including Internet forums, message boards, weblogs, wikis, podcasts, wall-postings, email, instant messaging, music-sharing, group creation and voice over IP, to name a few. Examples of social media applications are Google (reference, social networking), Wikipedia (reference), MySpace (social networking), Facebook (social networking), Last.fm (personal music), YouTube (social networking and video sharing), Second Life (virtual reality), and Flickr (photo sharing)").

social media, should make it clear that the list is non-exclusive as to the types of social media covered by the Policy.

It is also important to differentiate between employer-run social media and personal social media. "Employer-run" social media is exactly what it sounds like—social media that is sponsored by the employer to help promote the employer and its business. Examples of employer-run social media include: a company iPhone application; a Facebook page where consumers can post about products and services they have used; or a Twitter page where employees can tweet about new promotional events or exclusive discounts.[11] In all cases, employer-run social media will be developed and maintained by the employer's authorized employees. In contrast, "personal social media" is any social media not sponsored by the employer. It can include an employee's personal blog, Linked-In account, Facebook page, or any other social media platform not employer-controlled. This Article focuses on an effective Social Media Policy as it relates to personal social media because it is harder to define and manage than employer-run social media, and therefore, creates more employment-related issues.

B. *Define Standards of Employee Conduct*

After defining social media, the employer must define the type of employee conduct allowed and prohibited while using personal social media. Similar to social media's definition, the scope of conduct should be general so that the Policy will cover a wide range of employees' actions without requiring the employer to predict employees' future actions. Defining prohibited conduct too specifically can limit the Policy's effectiveness because the employee can argue that the Policy did not cover the conduct. The employer can keep the "employee conduct" definition broad by requiring employees to simply act ethically or mandating that employees exercise good judgment while using social media.[12] These standards of conduct can encompass an array of employee actions that cannot be foreseen when the Policy is created.[13] To define ethical conduct under the Policy, defer to any existing code

11. *See* Walmart, *Walmart Local Ad*, FACEBOOK, http://apps.facebook.com/walmartfb_ad_prod/ (last visited Feb. 16, 2012) (posting on-line coupons for consumers); *see also @Dell*, TWITTER, http://twitter.com/#!/DELL (last visited Feb. 16, 2012) (discussions between customers and employees about new products and services).

12. *See Best Buy Social Media Policy*, BEST BUY, http://forums.bestbuy.com/t5/Welcome-News/Best-Buy-Social-Media-Policy/td-p/20492 (last modified Apr. 13, 2011) (standard of conduct for employees is to "act responsibly and ethically").

13. *See id. See generally* CISCO, CISCO SOCIAL MEDIA POLICY, GUIDELINES AND FAQs, (2011), *available at* http://www.scribd.com/doc/33461366/Cisco-Social-Media-Policy-Guidelines-and-FAQs.

of conduct if such a code exists.[14] Practically, the employer needs all of its policies aligned, with ethical conduct meaning the same thing throughout the employer's policies. Addressing ethical issues specific to social media is acceptable as long as the employer notes that it is either in addition to the existing code of conduct, or to the extent a contradiction exists, it should be noted that the situation applies exclusively to social media so as to avoid contradicting policies which create ambiguity.[15] Once the Policy defines the standard of conduct, the Policy should reiterate that the same ethical conduct standard applies to all interactions, whether the conduct is verbal, written, or over social media.[16] No extra layer of protection exists for the employee just because the employee is using social media.[17] The employee's code of conduct should be subject to the employee's Section 7 rights under the National Labor Relations Act ("NLRA") and state off-duty conduct statutes discussed below.

Additionally, the employer may want to provide concrete examples of non-ethical conduct to guide its employees. This is an effective way to show employees what type of conduct is prohibited, as long as the Policy explicitly states that the list is only illustrative and is not intended to be exclusive.[18] The employer should diligently review recent case law and statutes and update the Policy accordingly to ensure that the Policy's examples are still disallowable as social media law develops.[19] Otherwise, the Policy could be found to be illegal on its face if it prohibits conduct that has been deemed legal.[20]

C. *Define Who Has Authority to Speak on the Employer's Behalf*

In every Policy, the employer should define who has express authority to speak on its behalf and in what context.[21] To protect the employer from potential liability, the Policy should state that no

14. *See Global Social Media Policy*, DELL (Aug. 15, 2011), http://content.dell.com/us/en/corp/d/corp-comm/social-media-policy.aspx (social media policy applies the same basic principles and rules contained in Dell's Code of Business Conduct).

15. *See* MATT LEE-ASHLEY, DEP'T OF INTERIOR, SOCIAL MEDIA POLICY (2010), *available at* http://www.doi.gov/notices/Social-Media-Policy.cfm (explaining when the Federal Advisory Committee Act is and is not subject to the Social Media Policy).

16. *See IBM Social Computing Guidelines*, IBM, http://www.ibm.com/blogs/zz/en/guidelines.html (last visited Feb. 20, 2012).

17. *See id.*

18. LOYOLA MARYMOUNT UNIV., SOCIAL MEDIA POLICY (2012), *available at* http://www.lmu.edu/Assets/Student+Affairs+Division/Judicial+Affairs/Social+Media+Policy.pdf (providing a non-exclusive list of social media misuse).

19. *See* Cmty. Hosps. of Cent. Cal., 335 N.L.R.B. 1318, 1320–22 (2001).

20. *Id.*

21. *See VUMC Social Media Policy*, VAND. U. MED. CENTER, http://www.mc.vanderbilt.edu/root/vumc.php?site=socialmediatoolkit&doc=26923 (last updated Jan. 25, 2010) (stating that only institutional representation via online social media platforms can only be initiated and authorized through the efforts of the VUMC. There can be no official VUMC sites unless they are developed or authorized by the VUMC).

employee has authority to speak on the employer's behalf on personal social media forums unless the employer expressly gives that authority.[22] Also, the Policy should explain the distinction between express authority given to employees to use employer-run social media and personal social media.[23] Generally, the express authority given to an employee to speak on the employer's behalf on employer-run social media does not extend to the employee's personal social media platforms.[24] The employer should clearly state whether the authority to represent the employer extends, or does not extend, to personal use of social media.[25] In order to protect against legal risks, however, the Policy should require that all employees use a disclaimer when identifying or affiliating with the employer in any way while using any social media platform, whether personal or employer-run.[26] This disclaimer is critical because it informs the audience reading the posted material that the statements are made in the author's individual capacity and express that individual's opinions and beliefs, not those of the employer.[27] To provide guidance, the Policy should contain a sample disclaimer that employees can use when discussing the employer or its products or services over the employee's personal social media.[28] The disclaimer should state that the individual is acting in his or her own capacity and not on the employer's behalf and that the individual is personally responsible for statements made over social media.[29] The employee should clearly and conspicuously post the disclaimer on the social media platform.

A disclaimer will work in most situations to protect against legal risk, but some situations may arise that the employer might not be able to disclaim away. For every employer, there are key employees who are presumed to have authority to represent the employer, such as the CEO, COO, or the employer's other public figures. Typically, key employees are thought to have authority to speak on the employer's behalf even if the employer did not provide express authority. For instance, the CEOs of Thompson Reuter, Zappos, and Royal Caribbean International maintain personal blogs where they discuss busi-

22. *See* Susan M. Heathfield, *Blogging and Social Media Policy Sample*, ABOUT.COM, http://humanresources.about.com/od/policysamplesb/a/blogging_policy.htm (last visited Feb. 27, 2012) (requiring permission before speaking on behalf of the company).

23. *See id.*

24. *See id.*

25. *See id.* (noting that policy guidelines only apply to work-related sites and issues).

26. *See Social Media Guidelines*, INTEL, http://www.intel.com/content/www/us/en/legal/intel-social-media-guidelines.html (last visited Feb. 27, 2012).

27. *Id.*

28. *Id.* (stating that if employees publish to a website outside of the company that they use a disclaimer such as: "The postings on this site are my own and don't necessarily represent Intel's positions, strategies, or opinions.").

29. *See* Heathfield, *supra* note 22.

ness developments and issues that arise within their respective companies.[30] Following the Haiti earthquake, Royal Caribbean's CEO blogged that Royal Caribbean decided to continue operating cruise ships after the Haiti earthquake with the Haitian citizens' support; viewers of the blog correctly assumed that he had the authority and knowledge to discuss these company issues.[31] This type of blogging can be a positive tool for communication between companies and their customers, but if misinformation is contained in a key employee's blog, the employer will have a hard time avoiding liability for false or misleading statements made by such key employees. For these situations, the employer needs to train key employees with apparent authority on personal social media's proper use because a disclaimer will most likely be insufficient to avoid or minimize liability.

D. *Define the Scope of Personal Social Media Use During Working Hours*

The Policy needs to define the scope of personal social media use allowed during working hours as accurately as possible. The scope should reflect the entity's culture, the employer's goals, and the level of use that the employer wants in the workplace. These factors are important because in a dispute the court will look to the "operational realities of the workplace" to determine if the Policy truly echoes the scope of personal social media use occurring at the workplace.[32] If the Policy and the employer's business practices do not match, the court might hold that the Policy is not valid because it has been nullified by the employer's inconsistent practices.[33] The employer can define the scope of personal use over social media however it wants subject to Section 7 rights under the NLRA and state off-duty conduct statutes discussed later in the Article, although typically the scope of use is structured in one of four ways: (1) completely bans all personal use of social media during working hours; (2) allows all personal use of social media during working hours; (3) restricts personal use to certain times and places during working hours; or (4) allows for reasonable personal social media use.

30. Rex Hammock, *Chief Executive Magazine Spurs a Rexblog Sally Fields Moment*, REXBLOG (Oct. 2, 2011), http://www.rexblog.com/2011/10/02/23639 (listing the personal blogs of Thompson Reuter, Zappos, and Royal Caribbean).

31. *See* Adam Goldstein & John Weis, *Earthquake in Haiti*, SEA VIEWS (Jan. 13, 2010), http://www.answeritroyally.com/blog/?cat=174&paged=3.

32. *See* City of Ontario v. Quon, 130 S. Ct. 2619, 2628 (2010) (discussing "operational realities of the workplace" in the context of searching an employee's text messages).

33. *See id.* at 2630 (noting that an employer's "clearly communicated" policy will shape an employee's expectations of privacy).

- **Option 1**: An employer has the right to ban all personal use of social media during working hours.[34] If an employer elects to do so, then the employer must make it unequivocally clear that absolutely no use is allowed and strictly enforce the Policy. The employer should specify that all equipment, including personal devices, used to access personal social media platforms during working hours are included under the Policy. Because the Policy is only as good as its enforcement, the employer must strictly monitor its employees' personal social media use at work if the employer wants to enforce the Policy in the future.[35] The difficulty with this option is that the employer must prove to the court that the operational realities of the workplace are such that employees do not use personal social media at work.[36] Thus, the employer should implement and maintain a strict monitoring program of its employees' personal use during work hours so that it can prove that the Policy is operative at the time of an employee violation. Practically speaking, almost all employers have moved away from this option because of the cost and time associated with implementing and monitoring use.
- **Option 2**: On the opposite end of the spectrum, the employer can allow employees to freely use personal social media during working hours. By encouraging personal social media use, the employer will potentially have the benefit of increased business exposure through its employees, and the employer will not have to use time and resources implementing a monitoring system.[37] The employer, however, might also see a decrease in employee productivity and may be exposed to potential liability if the employee posts illegal or incorrect information during working hours. To avoid employer liability, the employer will need to ensure that every employee is using a disclaimer and that all employees are

34. *See, e.g.*, Ron Callari, *Top Five Social Network Bans in the US*, INVENTORSPOT, http://inventorspot.com/articles/top_five_social_networks_bans_us_31137 (last visited Feb. 19, 2012) (illustrating entities that still ban social media); Austin Carr, *Facebook Still Banned at Goldman Sachs, $450 Million Investment Be Damned*, FAST COMPANY (Jan. 5, 2011), http://www.fastcompany.com/1714459/despite-450-million-investment-facebook-still-banned-at-goldman-sachs.

35. *See* Timothy A. Carney, *Employee Privacy and Technology – How Much Snooping Can Employers Do?*, GABLEGOTWALS EMPLOYMENT LAW PRACTICE (Apr. 20, 2011), http://ggemploymentlawupdate.com/2011/04/20/employee-privacy-and-technology-how-much-snooping-can-employers-do/ ("[A]n employer must be prepared to make a commitment to enforce its policy fairly and consistently to minimize the risk that it will be faced with allegations of discriminatory enforcement, that the policy was 'waived' by the lack of enforcement, or other legal or ethical challenges.").

36. *See Quon*, 130 S. Ct. at 2628 (noting that the "operational realities of the workplace" must be considered in evaluating an employee's privacy rights).

37. *See* Susan Rush, *How Zappos Makes Social Media a Part of Its Company Culture*, SMARTBLOG ON SOC. MEDIA (Jan. 10, 2011), http://smartblogs.com/socialmedia/2011/01/10/how-zappos-makes-social-media-a-part-of-its-company-culture (showing how policy at Zappos encourages use of social media).

properly trained on what is acceptable to post. Also, it will be difficult for the employer to discipline employees for loss of productivity due to personal use of social media during working hours or for behavior over personal social media if a serious violation occurs. Companies that adopt this option should conduct a cost-benefit analysis to ensure that the benefits of personal social media use outweigh the employer's potential liability.

- **Option 3**: The third option is to restrict the personal use of social media during working hours to specific times and places. Many employers have taken this approach because it recognizes the operational realities of the workplace. This approach acknowledges and recognizes that most employees access their personal social media accounts during working hours but limits the use so that it does not affect the employee's work performance. Under this option, the Policy should specify the time(s) and place(s) that employees are allowed to access and use social media.[38] For instance, the employer might allow access during meal or rest periods only.[39] Another example would be for the Policy to allow employees to use social media at all times except during customer interactions or while in the customer's view.[40] As with Option 1, the employer must be specific in the time(s) and place(s) when employees can access and use social media and strictly enforce these restrictions. For example, if the employer states that an employee can only access and use social media during breaks and the employee posts on Facebook during working hours, then the employer must enforce the Policy accordingly. Even though the employee's posted statements may not be harmful to the employer or its employees, the employer must address all prohibited postings equally. By enforcing every violation of the Policy, employees will not be able to argue that the employer is being discriminatory in its Policy enforcement based on whether the employer approves or disapproves of the statements contained in the social media posting. Failing to strictly enforce the Policy as to all employees and all violations may render it ineffective when the employer attempts to enforce it against one employee in one specific situation.
- **Option 4**: The final option is to allow for "reasonable use" of personal social media during working hours.[41] Under this option, the employer would allow employees to use personal social media at

38. *See, e.g.*, UNIV. OF WASH. SCH. OF NURSING – SEATTLE CAMPUS, SOCIAL NETWORKING POLICY AND GUIDELINES, (2011), *available at* http://nursing.uw.edu/sites/default/files/files/SoN-Social-Networking-Policy.pdf.

39. *See id.*

40. *See id.* (prohibiting social media use "while performing direct patient care activities or in unit work areas").

41. *See, e.g.*, COCA-COLA CO., ONLINE SOCIAL MEDIA PRINCIPLES (2009), *available at* http://www.viralblog.com/wp-content/uploads/2010/01/TCCC-Online-Social-Media-Principles-12-2009.pdf.

any time and at any place as long as it does not interfere with job performance or conflict with the employer's interests.[42] The employer would need to evaluate each instance on a case-by-case basis because no universal standard can be applied to every employee. The employer would have to evaluate the specific employee's position, the reasonableness of the use based on the employee's position, and how the employee's personal social media use affected performance. Because this option is the most subjective, the employer must extensively document the violation and the decision made with regards to such violation to show the employer's rationale for making its disciplinary decision. This option is preferable if the employer cannot monitor its employees to the extent needed to strictly enforce the Policy and wants more Policy enforcement flexibility. This method, however, requires the employer to provide additional training for the employees implementing the Policy. The employer will have to use extra resources training employees on how to determine what is "reasonable" under the Policy to avoid liability for wrongful actions taken on the employer's behalf.

E. *Prohibit Harassment and Discrimination*

By law, all employees have a right to work in an environment free of discrimination, which includes freedom from any form of employee harassment based on sex, religion, race, color, age, disability, national origin, sexual orientation, or any other form of discrimination or harassment prohibited by law.[43] The same anti-harassment and anti-discrimination standards in the workplace apply to social media communications that affect the employee's work environment.[44] Therefore, the Policy should include a provision that prohibits harassment and discrimination through social media when such conduct creates a hostile working environment. Also, the Policy should state that an employee's use of personal social media when related to the workplace is subject to the employer's anti-harassment and anti-discrimination policies.

These anti-online harassment and discrimination provisions in the Policy are important because of a surge in online harassment claims by employees for which the employer could potentially be vicariously lia-

42. *See id.*

43. 42 U.S.C. § 2000e-2(a) (2006).

44. U.S. Equal Emp't Opportunity Comm'n, Press Release, *Fry's Electronics Sued for Sexual Harassment and Retaliation*, (Sept. 29, 2010), *available at* http://www.eeoc.gov/eeoc/newsroom/release/9-29-10e.cfm ("[W]hile technology can put a new spin on how harassment manifests, the responsibility of employers to take harassment seriously is not new . . . text messages, instant messaging, and social networking certainly contribute to the blurring of formal lines of communication. However, the law holds employers liable for the actions of their supervisors and managers, so training them to prevent and redress harassment, no matter what the medium, is critical.").

ble.[45] Employees are increasingly harassing co-workers through electronic means rather than making comments around the office or in meetings. Even though the harassment is not as overt to the employer, the harassing conduct still adversely affects the employee's job or creates a hostile work environment for the harassed employee.[46] Most states have responded to this rise in online harassment by amending their harassment, stalking, and bullying laws to include online communications.[47] These anti-online harassment statutes vary by state with regards to prohibited conduct, employer's duty to stop harassment, and punishment, but all acknowledge the need to prohibit online harassment. For example, in 2009, Texas amended the Texas Penal Code to prohibit sending an electronic communication with the intent to harm or defraud any person, punishable as a third-degree felony offense.[48] In Delaware, the law goes further and prohibits any electronic communication that the person knows is "likely" to cause annoyance or alarm.[49] Because of the varying state laws, the employer should research state online harassment laws to make sure the Policy conforms to those standards promulgated in state(s) in which the employer conducts business.

The employer should be concerned with any employee's personal use of social media during working hours and off-duty that rise to the level of harassment or discrimination because the employer can be held vicariously liable under certain situations. In *Blakey v. Continental Airlines, Inc.*, the New Jersey Supreme Court held that the employer may be directly liable if the employer does not remedy employee harassment of a co-worker when the employer is put on notice of the harassment and the conduct is sufficiently connected to the workplace.[50] In this case, the employee filed sexual discrimination and retaliation complaints with the employer for alleged violations of Title VII of the Civil Rights Act; however, the employer made no efforts to stop the harassing employees from posting such messages after being put on notice of the conduct.[51] Also, the Court found that the conduct was sufficiently connected to the workplace because the

45. *See* Kiri Blakeley, *The 'New' Sexual Harassment*, FORBES.COM (Aug. 6, 2009), http://www.forbes.com/2009/08/06/sexual-harassment-office-forbes-woman-leadership-affairs.html ("Much of the problem is that newer technology–e-mail, IM, texting or posting on social-networking sites–makes it much easier for comments to be misconstrued on many levels.").

46. *Id.*

47. *State Cyberstalking, Cyberharassment and Cyberbullying Laws*, NAT'L CONF. OF ST. LEGISLATURES, http://www.ncsl.org/default.aspx?tabid=13495 (last updated Jan. 26, 2011) (chart showing that most states have some form of online harassment statute).

48. Act of June 1, 2009, 81st Leg., R.S., ch. 911, 2009 Tex. Sess. Law Serv. 2361 (West) (current version at TEX. PENAL CODE ANN. § 33.07 (West 2009)).

49. DEL. CODE ANN. tit. 11, § 1311(a)(2) (2007).

50. *See* Blakey v. Cont'l Airlines, Inc., 751 A.2d 538, 552 (N.J. 2000).

51. *See id.* at 543, 550.

harassment was occurring in an online community board for co-workers to share ideas and information for which the employer provided and approved access through the employer's internal computer system.[52] In *Delfino v. Agilent Technologies, Inc.*, the issue of employer liability was brought up again.[53] The employer, however, was not held liable for its employee who was sending threatening e-mails using the employer's computer system because the employer had no notice of the employee's conduct.[54] The court held that the lone fact that e-mails were being sent through the employer's computer system was insufficient to show that the employer was aware of and liable for the harassing behavior.[55]

Given the case law, the Policy should state that action will be taken against any behavior that rises to the level of harassment or discrimination that is connected to the workplace. Also, conservative employers should immediately take corrective action against offending employees when such conduct is discovered. Finally, employers should avoid any conduct that would suggest the employer has promoted, sponsored, initiated, or ratified the offensive statements or harassing material. The employer's restrictions on an employee's harassing and discriminatory behavior is subject to the employee's right to exercise his or her Section 7 rights under the NLRA and state off-duty conduct statutes discussed below.

F. *Include Allowed Uses of Social Media*

Though an employer may like to regulate all personal use of social media that it does not like, the employer can open itself up to liability if it adopts an overly-broad Policy which inadvertently prohibits employee's lawful use of social media.[56] The employer is allowed to regulate personal use of social media subject to: (1) state off-duty conduct statutes; and (2) Section 7 rights conferred by the NLRA.

Some states have codified the employee's right to not be regulated when not at work by creating "off-duty conduct" statutes.[57] In states

52. *See id.* at 545, 556.

53. Delfino v. Agilent Techs. Inc., 52 Cal. Rptr. 3d. 376, 380–81 (Ct. App. 2006).

54. *Id.* at 399.

55. *See id.* at 395–96 (holding that the employer was not vicariously liable for employee's misconduct noting that "the employer 'may have set the stage for [its employee's] misconduct, but the script was entirely of [the employee's] own, independent invention'" (quoting Lisa M. v. Henry Mayo Newhall Mem'l Hosp., 48 Cal. Rptr. 2d 510, 519 (1995))).

56. *See generally* Memorandum from the Office of Gen. Counsel on Social Media Cases to all Reg'l Dirs., Officers-in-Charge, and Resident Officers, OM 11-74 (Aug. 18, 2011) [hereinafter *N.L.R.B. Memo*], *available at* http://www.scribd.com/doc/62691653/NLRB-Report-on-Social-Media-Cases-Aug-2011 (finding that employee handbook rules on social media were unlawful because they were overly broad).

57. Brian M. Flock, *Some State Laws Prying Into Employee's Online Activities*, ABA NAT'L SYMP. ON TECH. IN LAB. & EMP. L. (2010), *available at* http://www2.americanbar.org/calendar/ll04271-national-symposium/Documents/c_03.pdf (noting

with such statutes, employers are prohibited from disciplining employees or making employment decisions based on conduct that occurs when an employee is not at work, subject to certain exceptions. For instance, in New York, employers cannot discipline employees for engaging in lawful recreational activities, the legal use of consumable products, or lawful political activities while: (1) outside of working hours; (2) off of the employer's premises; and (3) without the use of the employer-owned equipment, unless the employee's conduct creates a material conflict of interest related to the employer's trade secrets, proprietary information, or other proprietary business interest.[58] The New York statute is very broad and leaves the employer little room to prohibit off-duty conduct. The Colorado off-duty conduct statute, however, limits the employer from terminating an employee for engaging in lawful activity during nonworking hours except under three circumstances, when: (1) the employee violates a "bona fide" occupational qualification; (2) the employee violates a restriction reasonably and rationally related to the employment activities and responsibilities of a particular employer or particular group of employees; or (3) to avoid the appearance of a conflict of interest with any responsibilities of the employer.[59] On the opposite end of the spectrum, Texas has no off-duty conduct statute.[60] The Texas Workforce Commission has reaffirmed in its Social Media Issues Guidelines that there is no law in Texas that would prevent an employer from subjecting an employee to disciplinary action for adverse online comments even if it is done off-duty or using the employee's personal equipment.[61] The guidelines further state that the employer has an unequivocal right to take corrective action against the employee if the employee affects the company's working relationships whether the employee is at work or not.[62] Because of the variances, the employer should research the law in the state where the employer operates to determine if there is an off-duty conduct statute, and if so, what type of conduct it allows the employer to regulate. The Policy should incorporate the state off-duty conduct laws and only prohibit conduct which state law allows to be prohibited. This can be accomplished by including a statement that the Policy applies except as superseded by state law.

In addition to off-duty conduct statutes, Section 7 of the NLRA grants employees the right to engage in concerted activities for the

off-duty statutes include but are not limited to California, Colorado, New York, and North Dakota).

58. N.Y. LAB. LAW § 201(d)(2)(a), (3)(a) (Consol. 2003).

59. COLO. REV. STAT. § 24-34-402.5(1)(a)–(b) (2011).

60. *See Social Media Issues*, TEX. WORKFORCE COMMISSION, http://www.twc.state.tx.us/news/efte/social_media_issues.html (last visited Feb. 16, 2012).

61. *See id.*

62. *See id.*

purpose of mutual aid and protection.[63] These rights apply to both public and private employers and both unionized and non-unionized employees.[64] Section 8 of the NLRA prohibits employers from interfering with or restricting an employee's exercise of Section 7 rights.[65] Given the unequivocal rights granted to employees under the NLRA, the Policy must include a statement that the Policy in no way intends to interfere with the employee's rights under Section 7 to engage in protected concerted activities, such as the employees' right to discuss their work environment.[66] To provide guidance on what is considered a "protected concerted activity," the Office of the General Counsel for the National Labor Relations Board ("NLRB") issued a Memorandum explaining what the NLRB considered "protected concerted activities" in the social media context and the lawfulness of the parameters of employers' social media policies with regard to such protected concerted activities.[67] According to the Memorandum, the following social media policies were unlawful because the policies created a "chilling effect" on the employee's right to engage in protected concerted activities under Section 7 of the NLRA:

- Policy was unlawful because it prohibited employees from making disparaging remarks about the employer, coworker, or its supervisors or engaging in "disrespectful conduct" without including limiting language that the policy did not apply to employees' right to discuss terms and conditions of employment.
- Policy was unlawful because it restricted employees from revealing personal information regarding coworkers, clients, or partners without the employer's consent because it restricted employees' rights to disclose wages and other terms and conditions of employment with coworkers.[68]
- Policy was unlawful because it prohibited employees from using employer's logos and photographs of employer's store, brand, or product without written authorization because it restricted employees' right to engage in protected concerted activities such as using the company's name or logo on picket signs or handbills in connection with a protest of the employees' terms and conditions of the employment.[69]
- Policy was unlawful because it prohibited any communication or posts that constitute embarrassment, harassment, or defamation of the employer or its employees, or from making statements that lacked truthfulness or that might damage the reputation or

63. National Labor Relations Act, 29 U.S.C. § 157 (2006).

64. *See* N.L.R.B. v. Wash. Aluminum Co., 370 U.S. 9, 13–15 (1962).

65. National Labor Relations Act, 29 U.S.C. § 158(a)(1) (2006).

66. *See N.L.R.B. Memo*, *supra* note 56 (concluding that the lack of limiting language made employer's policy too broad and unlawful).

67. *Id.*

68. Giant Eagle, Inc., Case 6-CA-37260, Advice Memorandum dated June 22, 2011, at 3–4, *available at* https://www.nlrb.gov/case/06-CA-037260 [hereinafter *Giant Eagle*].

69. *Id.*

goodwill of the employer because it could restrict employees' right to criticize labor policies or treatment of employees.[70]

- Policy was unlawful because it prohibited an employee from posting comments on a personal Facebook page regarding the poor job performance of a co-worker and other staffing and workload issues that restricted the employee's right to discuss work conditions.[71]
- Policy was unlawful because it prohibited an employee from calling a supervisor a "scumbag" over a personal Facebook page because the employee had a right to protest supervisory actions with other co-workers via a personal Facebook page when it did not interrupt the work of other employees, statement was made during nonworking time, and the derogatory remark was not accompanied by verbal or physical threats.[72]

Based on these examples, it is clear that the employer can only regulate conduct to the extent it does not infringe on the employee's right to engage in "protected concerted activities." As a result, the Policy should use the limiting language noted above and the guidance in the NLRB's Memorandum to ensure that a court will deem the Policy lawful.

On January 24, 2012, following the initial drafting and presentation of this Article, the Office of the General Counsel for the NLRB issued a second Memorandum (OM 12-31) which may modify the sufficiency of the policy drafting recommendations provided herein regarding the effectiveness of limiting language.[73] Overly broad prohibitions should be avoided, and the employer should consider the relationship of any prohibition to a business specific need.[74] The Authors urge caution and recommend a complete review of the second Memorandum prior to implementing any social media policy.

G. *Prohibit Use of Confidential Information and Copyrighted Material*

The Policy should protect the employer's confidential information from being disclosed to third parties over social media, subject to the

70. *See* Flagler Hospital, Case 12-CA-27031, Advice Memorandum dated May 10, 2011, at 3–4, *available at* https://www.nlrb.gov/case/12-CA-027031 [hereinafter *Flagler Hospital*].

71. *Id.*

72. Am. Med. Response of Conn., Case 34-CA-12576, Advice Memorandum dated Oct. 5, 2010, at 9–10, *available at* https://www.nlrb.gov/category/case-number/34-ca-012576.

73. *See generally* Memorandum from Anne Purcell, Associate General Counsel, to all Reg'l Dirs., Officers-in-Charge, and Resident Officers, OM 12-31 (Jan. 24, 2012), *available at* https://www.nlrb.gov/publications/operations-management-memos.

74. *Id.*

employee's Section 7 rights under the NLRA noted above.[75] The disclosure of confidential information can create business losses if sensitive information reaches competitors or can damage the employer's reputation if negative information is posted on social media sites.[76] To protect the employer's confidential information, the Policy should incorporate the employer's confidentiality policy, if one exists.[77] Also, the Policy should reiterate that employees are subject to the employer's confidentiality policy while discussing work matters. Employees should never discuss or post on any social media site confidential information, non-public information, proprietary information, or trade secrets regarding the business, such as sales data, plans, company finances, strategies, product launch information, nor discuss or post confidential information regarding others, such as customers, vendors, suppliers, and co-workers unless they are exercising their Section 7 rights.[78] Additionally, the Policy should provide department-specific examples of confidential information so that employees can recognize what confidential information means in their own position.[79] Even though the Policy should restrict disclosure of its confidential information to the fullest extent by law, the Policy must allow for the employees' use of confidential information if it is related to employee wages, terms, or other employment conditions to comply with Section 7 of the NLRA.[80] Practically, the employer can control unauthorized dissemination of confidential information by limiting the number of people who have access or exposure to the information and ensure that those employees are properly trained on what constitutes confidential information and how to protect it from unauthorized use.

The Policy should also prohibit the unauthorized use of copyrighted material such as logos, trademarks, symbols, services, and products or publishing employees' addresses, telephone/fax numbers, or e-mail addresses, subject to the employees' Section 7 rights under the

75. *N.L.R.B. Memo*, *supra* note 56 (finding that employer's policy prohibiting employees from revealing personal information overly broad as restricting employees' Section 7 rights).

76. *NHS Employees Blasted for Facebook Leaks*, IT PRO PORTAL (Oct. 31, 2011), http://www.itproportal.com/2011/10/31/nhs-employees-blasted-facebook-leaks/ (citing study that found 152 security breaches at NHS which included a number of violations about staff that were posting personal information and photos about patients on Facebook pages).

77. *See generally Social Media User Guidelines*, U.S. ARMY CORPS OF ENG'RS, JACKSONVILLE DIST., 2, http://www.saj.usace.army.mil/Documents/JaxDistrictSocialMediaUserGuidelines.pdf (last visited Feb. 16, 2012) (asks employees not to violate the U.S. Army policy, privacy, confidentiality, and legal guidelines in place).

78. *See*, PFIZER, SOCIAL MEDIA PLAYBOOK (2011), *available at* http://socialmediagovernance.com/policies.php (detailing exactly what constitutes material nonpublic information and personal information).

79. *See* IBM, *supra* note 16 (providing examples of what is and is not acceptable online communications and practices).

80. *Giant Eagle*, *supra* note 68, at 3–4 (citing Cintas Corp., 344 N.L.R.B. 943 (2005)).

NLRA.[81] The Policy also should state that the employer will pursue all legal remedies against any employee who discloses trade secrets.[82] To this end, the employer should monitor and actively pursue any employee who discloses trade secrets so that the employer can prove that it is taking measures to protect its trade secrets even if the confidential information was inadvertently disclosed.[83] The employer should also take immediate action to have copyrighted material removed from social media websites.[84] If the employer does not take action to remove the copyrighted or trade secret material, the employer could risk losing the material's protected status.[85]

H. *Define Employees' Expectation of Privacy*

In the Policy, the employer should clearly define the employees' expectation of privacy when using personal social media in three different situations: (1) when the employee posts information to the general public over social media either during working or non-working hours; (2) when the employee uses personal social media during working hours or from employer-owned equipment; and (3) when the employee uses personal social media outside of working hours using the employee's personal equipment.

Under the first situation, the Policy should state that the employee has no reasonable expectation of privacy regarding postings made accessible to the general public whether during working or non-working hours.[86] Courts have consistently held that employees do not have a right to privacy for information shared over social media because the inherent purpose of using social media is to share information with others and not to keep information private.[87] Additionally, the courts look to the privacy policies of the social media websites where the information is being posted.[88] The privacy policies typically state that

81. *See* PFIZER, *supra* note 78; Michelle Sherman, *Protecting Trade Secrets in a Post-WikiLeaks World*, SOCIAL MEDIA LAW BLOG (Apr. 6, 2011), http://www.socialmedialawupdate.com/2011/04/articles/intellectual-property/protecting-trade-secrets-in-a-postwikileaks-world/.

82. Sherman, *supra* note 81.

83. *Id.*; Talhiya Sheikh, *Trade Secrets and Employee Loyalty*, WORLD INTELL. PROP. ORG., http://www.wipo.int/export/sites/www/sme/en/documents/pdf/trade_secrets_employee_loyalty.pdf (last visited Feb. 20, 2012).

84. Sherman, *supra* note 81.

85. *Id.*

86. *See* Romano v. Steelcase Inc., 907 N.Y.S.2d 650, 656 (Sup. Ct. 2010) (relying on United States v. Lifshitz, 369 F.3d 173, 190 (2d Cir. 2004) to extend the principle that no user has a reasonable expectation of privacy the moment an e-mail reaches its recipient or entries on Facebook and MySpace).

87. *Id.* (noting that individuals' privacy concerns are not granted serious consideration when the user chooses to share the information herself).

88. *Id.* (noting that the MySpace and Facebook privacy policies both state that the forums are public spaces and that even if your privacy settings are restrictive, the sites cannot guarantee that unintended users will not access the user's pages and warns that the information may become publicly available).

the website has the right to collect and disclose information posted in a broad range of situations.[89] As such, it is acceptable for the employer to state in the Policy that the employee has no reasonable expectation of privacy when the employee posts information over social media to the general public.

The employee's right to privacy becomes trickier when the employee posts information over social media that is only intended for a specific audience, not the general public. Case law distinguishes between social media postings to the general public and postings to social media sites that are password protected or protected in other ways to shield unauthorized users from viewing the posted content.[90] Though the employee might still not have a valid claim for invasion of privacy, the employer may still be in violation of the Stored Communications Act ("SCA") or the Fourth Amendment, which applies only to public employers.[91] The SCA prohibits intentional unauthorized access to stored electronic information without the employee's consent.[92] Thus, the employer should be extremely cautious about accessing social media platforms for which the employer is not an "intended user" and should not use illegal or coercive means to gain access.[93] In *Pietrylo v. Hillstone Restaurant Group.*, the court held that the employee had no expectation of privacy when the employee and co-workers posted information on a password-protected MySpace website.[94] Even though the employees had no right of privacy, the court still found that the employer violated the SCA because the manager, an unintended user, coerced one of the employees who had access to the password protected site to disclose the account's log-in information so that the manager could access the employee's group page.[95] The court found that the employer violated the SCA and awarded punitive damages because the employer used coercive means to gain access and intentionally and repeatedly accessed the social me-

89. *See* McMillen v. Hummingbird Speedway, Inc., 2010 Pa. Dist. & Cnty. Dec. LEXIS 270, at *6–7 (C.P. Ct. Jefferson Cnty. 2010) (noting that "Facebook's operators may disclose information pursuant to subpoenas, court orders, or other civil or criminal requests if they have a good faith belief that the law requires them to respond." (citing *Data Use Policy*, FACEBOOK, http://www.facebook.com/policy.php (last updated Sept. 23, 2011))).

90. *See* Pietrylo v. Hillstone Rest. Grp., No. 06-5754, 2009 WL 3128420, at *3 (D.N.J. Sept. 25, 2009).

91. *See* U.S. CONST. amend. IV; Stored Communications Act, 18 U.S.C. § 2701(a)(1) (2006); *see also* Adam S. Forman, #Winning Strategies for Addressing Social Media in the Workplace, NAT'L RETAIL FED'N, COMMITTEE ON EMP. L. 16, 16 (2011) (noting that the Fourth Amendment applies to public employers).

92. § 2701(a)(1).

93. *See* § 2701(c)(2).

94. *See Pietrylo*, 2009 WL 3128420, at *1, *3.

95. *See id.* at *3 (employee testified that she only gave manager login information because she did not want to get in trouble and that she felt pressured. She also testified that she knew the other employees would be upset that she shared the information, which showed that the manager was not an intended user of the MySpace page).

dia platform without consent, even though it was clear from the site that it was for invited members only.[96] The court also found a violation of the SCA when an employee and intended user of a site voluntarily gave the employer and a third-party unintended site user access to a password protected social media platform.[97] In *Konop v. Hawaiian Arilines, Inc.*, the employer gained access to a password protected website when an authorized user of the website voluntarily gave the employer the password.[98] The court stated that the employer still violated the SCA because the employer gained access to the communication without being an "intended user" of that service.[99] Based on these holdings, to avoid violating the SCA, the employer needs to gain access through proper means and should be an intended user of the service.

Under the second situation, the Policy should include a statement regarding the employee's expectation of privacy related to personal use of social media that is not posted publicly but occurs during working hours or on company-owned equipment. In the landmark Supreme Court case, *City of Ontario v. Quon*, the Court declined to define the employee's right of privacy regarding electronic communications at the workplace.[100] The Court stated that it would be hesitant to decide what constitutes a reasonable expectation of privacy for the employee because developments in electronic communications and their use in the workplace are changing so rapidly that the Court would have a difficult time developing a standard for what is a reasonable expectation of privacy that could be applied in all situations.[101] The Court did, however, state that a well-crafted, broad, robust, and "clearly communicated" social media policy is a critical factor in determining the scope of the employee's right to privacy.[102] And, the Court asserted that the employer's Policy should reflect the "operational realities of the workplace."[103] Because the means and dynamics

96. *See id.* at *5 (finding that it was clear on the website that the group was private and only for invited members and the employee intentionally accessed the website knowing the employer was not authorized in violation of the SCA).

97. Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 880 (9th Cir. 2002) (suggesting that employer must be an intended user regardless of how employer gets the login information to the site).

98. *Id.*

99. *Id.* (defining "intended user" as one who uses the service and is duly authorized to do so).

100. *See* City of Ontario v. Quon, 130 S. Ct. 2619, 2629–30 (2010) (noting the difficulty in predicting an employee's expectation of privacy with rapid changes in communication and information sharing).

101. *Id.*

102. *See id.* at 2625, 2629 (noting that the employer's policy clearly stated that the employee has no reasonable expectation of privacy and that company-owned equipment of all types would be audited periodically).

103. *See id.* at 2628–29 (discussing how the employer's policy was almost overturned because there were statements made by the employer that the text message would not be audited and that these statements could have overturned the policy).

of communication and information sharing continue to evolve, the employer, and not the Court, would be in the best position to define appropriate communication and behavior because the employer has a better understanding of the "operational realities of the workplace."[104] Applying *Quon*, the employer's Policy should define the employee's expectation of privacy in exact detail with regards to employee's use of personal social media during working hours and on company-equipment and should accurately reflect the operational realities of the workplace.

Finally, under the third situation, the Policy needs to stipulate the employee's expectation of privacy when using personal social media outside of working hours on the employee's personal equipment. Of course, as previously discussed, the employee's expectation of privacy is subject to any applicable off-duty conduct statutes. Furthermore, the privacy expectation should be tied to the access and authorization principles, including the employer's limitation on accessing information for which it is not an intended user as well as the prohibition on using illegal or coercive means to access the employee's personal social media platforms. Typically, the employer needs to use stronger language in the Policy regarding the reasonable expectation of privacy when regulating off-duty conduct and must show a legitimate work related purpose for regulating such activity.[105] The employer will open itself up to liability if it conducts fishing expeditions into the employee's personal lives through social media use if no nexus exists between the employer policies and legitimate business interests.[106] In *Stengart v. Loving Care Agency, Inc.*, the court found that although the social media policy was ambiguous as to personal use, the employee had a reasonable expectation of privacy regarding her personal e-mails.[107] The Court noted that even if the employer had a robust policy, it still would not have excused the employer from reading through the employee's personal e-mails to her attorney because the employer had no need or basis to read the specific contents of personal, privileged, attorney-client communications that occurred off-duty.[108] The Court's admonishment of the employer in the *Stengart* case should warn employers that even if there is an enforceable policy which bans all personal use of social media, the employer should only regulate off-duty social media use to the extent needed to enforce the Policy and be mindful of employees' privacy rights not connected to a legitimate business purpose.

104. *See id.* at 2630 (noting that an employee's expectation of privacy is shaped by the employer's policy).

105. *See* Stengart v. Loving Care Agency, Inc., 990 A.2d 650 (N.J. 2010).

106. *Id.* at 658 (noting that a stronger social media policy which prohibited personal use from work computers would not have been determinative but would have given the employer a stronger argument for searching e-mails).

107. *Id.* at 659, 663.

108. *Id.*

Regardless of whether the employee has a valid expectation of privacy or not, the employer should still not act on any of the information obtained or discovered from social media postings until it follows all of the Policy's procedures. In many circumstances, the employer may be able to view the information posted over social media but may not be able to use such information in employment decisions. Please see the training and enforcement section below for an explanation on how to proceed with enforcing the Policy. To ensure consistency within the organization, the employer should incorporate its privacy policy by reference and ensure that the principles in both policies are aligned. If available, the employer should rely on internal resources such as the compliance, audit, or risk departments to help develop and tailor a privacy provision specifically for the Policy.

I. *Comply with Federal Trade Commission Guidelines*

In October 2009, the Federal Trade Commission ("FTC") revised its *Guides Concerning the Use of Endorsements and Testimonials in Advertising* ("Guidelines") to include rules for posting Internet reviews.[109] The FTC revised the Guidelines to protect consumers against deceptive trade practices occurring over the Internet.[110] As such, the Policy should explain to employees how to abide by the Guidelines when endorsing the employer's products or services in the social media context. Based on the revised Guidelines, the Policy should (1) define what constitutes an endorsement; (2) detail how to correctly post an endorsement about the employer or its business; and (3) describe how and when an employee is required to use a disclaimer.[111]

First, the employer should define what constitutes an endorsement. The Guidelines define an endorsement as *any* advertising message conveyed to a consumer that would appear from the consumer's perspective to express the personal views of the person conveying the message.[112] Because the FTC has such a broad definition of endorsement, the Policy should inform employees that any outward expression by the employee about the employer or its business that is posted on a website could be considered an advertising message.[113]

Second, the Policy should explain to employees the appropriate way to post an endorsement. The Guidelines mandate that endorsements contain truthful and substantiated opinions or experiences by the endorser and that the endorser must be a "bona fide user" of such prod-

109. FTC Guides Concerning the Use of Endorsements and Testimonials in Advertising, 16 C.F.R. § 255.5 (2011).

110. *Id.*

111. *See id.*

112. *Id.* § 255.0(b).

113. *Id.* See examples in Guidelines for further explanation.

uct at the time the endorsement was given.[114] Thus, the Policy should state that employees should only post honest experiences and opinions about the employer's products or its business that the employee actually uses at the time an endorsement is posted.[115]

Third, the Guidelines require that if there is a connection between the endorsement and the seller of the product that could "materially affect the weight and credibility of the endorsement," it must be fully disclosed.[116] Further, the Guidelines require that the disclosure be "clear and conspicuous."[117] Thus, the Policy should require that if the employee is endorsing the employer or its business, the employee must fully disclose the connection between him or herself and the employer.[118] The Policy should also mandate that the employee use a "clear and conspicuous" disclaimer.[119] The disclaimer does not need to be verbose; it simply needs to state that the employee is employed by the business the employee is endorsing. It appears that the same disclosure standards would apply if the employee was posting negative reviews about a competing business.

So, why should the employer care about unauthorized postings of employees on social networking sites? Because, the FTC has stated that both advertisers and endorsers face potential liability for statements made in the course of endorsements.[120] The Guidelines suggest that potential liability could flow back to the employer if the employee makes false representations about the employer's products or services even if the employer never authorized or approved the postings.[121] Though the Guidelines do not explicitly address the rules regarding the employer-employee relationship in this context, the list of examples in the Guidelines is not an exclusive list of every possible use of endorsements, and the advertiser-endorser relationship is similar to the employer-employee relationship.[122] Also, these Guidelines need to be included in the Policy because the FTC is actively enforcing these Guidelines as violations of the Federal Trade Commission Act, which could have serious consequences for the employer.[123] If the

114. *Id.* § 255.1(c).
115. *Id.*
116. *Id.* § 255.5.
117. *Id.*
118. *Id.*
119. *Id.* (describing standard for full disclosure as "clear and conspicuous." *See* Example 8 and 9).
120. *Id.* § 255.2.
121. *Id.* § 255.1. Example 5 provides an example of a skincare products advertiser who participates in a blog advertising service. *Id.* The advertiser would be liable for the blogger's endorsement claims even though the employer did not make the specified claims represented by the blogger. *Id.*
122. *Id.* § 255.0(a).
123. *In re* Legacy Learning Sys., Inc., File No. 1023055, at 2, 7 (Agreement Containing Consent Order, Mar. 15, 2011), *available at* http://ftc.gov/os/caselist/1023055/110315llsagree.pdf.

FTC Guidelines are not followed, the employer could be forced to monitor employees, submit monthly reports about its endorsers to ensure that the affiliates are not misrepresenting themselves as independent or ordinary customers, and pay significant fines for noncompliance depending on the seriousness of the violation and the extent of employer involvement.[124] The FTC Guidelines, however, suggest that guidance, training, and monitoring bloggers paid to promote products can protect the advertiser from liability.[125] Thus, the Policy should train employees on how to endorse the employer's products and services online by including the pertinent Guidelines.

J. *Incorporate All Other Applicable Employer Policies and Laws*

The Policy should contain a statement that incorporates and applies all of the employer's other applicable policies. Typical other policies that need to be included are the: (1) e-mail or electronic communications policy; (2) anti-harassment and anti-discrimination policy; (3) code of conduct or ethics; (4) fraternization policy; (5) privacy policy; (6) document retention policy; (7) Sarbanes-Oxley Act compliance policy; (8) HIPPA policy; (9) conflict of interest policy; and (10) other policies that might relate to social media.[126] Specifically, employers should check their document retention policy to ensure that it includes storing electronic information from social media activities and incorporates all company-owned equipment including cell phones and tablets.[127]

Additionally, to ensure compliance with the Sarbanes-Oxley Act compliance program, the employer should include a statement that financial information posted over social media must be constantly updated to reflect material changes in financial conditions and operations.[128] The Policy should prohibit employees from releasing financial information over their personal social media so that the employer can control the accuracy of the financial information released to the public.

The Policy should also require compliance with other relevant social media guidelines or laws for which the employer does not have a pol-

124. *Id.* at 4–6.

125. 16 C.F.R. § 255.5.

126. *See, e.g.*, *Social Medial Handbook*, VAND. U., http://web.vanderbilt.edu/resources/social-media-handbook/important-policies-social-media/ (last visited Feb. 18, 2012) (guiding employees to read the other policies related to social media and informs employees that those policies govern all social media use).

127. Michele Sherman, *Does Your Sarbanes-Oxley Act Compliance Program Reflect Your Social Media Presence?*, SOC. MEDIA L. BLOG (June 21, 2011), http://www.socialmedialawupdate.com/2011/06/articles/social-media/does-your-sarbanesoxley-act-compliance-program-reflect-your-social-media-presence/.

128. *Id.*

icy.[129] Even if the employer does not have a policy for a specific law that affects social media, the Policy should state that the employee must comply with all state and federal laws when using social media. As stated previously, even though ideally all policies should align, specific nuances of the employer's business sometimes makes it impossible. On specific occasions, there will be rules in the Policy that change another policy's guidelines, and vice versa. For instance, in the Department of Interior's Social Media Policy, the employer explains to its employees when the Federal Advisory Committee Act is and is not applicable to the Social Media Policy so the employees are clear on which standard to follow when using social media.[130] In this and similar cases, the Policy should clearly state that the Policy's specific rule does not modify or apply to other policies.[131]

K. *Include Instructions on How to Respond to Requests Made Through Social Media*

Assuming the Policy has not given employees authority to speak on the employer's behalf when using personal social media, the Policy should include a section on how to respond to questions or information requests by non-employees, consumers, competitors, investors, or others. First, the Policy should reiterate that employees are prohibited from responding to any questions about the employer and its business unless expressly authorized by the employer.[132] Second, the Policy should direct all employees to either not respond to the inquiries or respond by posting the contact information of the employee or department with authority to represent the employer.[133] The Policy should provide the authorized representative or department's contact information so that the employee can repost that information as the response. By following this approach, the employer will be able to better manage and control the information being disseminated over social media while still allowing employees to use social media to promote the employer and its business.

129. *Social Media Policy*, CONN. LIGHT & POWER, http://www.cl-p.com/SiteInfo/Social_Media_Policy/?MenuID=4294985952 (last visited Feb. 16, 2012).

130. LEE-ASHLEY, *supra* note 15.

131. *See, e.g., id.* (explaining when the Federal Advisory Committee Act is and is not subject to the Social Media Policy).

132. *See, e.g.*, VAND. U. MED. CENTER, *supra* note 21 (stating that institutional representation via online social media can only be initiated through VUMC and the authorized departments and directly appoints department leadership responsible for posting on these authorized sites).

133. *See id.* (directing employees to contact the News & Communications Department if someone from media or press contacts or responds to social media posts).

III. DEVELOP, MONITOR, AND ENFORCE THE POLICY

A. *Develop the Policy*

Drafting a Policy is only the first step in creating an effective Policy. The Policy needs to evolve as the employer's interaction with social media changes and as the law defines the employees' rights to interact over social media and of employers to regulate those interactions. Because the area is so amorphous and quickly changing, the Policy should include a provision that allows the employer to modify the Policy at any time in its sole discretion.[134] Also, the employer should evaluate the Policy's scope, the specificity by which it regulates employees' actions, and social media's role within the employer's business to determine how often to review and update the Policy. For instance, a Policy that only mandates employees comply with the general laws and regulations and bans use of social media during working hours will not need to be updated as often as a Policy that allows employees to use social media reasonably during working hours and mandates off-duty conduct. This is because the latter Policy regulates specific conduct and requires the employer to monitor the employee's use during working hours. In either case, the employer should periodically review the Policy and relevant laws to determine if the Policy needs to be updated.

Additionally, the employer should notify the employees when it has updated the Policy.[135] The employer can distribute the updated Policy to employees, require a signed acknowledgment that each employee has received and read the updated Policy, or can notify the employees through e-mail or a posting on the company's intranet that the Policy has been updated and that the employees should familiarize themselves with the updated Policy.[136] Each time the Policy is updated, the employer should document how the employees were notified and what was modified so that it can demonstrate that the employees have knowledge of the current Policy.

As part of the development process, the employer should train its employees on the Policy. The employer must ensure that employees understand what the Policy says and how it applies to their job. The most effective way to implement the Policy and protect the employer from liability is to train your employees accordingly. It is not enough to generally train your employees on social media use. The employer should have specific training with departments that interact with social

134. *See, e.g.*, *Social Media Policy*, WESTMED MED. GROUP, http://www.westmedgroup.com/social_media_policy.aspx (last visited Mar. 1, 2012).

135. *See* Steven C. Bennett, *Social Networking Policies: Best Practices for Companies*, METROPOLITAN CORP. COUNS. (Jan. 5, 2010), http://www.metrocorpcounsel.com/articles/12109/social-networking-policies-best-practices-companies (recommending that employers give, but not promise, notice of policy changes).

136. *See* WESTMED MED. GROUP, *supra* note 134.

media or are impacted by social media directly, such as the public relations/communications, marketing, human resources ("HR"), or investor relations departments. This training should focus on issues applicable to the relevant employees' respective jobs. After the initial training, the employer should conduct periodic re-training to update employees about Policy modifications.

To avoid liability, the employer should ensure the HR department is proficient with the Policy's rules. The HR department employees are typically tasked with making employment decisions about information found, inadvertently discovered, or reported by employees over social media. The employer should provide guidance, in the Policy and through the training, about how to use information obtained through social media once in the hands of the HR department. Generally, the trainings should provide the following information:

- *Emphasize consistency*: HR department must establish and use the same procedures when conducting all searches and use the information found over social media uniformly for all employees.[137]
- *Define who is authorized to conduct these searches*: HR department must designate a person who is not tasked with making employment decisions to conduct searches over social media. This will prevent the disclosure or unlawful information to the HR employee who will make the employment decision.[138]
- *Define proper way of accessing social media*: HR department should only access social media in the public domain and not an employee's protected personal social media websites without authorization or by illegal, coercive, or deceptive means.[139]
- *Define the searches that can be conducted*: HR department must define the scope of the allowable searches, whether all personal social media websites can be searched or just business/professional websites such as Monster or LinkedIn.[140]
- *Define what information cannot be used*: HR department should be trained on what information cannot be used to make employment decisions such as genetic information/medical history, credit information obtained without the employee's authorization, and all Title VII protected information.[141]

137. *See* Forman, *supra* note 91, at 28 (suggesting that employers modify current hiring processes to "include a defined process for how to evaluate an applicant's online presence").

138. *See id.* at 29 (suggesting that employers appoint a neutral, non-decision-maker person to filter protected status information).

139. *Id.*

140. *Id.* at 27.

141. Fair Credit Reporting Act, 15 U.S.C. § 1681k (1998) (prohibits an employer from using third-party to conduct background check without consent); Acquisition of Genetic Information, 29 C.F.R. § 1635.8 (2011) (prohibits conducting Internet searches in a way that will likely result in an employer/covered entity obtaining genetic information).

- *Document everything*: HR department should document all searches thoroughly including what information was found, how it did or did not use that information to make an employment-based decision, and what employment actions resulted.
- *Consult with the legal department*: The HR department should consult with the legal department before it takes any employment action based on information found over social media.

With the proper training, the employer should be able to benefit from the use of social media while protecting itself against liability.

B. *Monitor Personal Social Media Use*

One of the biggest issues surrounding social media is how to properly monitor personal social media use during working hours. The employer's right to monitor pivots on the employee's right to privacy in the workplace. Additionally, the employee's right to privacy about electronic communications is contingent on the employer's Policy. As such, the employer should only monitor communications for which the employee has no reasonable expectation of privacy, as determined by the Policy. As a practical note, the employer should conduct a cost-benefit analysis of the time and resources it wants to spend on a monitoring system compared to the potential risks of employees using personal social media during working hours. This is a fact-based analysis that will depend on the employer's business.

The law has emphasized that monitoring should be accomplished only for lawful purposes.[142] The employer cannot monitor the employee's personal social media information to conduct a fishing expedition or for personal curiosity. In the Fourth Circuit case of *Van Alstyne v. Electronic Scriptorium, Ltd.*, the court held that the company violated the Stored Communications Act when the company's president accessed the employee's personal e-mail account and read the employee's e-mails during working and non-working hours, while they were involved in adverse litigation, and even after the employee had left the company.[143] The court awarded punitive damages and attorney's fees even though the employee suffered no actual damages. This holding shows that the courts have little tolerance for using employer's monitoring system to access employee's personal social media without a work related purpose.

The Policy should notify employees that employers will monitor the personal use of social media during working hours, while using company-owned equipment, and under whatever context is appropriate for the specific employer. By including this provision, the employee's right of privacy is restricted to the Policy's terms and conditions. Some states mandate notification to employees of electronic monitor-

142. *See* City of Ontario v. Quon, 130 S. Ct. 2619, 2630–31 (2010) (discussing the lawful purposes for an employer's search of an employee's text messages).

143. Van Alstyne v. Elec. Scriptorium, Ltd., 560 F.3d 199, 201–02 (4th Cir. 2009).

ing.[144] The employer should check the state law where it operates to ensure compliance with the electronic monitoring statutes. Though the state might not require notification, the employer should consider including such a provision in the Policy to put employees on notice that their actions are being monitored. This will bar the employee from later claiming a reasonable expectation of privacy with respect to its electronic communications.

The employer's next step, after defining the scope of activity to be monitored, is to implement a monitoring system. This is critical because the employer must comply with the monitoring standard it establishes to prove the Policy is in full force and effect.[145] If the employer states that it will monitor all personal use, it needs to have the resources to maintain that monitoring standard. The employer should consider the resources it will use to monitor social media use before implementing a monitoring system. There are many ways for the employer to monitor employees' personal social media use such as:

- Google/Marketing Alerts;
- Annual Audits;
- Internal Surveillance System;
- Vendor/Third-Party Monitoring Service; and
- Self-Monitoring.

One advantage of implementing a self-monitoring system is that the employer can reduce its monitoring efforts by placing an affirmative duty on the employee to report violations. If the Policy uses this type of monitoring system, it should detail how the employee can report a Policy violation. Typically, the reporting mechanism will direct employees to notify their HR department representative, and the HR department will review the issue. The employer should rely on its audit or compliance department, if the employer has one, before it creates a monitoring system because one might already be in place for other privacy or confidentiality purposes.

Of course, the employer's monitoring of employee's off-duty conduct is another issue which is not fully contemplated by the *Quon* case. However, applying the various principles already discussed in this Article, clearly the employer can monitor social media for which it is an "authorized user." The employer should not use illegal or coercive means to monitor its employees. Additionally, the employer should monitor employees only for legitimate work related purposes. As previously discussed, the employer's right to monitor off-duty conduct is always subject to the off-duty conduct statutes and Section 7 rights of the NLRA. Typically the same principles apply to conduct

144. DEL. CODE ANN. tit. 19, § 705(b) (2005); CONN. GEN. STAT. ANN. § 31-48 (1958) (updates available at http://www.ncsl.org/default.aspx?tabid=13463).

145. *See Quon*, 130 S. Ct. at 2630–31 (noting that the employer had a clearly communicated policy and followed its policy in monitoring employee's text messages).

occurring on and off-duty, except that the monitoring of off-duty conduct should only be used when there is a strong, legitimate work related purpose and not for conducting fishing expeditions into employees' personal lives.

C. *Enforce the Policy*

The Policy must either create or incorporate disciplinary actions from other employment policies. The Policy's enforcement is extremely important because the courts will evaluate its validity based on equal enforcement.[146] As such, the employer should treat all activity, including non-activity, that is subject to the Policy equally. The employer should extensively document the activity, the actions taken, and provide detailed explanations on why certain actions were or were not taken.[147] Whenever the employer takes separate and distinct actions against employees for what appears to be similar violations, the employer should document the distinctions in the activity or circumstances to identify a valid reason for taking dissimilar actions.

The employer should treat a violation under the Policy as it treats all other company policy violations. There are numerous instances where the employer takes immediate action regarding negative Facebook postings, or other statements made over social media, that the employer would not have taken if the same statements were made during a meeting or in the break room. For instance, in the *NLRB v. Flagler* case, several nurses complained to their managers about a perpetually absent co-worker whose absence was causing them to take on a heavier workload and disrupting their work schedules.[148] One of the nurses, who ultimately posted her frustrations on Facebook, was terminated for expressing the exact same frustrations the other nurses had previously voiced to the manager.[149] Unequal treatment of similar statements and actions can create ambiguity about how the Policy is being enforced.

The employer also needs to take time to thoroughly investigate the alleged violation of the Policy. In some cases, derogatory statements made over social media may appear unprovoked and disparaging; however, the employer may find, through its investigation, that the violating employee has been subjected to severe discrimination or harassment by another employee made subject of the violating post. Illegal and improper decisions can be prevented if the employer investigates and works through the corrective action process, as it does with other employer policies, before taking any action against the employee.

146. *See id.* (discussing enforcement of the employer's monitoring policy).
147. Forman, *supra* note 91, at 29 (recommending that employers take steps to evaluate how the company responded to similarly situated employees).
148. *Flagler Hospital*, *supra* note 70, at 2.
149. *Id.*

Finally, before taking any action, the employer should consider whether an employee's postings over social media could be considered a report of wrongdoing under the federal or state whistleblower laws or anti-retaliation statutes. Numerous laws protect employees for reporting the employer's violations and illegal actions when the report is made internally or to a government agency. However, it is unclear whether a posting over social media will constitute a "report" under the various laws because there is no case law on the issue. Because there is no clear guidance, the employer should evaluate the employee's statements on a case-by-case basis and conduct a complete investigation to determine if the statement is protected under the whistleblower or anti-retaliation laws before enforcing the Policy against the employee.

IV. SUMMARY

In summary, establish a complete Social Media Policy tailored to the employer and use it. Adopt the Policy components stated in this Article and modify them to conform to the employer and its business. Because the area of social media is developing so quickly, check the laws frequently, use and rely on outside counsel to provide changes in the law, and update the Policy accordingly.