# Social Media in the Workplace – Potential Traps for Employers and Employees

**by Phil J. Antis, Jr.**
**and David V. Bryce**

**Gordon Arata Duck Lunch Seminar, 2012**

## TABLE OF CONTENTS

## I. Introduction

Social media is becoming an increasingly prevalent aspect of modern life. As of October 2012, Facebook is used by over 1 billion people, Linked-In has 175 million users, and Twitter has 140 million users. With its increasing spread, the impact of social media on the workplace is rapidly growing in importance. Already, social media is commonly used by employees to communicate with each other, and is used as a source of information about co-workers, supervisors, and companies' products and services.

In view the rise of social media, both in the workplace and outside of it, there is a growing need for employers to familiarize themselves with laws affecting their employees' use of social media, and an employer's ability to regulate and monitor that use. Currently, few employers maintain social media policies; but, as the use of social media continues to expand, many employers would be wise to consider implementing social media policies, and, those employers who already have such policies in place need to continually review them to ensure that they do not run afoul of rapidly evolving laws pertaining to social media.

This paper presents an overview of some of the issues that employers with social media policies, or considering them, need to be cognizant of and responsive to. While the paper is not intended to serve as a comprehensive guide to the laws affecting social media policies in the workplace, and consultation with an attorney is urged with respect to the review and implementation of such policies, it is hoped that the paper will familiarize employers with a sampling of some of the more important legal issues relating to social media policies in the workplace.

## II. Social Media and Hiring

Through social media, many people make a significant amount of personal information available over the Internet. Social media thus provides employers with the possibility of getting a more personal view of potential employees than might otherwise be possible. There are, however, many potential legal pitfalls that may arise if an employer uses social media to conduct background checks on prospective employees.

Most fundamentally, looking up the social media presence of job applicants or interviewees may implicate employment discrimination laws. For instance, federal and state laws generally bar any hiring decisions that are based on certain protected categories, including race, religion, age, gender, disability, and military status. By viewing a job applicant's Facebook page, an employer may discover that the applicant is a member of a protected class, knowledge the employer would not otherwise have during the application process.

For instance, an employer may receive a job application from "Mary Smith" that (properly) contains no information about Mary's race or whether Mary is disabled. If it decides to look up her Facebook page, the employer may discover that Mary is an African-American who is wheelchair bound. Upon learning Mary's race and disability status, if the employer elects not to offer Mary an interview, it faces liability for making an adverse hiring decision based on the knowledge it obtained from Mary's Facebook page that she is a member of a protected class.

In sum, because social media may reveal information about a person's membership in various protected classes, employers who use social media to conduct background checks on prospective employees face potential liability for using

information learned in the course of the "social media" background check in a manner that discriminates on the basis of race, color, religion, sex or national origin. The risks associated with using social media to review an applicant's background do not mean that an employer should entirely disregard a social media review of an applicant. Employers who conduct social media reviews, however, should do so in a manner designed to minimize exposure to discrimination claims. Some recommendations for limiting liability in connection with the use social media in the hiring process are presented below in § VIII.

## III. State Laws and Employer Social Media Policies

Developing a social media policy for use in the workplace requires sensitivity to numerous state and federal laws. A seemingly cautious or conservative social media policy may run afoul of various laws. This section of the paper discusses some state laws that an employer will want to bear in mind in crafting any social media policy. As noted, this paper does not include a discussion of all potentially applicable state and federal laws; therefore, any employer considering implementing a social media policy should consult with an attorney to ensure that the policy is consistent with all applicable state and federal laws.

### A. Off-Duty Conduct Laws

Employers with social media policies, or who may consider implementing social media policies, should be aware of what are commonly referred to as "off-duty conduct laws." These laws, present in some form in at least 29 states, prohibit employers from taking adverse employment actions based on an employee's otherwise lawful actions outside the workplace and off work-hours. With respect social media policies, it is

important to consider off-duty conduct statutes because disciplining an employee for an action learned about from social media that is protected by an off-duty conduct statute may subject an employer to liability.

These statutes vary in scope, but the most comprehensive off-duty conduct laws exist in California, New York, Colorado, North Carolina, and North Dakota.[1] For instance, pursuant to New York's statute, an employer cannot take an adverse employment action based on an employee legally using consumable products or legally participating in recreational activities outside of work hours, off of the employer's premises, and without use of the employer's equipment or other property.[2]

Texas does not have an off-duty conduct statute. According to the Texas Workforce Commission, it is not unlawful under Texas law for an employer to take an "action against an employee for off-duty conduct if such conduct has the effect of damaging company business or work relationships."[3] Louisiana does have an off-duty conduct statute, but it applies solely to tobacco use, providing that employers cannot make personnel decisions based on an employee's use of tobacco, so long as that use complies with applicable laws and any workplace policy regulating tobacco use.[4]

---

[1] *See, e.g.*, CAL. LAB. CODE § 96(K) (2004); N.Y. LAB. LAW § 201-D (2004); Colo. Rev. Stat. § 24-34-402.5 (2004); N.C. GEN. STAT. § 95-28.2 (2004); and N.D. CENT. CODE § 14-02/4-03 (2003).

[2] *See* N.Y. LAB. LAW § 201-D. Courts have applied a narrow definition to "recreational activity." For instance, it has been held that a romantic relationship is not a "recreational activity" that is entitled to protection under the law. *State v. Wal-Mart Stores*, 207 A.D.2d 150 (N.Y. App. Div. 3d Dep't 1995).

[3] *See Social Media Issues*, Tex. Workforce Commission, http://www.twc.state.tx.us/news/efte/social_media_issues.html (last visited Oct. 11, 2012). The Workforce Commission's guidelines do recognize that, as discussed below, an employee's actions may be protected under the NLRA. *See id.*

[4] *See* LA. REV. STAT. § 23.966 (2004

Employers' social media policies must be crafted to ensure that they are in compliance with applicable state off-duty conduct statutes. Employers should also be aware that certain states have statutes that protect employees for exercising their political beliefs, and that these statutes may include protections for certain social media activities, for instance, blogging.[5]

**B. Social Media Privacy Laws**

Employers should also be aware of increasing legislative activity surrounding issues of social media privacy. Social media privacy issues, in part, address whether an employer may require an employee to provide log-in information to his personal social media accounts.

In 2012, Maryland became the first state to prohibit employers from requiring employees or job applicants to disclose their personal social media log-in information.[6] The legislation was spurred by reports that the Maryland Department of Corrections asked job applicants to provide their Facebook usernames and passwords. Maryland's law, among other things, prohibits employers who do business in the state of Maryland from requesting a user name, password or any other means of accessing a personal account or service through an electronic communications device, including social media accounts.[7]

Maryland's passage of a social media privacy act appears to be the beginning of a trend. For instance, California adopted its own social media privacy law in September

---

[5] *See, e.g.*, CAL. LAB. CODE § 1101-02; N.Y. LAB. CODE § 201-d; and CONN. GEN. STAT. ANN. § 31-51q.

[6] Md. S.B. 433, signed into law May 2, 2012 and effective October 1, 2012.

[7] *See id.*

2012, enacting legislation that prohibits employers from demanding employees' and job applicants' personal email and social media log-in information.[8] As many as 15 other states are presently considering similar legislation, and legislation has been introduced in the United States Congress to bar employers from requiring any employee to provide its employer with access to the employee's personal social networking accounts.[9] As social media privacy laws are rapidly gaining currency, employers with social media policies, or those considering them, must be conscientious that their policies do not seek to acquire protected information from employees or job applicants. Even in states where such legislation is not being considered, asking for an applicant or employee for access to such personal information seems to do more harm than good, especially with respect to an employer's current workforce.

## IV. The National Labor Relations Act and Employer Social Media Policies

The National Labor Relations Act ("NLRA") was passed into law in 1935, long before the development of and widespread use of social media. So it may be surprising to learn that the NLRA is playing an increasingly important role with respect to the legality of employers' social media policies.

[8] Ca. S.B. 1349, signed into law September 26, 2012 and effective January 1, 2013. The law does not apply to passwords or other information used to access employer-issued electronic devices, including company laptops and smartphones. The bill further stipulates that nothing in its language is intended to infringe on employers' existing rights and obligations to investigate workplace misconduct. In addition to the laws in Maryland and California, Illinois, on August 1, 2012, amended its Right to Privacy in the Workplace Act to limit employers' access to applicants' and employees' password protected social media accounts. Ill. H.B. 3782.

[9] H.R. 5050, Social Networking Online Protection Act.

The NLRA applies to most employees in the private sector.[10] It was passed primarily for the purpose of protecting the rights of employees to engage in concerted activity such as unionization and collective bargaining. Section 7 of the NLRA expressly protects employees' rights to undertake concerted activities that are related to improving the terms and conditions of their workplace.[11]

The NLRA is enforced by the National Labor Relations Board ("NLRB"), an independent federal agency whose governing board, and general counsel, are political appointees. According to the NLRB, an employee's actions are "concerted," and thus potentially protected under the NLRA, when the employee acts with the authority of other employees, seeks to initiate or induce group action among employees, or brings employee complaints to the attention of management. Throughout its existence, the NLRB has uniformly held that an employer violates the NLRA if it takes actions that "reasonably tend to chill employees in the exercise of their Section 7 rights."

In recent years, the NLRB has been extremely active in the area of employer social media policies, finding that numerous employment actions taken pursuant to such policies are in violation of the NLRA, and even invalidating sections of employers' social media policies. Therefore, employers with social media policies, or those considering them, must be conscientious of the NLRB's actions with respect to the NLRA and social media. Recent NLRB decisions and memoranda are discussed below.

[10] *See* 29 U.S.C. §§ 151-169 (2010). There are exceptions for agricultural workers, independent contractors, and supervisors (with certain limitations).

[11] *See id.* § 157.

### A. *Hispanics United of Buffalo, Inc.*

On September 2, 2011, an NLRB administrative law judge issued one of the first ever decisions involving the NLRA and social media. In *Hispanics United*, it was held that an employer violated the NLRA by discharging five employees for comments made by the employees on their Facebook pages during non-working hours.[12]

An employee of Hispanic United of Buffalo ("HUB"), a non-profit social service company, had criticized the job performance of another employee. The employee whose performance had been criticized went on Facebook, outside of work hours, and posted a message stating that she was fed up with the employee being critical of her and asking other co-workers their opinions. Four co-workers responded to the post, and, using language that included various obscenities, stated that they too were angry at the employee in question.

When the executive director of HUB learned of the five employees' Facebook posts, she discharged the employees, contending that their posts constituted bullying and harassment. The discharged employees filed a complaint with the NLRB, and an administrative law judge agreed that the employees' Facebook postings were protected concerted activity under the NLRA, and that HUB had therefore violated the NLRA by discharging the employees. In reaching his holding, the administrative law judge noted that employees' discussions about criticisms of their job performance are protected under the NLRA, even if the criticisms are made by a co-worker as opposed to a supervisor. According to the judge, "the discriminatees herein were taking a first step towards taking group action to defend themselves against accusations they could reasonably believe [their colleague] was going to make to management. By discharging the discriminateees

[12] *Hispanics United of Buffalo, Inc.*, Case No. 3-CA-27872 (Sept. 2, 2011).

. . . [HUB] prevented them [from] taking any further [concerted action] vis-à-vis [their colleague's] criticisms." HUB was ordered to reinstate the discharged employees and to pay them back pay.

The judge in *Hispanics United* noted that the Facebook posts were not made at work and occurred outside working hours. Furthermore, he found that although the postings included obscenities, they were not so extreme as to lose protection under the NLRA, by, for instance, constituting threats. The judge additionally noted that the comments in question did not violate HUB's anti-harassment policy because they had no nexus to any characteristic protected under the policy, such as race or gender.

The import of *Hispanics United*, at least in part, is that an employer cannot take adverse employment actions against employees who, outside of work hours, post messages to social media that are critical of a co-worker and could reasonably be construed as constituting "concerted activity." By comparison, as evidenced in a decision issued by the NLRB shortly after *Hispanics United*, an employee who makes postings on Facebook after work hours in which he alone "rants" about his supervisor will not necessarily constitute protected "concerted activity."[13]

### B. Recent Memoranda on Social Media Cases by the Office of the General Counsel for the NLRB

The NLRB has also recently released three memoranda by its general counsel that discuss various instances in which the NLRB has concluded that employer social media

[13] *Frito Lay, Inc.*, Case No. 36-CA-10882 (Sept. 19, 2011). In *Frito Lay*, the employee, shortly after leaving work, posted profanity laced messages on his Facebook page criticizing his supervisor for not allowing him to leave work early due to illness without being docked time. In part because no other employees responded to his posts, the NLRB concluded that the posts constituted unprotected "ranting" as opposed to "concerted activity."

policies violate the NLRA.[14] These memoranda indicate that the NLRB is becoming increasingly vigilant in the area of employer social media policies. Any employer with such a policy, or considering implementing one, must be familiar with the NLRB's memoranda regarding social media.

Some examples of the cases outlined in the memoranda that are worth noting:

- In one case, the NLRB found a provision of an employer's social media policy unlawful that prohibited employees from making disparaging remarks about the employer on social media because the policy did not expressly state that the policy did not apply to employees' rights to discuss the terms and conditions of their employment on social media.

- In another case, the NLRB determined that a car dealership wrongfully terminated an employee who posted comments on Facebook criticizing a sales event held by the dealership. According to the NLRB, the employee's comments related to the terms and conditions of employment because they discussed the payment of sales commissions.

- The NLRB found that a employer social media policy instructing employees that "offensive, demeaning, abusive or inappropriate remarks are as out of place online as they are offline" was overbroad and unlawful because it could be construed to include protected criticisms of an employer's labor policies or treatment of employees.

- The NLRB found that a provision in an employer social media policy instructing employees "to think carefully about friending co-workers" was overbroad and unlawful because it discouraged communications among workers, and therefore interfered with the ability of employees to engage in protected concerted activity as allowed by Section 7.

- Finally, although not included the memoranda, on September 7, 2012, the NLRB issues a decision finding that Costco's social media policy prohibiting employees from using social media to

[14] *See NLRB Office of the General Counsel, Memorandum OM* 12-59, May 30, 2012; *NLRB Office of the General Counsel, Memorandum OM* 12-31, January 24, 2012; and *NLRB Office of the General Counsel, Memorandum OM* 11-74, August 18, 2011.

> defame the company violated Section 8(a)(1) of the NLRA.[15] The portion of Costco's policy at issue stated that "Employees should be aware that statements posted electronically (such as to online message boards or discussion groups) that damage the company, defame any individual or damage any person's reputation or violate the policies outlined in the Costco Employment Agreement may be subject to discipline, up to and including termination of employment." In striking down this provision, the NLRB administrative judge noted that although it did not expressly refer to protected Section 7 activity, the provision, read literally, could apply to communications in which an employee criticized Costco's workplace conditions, and made no exception for such communications.[16]

Employers with social media policies, or who may be considering them, must be aware of the protections afforded employees under Section 7 of the NLRA. This is particularly true in view of the NLRB's recent aggressive posture in the area of employer social media policies, and its broad interpretation of the NLRA in the social media context. Generally, employers should be aware that their employees' social media activity will be protected if it concerns wages, hours, benefits, or other terms and conditions of employment. Social media policies should be careful not to infringe upon these rights.

## V. Harassment and Discrimination Issues to Consider with Respect to Employer Social Media Policies

Various state and federal laws protect an employee's right to work in a workplace that is free from discrimination and harassment. Social media, as countless stories in the media illustrate, provides a forum in which much harassment occurs. Therefore, in crafting a social media policy, employers must pay special attention to addressing

[15] Section 8(a)(1) makes it unlawful for an employer to interfere with, restrain, or coerce employees in their exercise of the rights guaranteed by Section 7 of the NLRA.

[16] *Costco Wholesale Corp. and United Food and Commercial Workers Union, Local 371*, Case No. 34-CA-012421 (Sept. 7, 2012).

harassment and discrimination by employees or supervisors through various social media platforms.

The need for employers to be proactive with respect to harassing actions by their employees on social media is directly related to the fact that employers can, in certain circumstances, be liable for their employees' social media postings that occur outside the workplace. For instance, if an employee is harassing a co-worker on Facebook, particularly with respect to race or sex, and the employer knows or should know of the harassment, the employer could be vicariously liable for the harassment if it fails to take corrective action.[17]

Because of the possibility of vicarious liability for an employee's harassing or discriminatory postings on social media that are directed to other employees, employers' social media policies should include provisions prohibiting such harassment and stating that corrective action will be taken for any online behavior that rises to the level of harassment or discrimination and that is connected to the workplace. In this regard, employers should be aware of state laws directed toward online harassment, and reference such laws in their social media policies. For instance, in 2009, Texas amended

[17] *See, e.g., Blakey v. Continental Airlines, Inc.*, 751 A.2d 538, 552 (N.J. 2000) (holding employer liable for online harassment by its employees of co-worker when employer was on notice of harassment and took no action to stop it and when harassment was sufficiently connected to the workplace). Employers should also be aware of the possibility of vicarious liability in situations where an employee is using the employer's computer system for harassing or illegal purposes. There is some authority that the Communications Decency Act, 47 U.S.C. § 230 provides immunity to employers who provided their employees with Internet access. Immunity may, however, not be afforded in circumstances wherein an employer has a duty to act. *Compare Delfino v. Agilent Technologies*, 145 Cal. App. 4th 790 (2006) (holding that employer was immune from liability pursuant to Communications Decency Act when employee used employer's computer system to send threatening emails, but also noting that employer was unaware of emails and that employee was acting outside scope of employment) *with Doe v. XYC Corp.*, 887 A.2d 1156 (N.J. App. Ct. 2005) (holding that employer could be found liable for negligence when employee was using employer provided computer to view child pornography and rejecting employer's claim that its privacy policy prevented it from investigating the employee's activities).

its penal code statute to make it a third-degree felony to use a fake name or identity to create a Web page or post messages on a social networking site without consent and "with the intent to harm, defraud, intimidate, or threaten any person."[18]

[18] Tex. Pen. Code Ann. § 33.07 (Vernon 2010).

## VI. Employers Need to be Aware of Laws Restricting Monitoring and Protecting an Employee's Right to Privacy

The majority of employer workplace policies include statements that any employee emails, messages, or other communications sent or received on the employer's network systems or equipment are not private and are subject to monitoring. Such statements are typically intended to guard against potential violations of state laws protecting the right of privacy. As the right of privacy is tied to one's "reasonable expectations" of privacy, it is important for employer policies and handbooks to inform employees that they should have no expectation of privacy for any social media activity that is sent or received on employer-owned networks or equipment.

As discussed above, there is authority that employers may be vicariously liable for employees' harassing or discriminatory social media postings that are sufficiently connected to the workplace and that an employer knew or should have known of. This, or course, raises the question of what actions, if any, an employer should take to monitor an employee's use of social media and other electronic communications.

With respect to monitoring, employers must be careful to not run afoul of various laws protecting employees' electronic communications. For instance, the Stored Communications Act ("SCA") prohibits the knowing or intentional unauthorized access to "a facility through which an electronic communication service is provided."[19] The upshot of the SCA is that an employer cannot, absent authorization, access a password protected personal email account or personal social networking account even when the communications in question are stored on the employer's own network systems. With certain qualifications, an employer who obtains authorization from an employee can

[19] *See* 18 U.S.C. §§ 2701, 2707.

access personal communications that are stored on the employer's system. But the question of whether such authorization needs to be specific, or can be general, has yet to be addressed by the courts. Employers should not presume that an employee's signed acknowledgment of the receipt and review of an employee handbook stating that such authorization exists complies with the SCA.

In addition to the SCA, employers should be aware of the Electronic Communications Privacy Act (commonly known as the "Wiretap Act").[20] The Wiretap Act bars the intentional interception of electronic communications. The Act, however, has been interpreted to mean that an interception occurs only if it is contemporaneous with the communication itself. Thus, an employer's subsequent review of stored email and electronic communications has been held to not implicate the Act.[21]

Based on a recent 7th Circuit Court of Appeals holding, there is authority that auto-forwarding emails from employee's email account to a supervisor's account for review may violate the Wiretap Act.[22] Therefore, employers should not assume that such actions are not subject to the Act because they do not involve "contemporaneous" monitoring. With this in mind, employers should consider obtaining written authorization and consent from employees for any type of IT action that involves the interception of communications. In doing so, employers need to be mindful of the fact that handbook policies on the subject of electronic monitoring will not necessarily

[20] *See* 18 U.S.C. § 2510 et seq.

[21] *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (9th Cir. 2002).

[22] *See U.S. v. Szymuszkiewicz*, 622 F.3d (7th Cir. 2010).

constitute the authorization necessary to avoid liability under the Wiretap Act.[23]

## VII. Federal Trade Commission Regulations with respect to Postings about an Employer's Products or Services

It has become increasingly common for companies to hire marketers to blog positively or create buzz about their products and services. Many employees also use social media to post favorable reviews or comments about their employer's products and services. Sensitive to the possibility that such practices may mislead consumers and constitute false advertising, the Federal Trade Commission ("FTC") promulgated regulations concerning the use of social media by employees (or agents of employers) to discuss their employer's products and services.[24] In crafting any social media policy, employers need to be aware of these FTC regulations.

Basically, the regulations provide that when an employee endorses his employer's products or services using social media, the employee must reveal that he works for the company whose products or services he is endorsing. Failure to provide such a disclaimer can result in liability for both the employee and employer in the event that the statements in question are false or unsubstantiated.[25] Employers should be aware that the FTC is actively enforcing its regulations regarding the endorsement of products and services on social media. For instance, Legacy Learning Systems ("LLS") recently agreed to pay a $250,000 fine to settle a lawsuit brought by the FTC alleging that LLC

[23] *Garza v. Bexar Metro. Water Dist.*, 639 F. Supp.2d 770 (W.D. Tex. 2009) (holding that employer's statement in employee handbook that employer reserved right to monitor and access any telephone or email messages stored on employer's system was not sufficient to imply employee's consent to interception of his telephone calls).

[24] 16 C.F.R. § 225 et seq.

[25] The FTC's regulations do not create a private cause of action; however, the FTC itself may investigate or file suit against offending employees and employers.

used outside marketing services to post positive reviews on various social media sites of LLS's guitar lesson DVDs without requiring the marketers to disclose that they were receiving commissions from LLS for sales connected to their endorsements.

## VIII. Recommendations for Employer Social Media Policies

This paper does not present an exhaustive list or discussion of the laws that may be implicated by an employer's social media policy. Considering rapidly evolving social media technology and legislation, any such discussion would quickly become outdated. Thus, employers with or considering social media policies should consult an attorney to ensure that their policies are consistent with existing (and rapidly evolving) laws affecting social media. With this caveat in mind, the following non-exhaustive list of guidelines provides a general framework for an effective employer social media policy:

- Understand that pursuant to Section 7 of the NLRA, employees have the right to engage in certain social media activity that criticizes their employer, superiors, co-workers, or the terms and conditions of employment. Furthermore, employees have the right under the NLRA to "friend" co-workers and to discuss co-workers so long as in doing so there is a sufficient nexus with activity protected by Section 7.

- Related to the NLRA, recent decisions by the NLRB indicate that social media policies that are overbroad or ambiguous are likely to be construed as infringing on employees' Section 7 rights. Thus, employers' social media policies should be drafted with specificity. Blanket prohibitions of certain activities, e.g. talking the press, talking about co-workers, are likely to violate the NLRA.

- The focus of any employer social media policy should be on restricting the use of social media for purposes that are clearly not protected by the NLRA.

- Include a statement barring harassment of co-workers over social media and providing that employees must report any such harassment. Similar statements regarding discrimination should be included.

- Be aware of off-duty conduct laws and ensure that the policy does not run afoul of such laws.

- With respect to the use by employees of employer owned networks and equipment, make clear that employees should have no expectation of privacy.

- Ensure that any monitoring of employee communications over social media, or otherwise, is done in a manner that is consistent with applicable federal and state laws.

- Include a statement in the policy that the use of social media cannot interfere with the performance of job duties.

- Inform employees that if they endorse any of the employer's products or services online, they must identify themselves in the posting as an employee.

- Address issues regarding intellectual property by specifying that any use of social media must comply with applicable restrictive covenants and confidentiality agreements.

- Be wary of disclaimers, which the NLRB has indicated will not be effective when a social media policy restricts allowable Section 7 activity.

- In the hiring context, do not conduct social media reviews of job applicants; limit such reviews to background checks on finalists for job openings who have already been interviewed. Additionally, for companies with HR staffs, the best practice is for HR personnel to conduct the social media review.