

# *Chapter 12*

## **Employee Blogging and Social Media**

- § 12:1 Introduction
- § 12:2 Concerns with Employee Blogging Social Networking
  - § 12:2.1 Generally
  - § 12:2.2 Cyber-Bullying
- § 12:3 Sources of Protection for Bloggers
  - § 12:3.1 NLRA—Concerted Activity
  - § 12:3.2 Whistleblower and Retaliation Laws
  - § 12:3.3 First Amendment Retaliation
  - § 12:3.4 Discrimination Laws
  - § 12:3.5 State Privacy Protection and Off-Duty Conduct Laws
    - [A] New York Labor Law
      - [A][1] The Definition of “Recreational Activities”
      - [A][2] Limits on the Scope of “Recreation”
    - [B] California Labor Law
      - [B][1] The Scope of “Lawful Conduct” Under Section 96(k)
      - [B][2] The Scope of Privacy Rights Under California Law
  - § 12:3.6 Employer Liability in the Context of Blogging and Social Networking
    - [A] Liability for Hiring Decisions
    - [B] Federal Trade Commission Issues
  - § 12:3.7 Privacy and Discoverability of Online Information
  - § 12:3.8 Pending Issues
- § 12:4 Practice Pointers

## § 12:1 Introduction

Social networking websites such as Twitter, MySpace, and Facebook have drastically increased the number of people participating in some form of online forum.<sup>1</sup> Adding this to the population of people who use “blogs” shows that the overall online community is expanding exponentially. A social networking site is a website that provides a virtual community for people to interact for personal or business purposes, featuring a “profile” that includes biographical data and functions that allow the user to upload pictures or other information while posting comments and thoughts; a blog (short for “weblog”) is a website featuring regular entries of commentary, descriptions of events, or multimedia. Most blogs are maintained by individuals, and they generally address specific topics or serve as personal diaries. The blog search engine Technorati has indexed more than 133 million blog records since 2002, and marketing experts estimated that, in 2008, approximately 25 million Americans blogged.<sup>2</sup> While the percentage of bloggers under thirty years of age is dropping with the increasing popularity of social networking,<sup>3</sup> the combination of social networking and blogging surpassed email in popularity in 2009 with 67% of the worldwide population participating.<sup>4</sup>

These forms of online activity raise a host of concerns for employers. Many employees discuss their jobs or careers and create posts about an employer that may be public and available for long periods of time before that employer discovers them. How, then, can an employer safeguard against dissemination of trade secrets, protect a clean public image, and monitor for defamatory, embarrassing, or potentially damaging statements? More importantly, what actions can an employer take when it discovers objectionable online content?

Unfortunately, current law provides little in the way of guidance. State and federal employment statutes do not explicitly regulate employees’ online activity, and there is little case law on the subject. However, certain state and

- 
1. For example, Facebook is approaching 600 million users and Twitter users post 90 million “tweets” per day. Joel Schroeder & Leita Walker, *Social Media in Civil Litigation*, Law360.com, Oct. 12, 2010, [http://employment.law360.com/print\\_article/200684](http://employment.law360.com/print_article/200684).
  2. Technorati, *State of the Blogosphere 2008*, available at <http://technorati.com/blogging/state-of-the-blogosphere/>.
  3. Press Release, Pew Internet, Social Media and Young Adults, Feb. 3, 2010, [www.pewinternet.org/Press-Releases/2010/Social-Media-and-Young-Adults.aspx](http://www.pewinternet.org/Press-Releases/2010/Social-Media-and-Young-Adults.aspx).
  4. NIELSEN, GLOBAL FACES AND NETWORKED PLACES, Mar. 2009, [http://blog.nielsen.com/nielsenwire/wp-content/uploads/2009/03/nielsen\\_globalfaces\\_mar09.pdf](http://blog.nielsen.com/nielsenwire/wp-content/uploads/2009/03/nielsen_globalfaces_mar09.pdf).

federal laws may protect these employees, and employers should stay apprised of further developments in the area. Additionally, crafting a technology policy that addresses the challenges and potential issues presented by employee online activity is practically essential.

## § 12:2 Concerns with Employee Blogging and Social Networking

### § 12:2.1 *Generally*

Employees opine online about a range of topics, which may include their hobbies, travels, politics, and—not surprisingly—their jobs. For example, employees might use their blogs or social media to vent about their job assignments, their supervisors, or office policies and politics. The increase in employee online activity raises the following potential concerns:

- (1) Reduced productivity if employees are blogging or using social media during company time (and using company resources);
- (2) Leaking confidential information and/or trade secrets (either intentionally or inadvertently);
- (3) Posting defamatory, offensive, or inappropriate comments that may subject an employer to liability; and
- (4) Postings that may have a disparaging effect on a company and its products, services, goodwill, or overall image (sometimes known as “cybersmearing”).

Social media websites such as Twitter, Facebook, and MySpace present a host of unique problems for employers. For example, the convenience and ease of use that make a website like Twitter so attractive to its users also make the postings on the site very difficult for employers to monitor, much less to restrict. Messages can be posted on Twitter anytime and anywhere via text message. Employees may post throughout the workday on company time using their personal communication devices without the employer being aware of such activity. Furthermore, because users are able to post their messages immediately, their postings are often not carefully considered and are more likely to be based on emotion rather than reason. As the number of people using these social networking sites continues to explode, employers need to keep abreast of the rapidly changing technology and the employment challenges it creates.

While violations of company policy or breaches of loyalty often present clear cases, a number of statutes and laws may provide some protection to employees who use social media or blog. This raises a general question: If an

employer does not approve of the content of an employee's online posting, can the employer legally discipline the employee?<sup>5</sup>

### § 12:2.2 **Cyber-Bullying**

The main issue with the increase of social networking and other online activity is not that these forums are creating new claims, but that conduct creating these claims can now occur through many new forums. An example of this concern is the rise of "textual" or online harassment and "cyber-bullying."

Cyber-bullying is a real-time, modern way of delivering abuse.<sup>6</sup> Common forms of cyber-bullying are email (the oldest form), texting, phone calls, and social media—now the primary vehicle.

- 
5. There are numerous instances of terminations or revoked job offers resulting from online activity. An intern at Anglo Irish Bank in New York was terminated after requesting time off for a "family emergency" and then posting time-stamped pictures of himself in a fairy costume at a Halloween party. A Microsoft employee who posted pictures of new Apple computers arriving at Microsoft with a caption stating that Microsoft was getting the computers was fired as a "security risk." Virgin Atlantic Airways fired thirteen crew members for offensive posts on Facebook about stereotypes, airplane parts, and sanitary conditions on the planes. A job offer with Cisco was allegedly revoked after the candidate "tweeted" about the dilemma of accepting the paycheck with hating the work. The candidate claims to have rejected the offer prior to the tweet, stating that it was not revoked. Martha Lessman, *Social Media: Not Just for Chitchat Anymore*, Law360.com, May 12, 2009.
  6. While cyber-bullying is much more common among high school students, where there are numerous stories of teen suicide as a result of online harassment and bullying, cyber-bullying is also a growing trend in the workplace. One of the most famous cases of teen suicide as a result of cyber-bullying is the case of Megan Meier. Megan, thirteen, killed herself after a former friend and that friend's mother created a MySpace page, posing as a sixteen year-old boy, and eventually ended the online friendship by telling Megan, among other things, that "the world would be a better place without you." The friend's mother, Lori Drew, was prosecuted for violating the Computer Fraud and Abuse Act. *United States v. Lori Drew*, 259 F.R.D. 449 (C.D. Cal. 2009). Drew was convicted, but later acquitted. In response, Missouri passed what has become known as "Megan's Law," MO. REV. STAT. 565.225, "Offenses Against the Person," which expanded the existing statute to prohibit abusive "communication by any means," designed to include Internet abuse. Linda Sanchez of California introduced the "Megan Meier Cyberbullying Prevention Act" in the House of Representatives on May 22, 2008, specifically with the intention of focusing on and prohibiting cyber-bullying. H.R. 6123. The bill did not pass. Most recently, in January 2010, Phoebe Prince, a fifteen-year-old Irish student who had recently moved to Massachusetts, killed herself after cyber-bullying and harassment. Six teenagers were charged. Pretrial hearings began on September 15, 2010, and the trial should occur in 2011. Hazel Slade, *Six Face*

Social networking sites have created new problems when it comes to harassment.<sup>7</sup> First, people seem more likely to harass someone through electronic communication such as texting or Facebook rather than in person. Because anonymity is possible, human resources departments struggle to address cyber-bullying, and like textual harassment, cyber-bullying is easier to do when not face-to-face. Second, harassment through social media, such as Facebook, is more public because it is broadcast to a wider group. This increases the risk of a third party claiming a sexually hostile working environment, for example, if an employee's computer can be seen by co-workers.<sup>8</sup> Third, Facebook now provides provocative as well as potentially offensive and harassing functions that enable a user to "superpoke" another user, which

---

*Court After Death of Bedford-Born Teenage Girl*, BEDFORDSHIRE ONSUNDAY, Sept. 26, 2010, [www.bedfordshire-news.co.uk/News/Six-face-court-after-death-of-Bedford-born-teenage-girl.htm](http://www.bedfordshire-news.co.uk/News/Six-face-court-after-death-of-Bedford-born-teenage-girl.htm). As in Missouri, a state statute was passed in Massachusetts designed to address bullying in schools and specifically addressing cyber-bullying in response to the suicides of Phoebe and eleven-year-old Carl Walker. Mass. Acts of 2010, ch. 92, available at [www.malegislature.gov/Laws/SessionLaws/Acts/2010/Chapter92](http://www.malegislature.gov/Laws/SessionLaws/Acts/2010/Chapter92); Noah Bierman, *Grieving Family by His Side, Governor Signs Legislation*, BOS. GLOBE, May 4, 2010, available at [www.boston.com/news/local/massachusetts/articles/2010/05/04/grieving\\_family\\_by\\_his\\_side\\_governor\\_signs\\_legislation/](http://www.boston.com/news/local/massachusetts/articles/2010/05/04/grieving_family_by_his_side_governor_signs_legislation/). Other instances of teen suicide as a result of cyber-bullying are the suicide of thirteen-year-old Ryan Halligan in Vermont and eighteen-year-old Tyler Clementi, *States Pushing for Laws to Curb Cybrebullying*, ASSOCIATED PRESS, Feb. 21, 2007, available at [www.foxnews.com/story/0,2933,253259,00.html](http://www.foxnews.com/story/0,2933,253259,00.html); Jonathan Lemire, Michael J. Feeney, and Larry McShane, *Rutgers' Tyler Clementi Complained of Video Voyeur Before Fatal Fall From George Washington Bridge*, N.Y. DAILY NEWS, Oct. 1, 2010, [http://www.nydailynews.com/ny\\_local/2010/10/01/2010-10-01\\_he\\_wanted\\_roomie\\_out\\_rutgers\\_suicide\\_complained\\_of\\_video\\_voyeur\\_before\\_fatal\\_fal.html](http://www.nydailynews.com/ny_local/2010/10/01/2010-10-01_he_wanted_roomie_out_rutgers_suicide_complained_of_video_voyeur_before_fatal_fal.html).

7. Michael S. Cohen (partner with Duane Morris in Philadelphia), Camille Hébert (an employment discrimination professor at the Moritz College of Law at The Ohio State University), and Michael Latimer (partner with Harkins, Latimer & Dahl in San Antonio) all agree that social networking sites like Facebook and Twitter are additional means for one employee to subject another to harassment or discrimination. In Princeton, New Jersey, Workrights Institute president Lewis Maltby stated that "[t]hese issues are on the leading edge of the law right now." Cohen predicted a one- to two-year lag before social media harassment cases get through the litigation process. *Attorneys Provide Advice to Employers on Blocking Harassment Via Facebook*, bna.com, July 28, 2010.
8. Christine Caulfield, *Virtual Sexual Harassment Nothing to LOL About*, EmploymentLaw360.com, Nov. 6, 2009 [hereinafter Caulfield], available at <http://employment.law360.com/articles/131373>; Tresa Baldas, *'Textual Harassment' No Laughing Matter*, NAT'L L.J., July 16, 2009 [hereinafter Baldas], available at [www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202432277162](http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202432277162).

allows the user to “spank,” “shower with,” and “fling a thong at” another user.<sup>9</sup> Texts and websites also create a record of the conversation as opposed to a “he-said-she-said” verbal exchange. In one situation, an “office Casanova” broadcast his “exploits” on Facebook. When the posts and comments became explicit, one woman who was the subject of a post claimed she was sexually harassed.<sup>10</sup>

While cyber-bullying can create an unprofessional and offensive work environment, it can also put a company’s reputation at risk. If the exchanges are leaked outside the company, competitors can use them as a tool to damage their rival’s reputation or credibility.

A high-profile case of cyber-bullying in Australia revolved around a stolen sandwich. The exchange, which eventually led to the participants’ termination, was sent to other firms, here because it was humorous, not because of a leak or corporate espionage. But the risk of negative publicity is still present.

Policing cyber-bullying can be difficult. In addition to anonymity, tone can often be mistaken in online communication that can lead to unintentional bullying. Also, managers are common culprits of cyber-bullying. As with many issues involving social media, it is important to maintain a company policy that stays up to date with technology.<sup>11</sup>

Some states have passed statutes penalizing offensive or harassing social media communications, while other states have more general statutes prohibiting electronic forms of harassment or stalking, or have statutes aimed at cyber-bullying.<sup>12</sup>

---

9. Joel Schroeder & Leita Walker, *Social Media in Civil Litigation*, Law360.com, Oct. 12, 2010, available at [www.law360.com/web/articles/200684](http://www.law360.com/web/articles/200684).

10. Caulfield, *supra* note 8; Stephanie Chen, *Workplace Rants on Social Media Are Headache for Companies*, CNN.com, May 12, 2010, [www.cnn.com/2010/LIVING/05/12/social.media.work.rants/index.html?hpt=C2](http://www.cnn.com/2010/LIVING/05/12/social.media.work.rants/index.html?hpt=C2).

11. Eleanor Dallaway, *Cyber-Bullying Plagues Workplace*, infosecurity.com, Apr. 23, 2010, [www.infosecurity-magazine.com/view/8987/cyberbullying-plagues-workplace/](http://www.infosecurity-magazine.com/view/8987/cyberbullying-plagues-workplace/); Bullying Statistics, *Bullying Statistics 2009*, [www.bullyingstatistics.org/content/bullying-statistics-2009.html](http://www.bullyingstatistics.org/content/bullying-statistics-2009.html).

12. New Jersey (Social Networking Safety Act, H.R. 3757, 213th Leg. (N.J. 2009)), Texas (Online Harassment, TEX. PENAL CODE ANN. § 33.07 (2009)), and Mississippi (H.R. 1427, 95th Leg. (Miss. 2010)) have passed statutes focusing on sexually offensive or harassing social networking communications. Forty-seven states have passed statutes that explicitly include electronic forms of communication within stalking and harassment laws. “State Electronic Harassment or ‘Cyberstalking’ Laws,” National Conference of State Legislatures.com, Oct. 11, 2010, <http://www.ncsl.org/default.aspx?tabid=13495>. Arkansas, Idaho, Iowa, New Jersey, Oregon, Missouri, New York, Rhode Island, and Vermont have all passed laws against cyber-bullying. “Cyber Bullying State Laws and Policies,” CyberBullyAlert.com, Oct. 8, 2008, <http://www.cyberbullyalert.com/blog/2008/10/cyberbullying-state-laws-and-policies/>.

## § 12:3 Sources of Protection for Bloggers

### § 12:3.1 NLRA—Concerted Activity

Section 7 of the National Labor Relations Act, 29 U.S.C. § 157, prohibits an employer from interfering with union organization or with “concerted activity”—the ability of employees to discuss benefits, wages, and other terms and conditions of employment. The NLRA protects employees’ rights to communicate among themselves about these issues and bring them to the employer’s attention. These rights are protected both during work hours and while off duty. The language of section 7 applies to all employees in the workplace who are engaged in “concerted activity for mutual aid and protection,” not just those who are already involved with unions. *See NLRB v. Wash. Aluminum*, 370 U.S. 9 (1962) (interpreting section 7 and applying the law in a nonunion context). If an employer fires an employee for online comments about low wages, poor benefits, or long work hours, that employee may have a viable claim under section 7 of the NLRA.

However, attacks on an employer that are unrelated to employment conditions are not protected by the NLRA. If an employee attacks the employer generally, without reference to the terms and conditions of employment, the speech is not protected under the Act. *See NLRB v. Local Union 1229 (Jefferson Standard)*, 346 U.S. 464, 476–77 (1953) (refusing to extend protection to speech that attacked the quality of an employer’s product, without more).

### § 12:3.2 Whistleblower and Retaliation Laws

Dozens of federal laws protect whistleblowers and shield workers from retaliation. Additionally, a number of states, including New York and California, provide protection for employees who report wrongdoing, internally or externally.

Generally, in order to invoke the protection of a whistleblower statute, the employee must first have made some report to a government agency. In other words, they must actually “blow the whistle.” Similarly, anti-retaliation laws protect employees who report wrongdoing (such as discrimination and harassment) through internal channels. Blogging about problems or violations of law, without more, may not be enough to be covered under this umbrella. However, because whistleblowers may use these forums as well, employers should be aware of the issue and maintain a policy about publication of company affairs on the Internet.

### § 12:3.3 *First Amendment Retaliation*

In addition to the whistleblower and retaliation laws applicable to all employers, government employers are also subject to retaliation claims based on the First Amendment. See 42 U.S.C. § 1983. Recently, in the unpublished decision of *Richerson v. Beckon*, No. 08-35310, 2009 U.S. App. LEXIS 12870 (9th Cir. June 16, 2009), the Ninth Circuit addressed the issue of employee blogging in the context of a First Amendment retaliation claim. In that case, Richerson, a school teacher, maintained a publicly available blog titled “What It’s Like on the Inside,” which included several highly personal and critical comments about her employer, union representatives, and fellow teachers. For example, in her blog, Richerson referred to a new employee as “White Boy” and a “smug know-it-all creep,” and equated the teacher union’s chief negotiator to Hitler. After the blog was discovered, several teachers and other school employees complained to the school district’s human resources director about the blog. Additionally, at least one person to whom Richerson was assigned to mentor refused to work with her any longer. Thereafter, the school district’s director of human resources transferred Richerson from her position as a “curriculum specialist” and “instructional coach” to a classroom teaching position. The district contended that Richerson was reassigned because her blog had undermined her ability to enter into trusting relationships as an instructional coach. Richerson sued the district, alleging that her duties were reassigned in retaliation for the exercise of her First Amendment free speech rights. The district court granted summary judgment for the district.

The Ninth Circuit affirmed the district court’s ruling that the reassignment did not violate Richerson’s constitutional rights. In so ruling, the court applied the balancing test set forth in *Pickering v. Bd. of Educ.*, 391 U.S. 563 (1968), and weighed the administrative interests of the school district against Richerson’s right of free speech under the First Amendment. The court concluded that, because Richerson’s blog postings eroded her work relationships, the balance tipped in favor of the school district.

### § 12:3.4 *Discrimination Laws*

Should employers seek to investigate and reprimand employees for personal blogs that may be potentially injurious to the company’s good will or reputation, employers must be sure to conduct such investigations and take enforcement actions in a nondiscriminatory manner. Enforcement against employee blogs can lead to discriminatory enforcement claims. For example, Delta Air Lines terminated an employee for posting sexually suggestive photographs of herself in a Delta uniform on her blog, entitled “Queen of the Sky.” The employee then filed a sex-discrimination complaint against Delta with

the Equal Employment Opportunity Commission and a multi-million dollar lawsuit against Delta, claiming that other employees, primarily men, have posted photographs of themselves in uniform on the Web without incident. The case is still pending. *Simonetti v. Delta Airlines, Inc.*, No. 05-2321 (N.D. Ga. filed Sept. 7, 2005).

In an earlier case involving airline employees' blogs, *Blakey v. Cont'l Airlines*, 164 N.J. 38 (N.J. 2000), the Supreme Court of New Jersey, overruling the New Jersey Superior Court and Superior Court Appellate Division, found that the continuation of harassment through an online forum could be closely related to the workplace and lead to employer liability. In *Blakey*, a number of male pilots posted inflammatory, debasing, and derogatory comments about a female pilot on a computer forum maintained by Continental for all of its employees. *Id.* at 51-53. The court held that, although Continental did not have a duty to monitor private communications of its employees, Continental had a duty to take effective measures to stop co-employee harassment that it knew, or had reason to know, was occurring in a workplace-related setting. *Id.* at 62. The court concluded that the employer-run online bulletin board was essentially the same as a bulletin board in an employee lounge or break room, and therefore, it was part of the workplace. *Id.* at 56.

### § 12:3.5 **State Privacy Protection and Off-Duty Conduct Laws**

Some states, notably New York and California, have off-duty conduct statutes. These laws limit the ability of an employer to discipline or terminate an employee for engaging in lawful, off-duty political or recreational activity that does not present a conflict with the employer's business. The case law interpreting these statutes is limited, but blogging could conceivably fall under the umbrella of protected activities under certain circumstances.

In addition to New York and California, similar statutes have been enacted in Colorado, Connecticut, North Dakota, Missouri, and New Jersey.

#### **[A] New York Labor Law**

New York Labor Law prohibits discrimination against an employee for his or her participation in "legal recreational activities outside work hours." N.Y. LAB. LAW § 201-d(2)(c). The statute defines "recreational activities" as "any lawful, leisure-time activity, for which the employee receives no compensation and which is generally engaged in for recreational purposes, including but not limited to sports, games, hobbies, exercise, reading and the viewing of television, movies and similar material." N.Y. LAB. LAW § 201-d(1)(b). These recreational activities must take place outside of working hours, off the employer's

premises, and without use of the employer's property to qualify for protection. N.Y. LAB. LAW § 201-d(2)(c). The statute also protects an employee's right to engage in legal political activities on the employee's own time and without use of company property. N.Y. LAB. LAW § 201-d(2)(a).

**[A][1]            *The Definition of "Recreational Activities"***

Since the law was enacted in 1992, there have been very few decisions—and none on blogging or social media—interpreting the scope of “recreational activities.” Early district court decisions construed the term fairly broadly, but subsequent New York state appellate decisions and a decision by the Second Circuit have narrowed the statute's reach.

In 1995, the Southern District ruled that cohabitation was a protected activity under section 201-d. *Pasch v. Katz Media Corp.*, No. 94 CIV. 8554, 1995 WL 469710, at \*3 (S.D.N.Y. Aug. 8, 1995). In *Pasch*, an employee alleged she was fired for maintaining a “personal relationship” and cohabiting with a company executive. Based on the legislative history of section 201-d, the district court took a position contrary to an earlier appellate division decision, *State v. Wal-Mart Stores*, 621 N.Y.S.2d 150 (N.Y. App. Div. 1995).

Three years later, the district court held that “friendships,” or non-romantic personal relationships, were also protected under section 201-d. *Aquilone v. Repub. Bank of N.Y.*, No. 98 Civ. 5451, 1998 WL 872425, at \*6 (S.D.N.Y. Dec. 15, 1998). The court cited the reasoning of *Pasch*, noting that the New York Court of Appeals had yet to rule on the issue. *Id.*

However, New York state courts have refused to take such a broad view of section 201-d, and a more recent Second Circuit case adopts this trend. The Third Department held in 1995 that cohabitation is not protected under the Labor Law—the decision later questioned by the Southern District, as noted above. *Wal-Mart Stores*, 621 N.Y.S.2d at 152. The court in *Wal-Mart* found that dating and other personal relationships are “entirely distinct from and, in fact, bear[ ] little resemblance to ‘recreational activity.’” *Id.* This reasoning has been adopted by appellate courts in the First and Second Departments. *Hudson v. Goldman Sachs & Co.*, 725 N.Y.S.2d 318, 319 (N.Y. App. Div. 2001) (holding that, per *Wal-Mart*, romantic relationships are not protected under section 201-d); *Bilquin v. Roman Catholic Church*, 729 N.Y.S.2d 519 (N.Y. App. Div. 2001) (holding, contrary to *Pasch*, that cohabitation is not protected recreational activity). The Second Circuit weighed in on the issue in 2001 and held, contrary to *Pasch* and *Aquilone*, that romantic relationships are not protected activity. *McCavitt v. Swiss Reinsurance Am. Corp.*, 237 F.3d 166, 167–68 (2d Cir. 2001) (noting fundamental differences between the nature of the listed activities and “romantic dating”).

The disputed issues to date have centered around personal relationships, not around activities resembling blogging or social networking. While recent decisions have taken a narrow view, it is likely that blogging fits more squarely into the definition of recreation, potentially as a “hobby.” The bigger issue under the off-duty statutes arises when examining social networking profiles. Pictures or “status updates” referring to off-duty activity that may be illegal may not be protected, while off-duty activity such as smoking or drinking (provided the employee is of legal age) may be protected.

### **[A][2] Limits on the Scope of “Recreation”**

The protection for recreational activity is limited: An employer may refuse to hire, discipline, or terminate an employee if the activity “creates a material conflict of interest related to the employer’s trade secrets, proprietary information or other proprietary or business interest.” N.Y. LAB. LAW § 201-d(3)(a). The statute plainly leaves room for employers to argue that they can discipline an employee whose online activity contains material that reveals trade secrets or otherwise disparages the employer.

Courts recognize that employees owe a duty of loyalty to their employers. Implicit in any employment relationship is the absolute duty of an employee not to use or divulge confidential knowledge or information acquired during his employment. *See* *Bus. Networks of N.Y., Inc. v. Complete Network Solutions, Inc.*, No. 605463/98, 1999 WL 126088, at \*5 (N.Y. Sup. Ct. Feb. 19, 1999) (citing 60 N.Y. JUR. *Trademarks, Tradenames and Unfair Competition* § 112), *aff’d*, 696 N.Y.S.2d 433 (N.Y. App. Div. 1999). Consequently, an employee divulging trade secrets may be liable for a breach of a duty of loyalty.

The more difficult question is whether an employer can take action against an employee whose blog or social networking page contains embarrassing material that is facially unrelated to the company. For example, could an employee rely on the Labor Law’s off-duty protection if the employee is fired due to sexually explicit material on the employee’s blog? An employer may argue that this embarrassing material undermines some business interest, whether financial or something less tangible, such as the company’s goodwill or reputation. Whether such online content falls under the Labor Law exception is likely to be evaluated on a case-by-case basis based on the specific factual circumstances.

### **[B] California Labor Law**

California has a similar off-duty conduct statute. The law prohibits discharge or discrimination in employment based on “lawful conduct occurring during nonworking hours away from the employer’s premises” and allows California’s Labor Commissioner to pursue these claims on an employee’s

behalf. CAL. LAB. CODE §§ 96(k), 98.6. However, California courts have construed these protections narrowly, limiting claims under section 96(k) to those alleging violation of constitutional rights. Also, notably, the California State Constitution protects the right to privacy, and unlike federal constitutional claims, that right may be enforced against private employers. Both of these considerations should affect the way employers investigate and respond to problems presented by employee online content.

**[B][1]      *The Scope of “Lawful Conduct”  
Under Section 96(k)***

The language of section 96(k) appears broad, but has been applied narrowly by the courts. Indeed, California appellate courts have held that the statute creates no substantive rights, but instead allows the commissioner to pursue violations of existing civil rights. In order to state a claim under section 96(k) for termination or discrimination in violation of public policy, the employee must allege violations of “recognized constitutional rights.”<sup>13</sup> *Barbee v. Household Auto. Fin. Corp.*, 113 Cal. App. 4th 525, 533–34 (Cal. Ct. App. 2003); *see also* *Grinzi v. San Diego Hospice Corp.*, 120 Cal. App. 4th 72 (Cal. Ct. App. 2004) (“to establish a tortious discharge claim under [section] 98.6, [plaintiff must allege the] discharge occurred because she asserted a recognized constitutional right”) (citing *Barbee*).

In *Barbee*, the court addressed a wrongful termination claim under section 96(k). The plaintiff employee was terminated when it was discovered that he had continued to date a subordinate after the relationship had been discovered by management and ostensibly ended. *Barbee* claimed a violation of his right to privacy and termination in violation of section 96(k). The court found that, under these circumstances, no reasonable expectation of privacy existed, based on the following facts:

- (1) There was no established custom or community norm giving rise to a privacy right in such situations;
- (2) The employer had an interest in avoiding conflicts of interest; and
- (3) The company had a policy discouraging these relationships and requiring disclosure.

Further, because no violation of his constitutional privacy right existed, no claim could exist under section 96(k). *Barbee*, 113 Cal. App. at 532–33. The

---

13. It is important to note that certain civil rights provisions of the California Constitution apply to private action and, thus, to private employers—notably the right to privacy and protections against discrimination. These are discussed below.

court performed this analysis in the context of private employment because the privacy guarantees of California's Constitution apply to private actors. *Hill v. Nat'l Collegiate Athletic Ass'n*, 7 Cal. 4th 1, 20 (Cal. 1994).

In *Grinzi*, the employer terminated the employee, informing her that the cause was improper use of company email. The plaintiff employee alleged this was pretext and that the true reason was her involvement in an investment club the employer believed to be an illegal Ponzi scheme. The plaintiff claimed a violation of her First Amendment free speech rights under the federal constitution and section 96(k). The appellate court affirmed the trial court's dismissal. Because the employer was a private entity, no cause of action for violation of free speech rights could be sustained absent state action, either through the First Amendment or the labor law. *Grinzi*, 120 Cal. App. 4th at 86.

Whether or not blogging and social networking are protected under California's "lawful conduct" statute turns on whether employee discipline or termination would impinge on constitutional rights. Perhaps the most obvious suspect, the right to free speech, is not an issue for private employers. Unlike the protections for privacy in the California Constitution analyzed in *Barbee*, California's protections for free speech require state action. See *Golden Gateway Ctr. v. Golden Gateway Tenants Ass'n*, 26 Cal. 4th 1013, 1031 (Cal. 2001). However, privacy rights are enforceable against private actors and could affect employer liability.

### **[B][2]      *The Scope of Privacy Rights Under California Law***

As mentioned above and as stated in the *Hill* case, the right to privacy guaranteed in article 1, section 1 of the California Constitution is applicable against private actors. This may have implications for private employers, who could be subject to direct suit or a suit through the labor commissioner under section 96(k) for violations of the right to privacy.

A plaintiff alleging an invasion of privacy in violation of state constitutional right to privacy must establish each of the following:

- (1) a legally protected privacy interest;
- (2) a reasonable expectation of privacy in the circumstances; and
- (3) conduct by defendant constituting a serious invasion of privacy.

*Hill*, 7 Cal. 4th at 39–40. In cases of search and seizure, the state protection is "no broader than . . . the 'privacy' protected by the Fourth Amendment."

A recent Ninth Circuit decision addressed employee privacy rights in electronic communications, in the context of text messaging on employer-provided electronic pagers. The plaintiff was a member of the city's police

force. *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 895 (9th Cir. 2008). The city provided alphanumeric pagers to the police force through Arch Wireless, and each pager had a monthly usage limit. If an employee went over the text limit, the employee would generally pay for the overages. An informal policy was in place under which (a) the employee could pay the overage without incident, or (b) the department could review the messages to determine the amount owed for personal use. The department supervisor told the officers that text messages would be considered “email” subject to the city’s acceptable network use policy (which explicitly gave the city the right to search email and denied any expectation of privacy). This oral statement was later put in writing in a memorandum sent to the officers. After a few billing cycles, the department supervisor told officers that it was not his intent to audit the text messages to see if the overage was due to work-related transmissions and suggested that the officers reimburse the city for the overages. Whether this subsequent oral statement abrogated the department’s written policy and memorandum and gave employees a reasonable expectation of privacy was a point of debate throughout the case.

After repeated overages, the supervisors decided to determine if the character limit for the text messages was too low. The supervisors were investigating to determine whether the overages were due to work-related or personal messages. The supervisors requested transcripts of text messages from Arch Wireless for the months of August and September 2002 for two employees, including Jeff Quon, who exceeded character allowances. The department discovered that many of Quon’s messages “were personal in nature, and were often sexually explicit.” *Id.* at 898. Quon brought suit, alleging violations by Arch Wireless of the Stored Communications Act and invasion of the right to privacy by the police chief.

In examining whether Quon had a reasonable expectation of privacy in his text messages and whether the search by the city was reasonable under the circumstances, the Ninth Circuit held that there was a legitimate expectation of privacy in the text messages based on the informal policy followed by the department. While “address” information—such as the sender, recipient, date, and time—may not be subject to an expectation of privacy, the content of those messages generally is protected. Because the city’s official email policy allowing the employer unfettered access was not the “operational reality” in the department, the court held that Quon had a reasonable expectation of privacy in the content of his text messages. *Id.* at 906–08. Additionally, even though the department redacted any messages that were sent while Quon was off-duty and examined only messages Quon sent during work hours during August and September, the court held that the full review of these text messages by the department was unreasonable—the messages could have been reviewed in a redacted format or otherwise manipulated to protect the

content. Because less intrusive methods were feasible, the search violated Quon's right to privacy. *Id.*

The Supreme Court, however, disagreed with the Ninth Circuit's conclusion that the department's search was not reasonable in scope. *City of Ontario v. Quon*, 130 S. Ct. 2619, 560 U.S. \_\_\_\_ (2010). However, before discussing whether the search was reasonable in scope, the Court assumed, *arguendo*, that Quon had a reasonable expectation of privacy in the text messages sent on the pager, that the review of the transcript constituted a search within the meaning of the Fourth Amendment, and that the principles applicable to a government employer's search of an employee's physical office apply with at least the same force when the employer intrudes on the employee's privacy in the electronic sphere. The reason the Court accepted these assertions was a general concern that establishing a bright-line test would not be prudent given the ever changing and expanding use of technology. The Court cautioned that elaborating too fully on how the Fourth Amendment applies in an electronic forum before such technology's role in society is clear could create error in the future.

After making these assumptions, the Court determined that the search's objective was justified at its inception because there were "reasonable grounds for suspecting that the search [was] necessary for a noninvestigatory work-related purpose." *Quon*, 130 S. Ct. at 2623, citing *O'Connor v. Ortega*, 480 U.S. 709, 726 (1987). Because the search was an "expedient and efficient way to determine whether Quon's overages were the result of work-related messaging or personal use," the search was not "excessively intrusive." *Quon*, 130 S. Ct. at 2631, citing *O'Connor*, 480 U.S. at 726. The Court also concluded that Quon did not have a reasonable expectation to think the messages were "immune from scrutiny." *Quon*, 130 S. Ct. at 2631. Because Quon was told the messages were subject to auditing, received no assurances of privacy, and possessed the pager for the work-related purpose of increasing SWAT response time, the Court decided that a reasonable employee would or should know that the employer might audit the messages to determine if there was any inappropriate use. *Id.* Based on this analysis, the Court found the search permissible in scope. *Id.* For the same reasons, the Court also concluded that the search would be "regarded as reasonable and normal in the private-employer context." 130 S. Ct. at 2633.

The Court also rejected Quon's argument that the search was not the least-intrusive method of examining the text messages. 130 S. Ct. at 2632. The Court has "repeatedly refused to declare that only the least intrusive search practicable can be reasonable under the Fourth Amendment." *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 663 (1995); *see also Bd. of Ed. of Indep. Sch. Dist. No. 92 of Pottawatomie Cty. v. Earls*, 536 U.S. 822, 837

(2002). The Court decided that this standard would set the bar too high and result in barriers to virtually all search-and-seizure powers because a judge will always be able to imagine a less-intrusive alternative means. *Quon*, 130 S. Ct. at 2632, citing *United States v. Martinez-Fuerte*, 428 U.S. 543, 557, n.12 (1976).

The Court signaled that in the future it will likely give considerable deference to employer policies, which it declared “will of course shape the reasonable expectations of their employees, especially to the extent that such policies are clearly communicated.” *Quon*, 130 S. Ct. at 2630.

### § 12:3.6 ***Employer Liability in the Context of Blogging and Social Networking***

How is *Quon* relevant to employee blogging? In order to prevent an employee from claiming a privacy right in blog-related materials and activities that take place through the use of company technology, employers should promulgate well-defined technology policies that explicitly state that network and equipment use is subject to monitoring and search. While publicly available blog postings would not be the subject of any privacy protection, stored or archived material on a work computer could potentially qualify.

However, even where an enforceable corporate policy is in place, employee communications originating from employer-owned equipment may be protected against disclosure or employer monitoring, depending on the nature of the communications. In *Stengart v. Loving Care Agency, Inc.*, 990 A.2d 650 (N.J. 2010), the New Jersey Supreme Court, by focusing on the ambiguity of the computer policy, rejected an employer’s claimed right to review and retain emails sent by an employee to her attorney through her web-based email account via the employer’s laptop computer. Specifically, the court stated that the policy did not even address the use of personal email accounts, let alone if such use would be permissible or not and whether the emails would be considered company property. *Stengart*, 990 A.2d at 663 (the policy’s acknowledgment that occasional personal use of email was permitted created doubt about whether those emails were company or private property). However, the court limits its holding to protecting the *contents* of attorney-client communications. *Stengart*, 990 A.2d at 665 (“Our conclusion . . . does not mean that employers cannot monitor or regulate the use of workplace computers. . . . But employers have no need or basis to read the specific contents of personal, privileged, attorney-client communications in order to enforce corporate policy”). Other courts have found employees’ email

communications with their attorneys to be protected despite using employer-owned computers.<sup>14</sup>

In contrast to *Stengart's* finding that the company's policy was ambiguous as to whether personal emails were part of the company's business records, the court in *Scott v. Beth Israel Med. Ctr., Inc.*, 847 N.Y.S.2d 436 (N.Y. Sup. Ct. 2007) held that an employee had waived the attorney-client privilege by using the employer's computer system to communicate with his attorney. In *Scott*, the employer had a policy that provided in relevant part that all of the employer's computer systems should be used for business purposes only, that all information and documents created, saved, or transmitted through the employer's communications and computer systems are company property, and that "employees have no personal privacy right in any material created, received, saved or sent using Medical Center communication or computer systems. The Medical Center reserves the right to access and disclose such material at any time without prior notice." *Id.* at 2. As a result of the clear language of this policy, the court held that the employee had no reasonable expectation of privacy.<sup>15</sup>

- 
14. See *Nat'l Economic Research Assocs., Inc. v. Evans*, 21 Mass. L. Rptr. 337, 2006 WL 2440008 (Mass. Super. Ct. Sept. 25, 2006) (finding the employee's expectation of privacy in emails with his attorney to be reasonable because the policy manual did not expressly declare that it would monitor the content of Internet communications, nor did it expressly declare or suggest that the employer would monitor content of email communications made from an employee's personal email account via the Internet when viewed on an employer-issued computer); *In re Asia Global Crossing, Ltd.*, 322 B.R. 247, 257 (Bankr. S.D.N.Y. 2005) (employee's use of the company's email system did not eliminate the attorney-client privilege because evidence of the existence of a corporate policy banning personal use of email and allowing monitoring was equivocal); *Convertino v. U.S. Dep't of Justice*, 674 F. Supp. 2d 97 (D.D.C. 2009) (finding a reasonable expectation of privacy in attorney-client emails sent via employer's email system).
  15. See also *United States v. Etkin*, 2008 U.S. Dist. LEXIS 12834, at \*14-\*16 (S.D.N.Y. 2008) (employees do not have a reasonable expectation of privacy when employers warn the employees via log-on notices or flash-screen warnings of a policy through which the employer could monitor or inspect the computers at any time); *United States v. Angevine*, 281 F.3d 1130 (10th Cir. 2002) (holding no reasonable expectation of privacy where employer's policy "clearly warned computer users [that] data [wa]s 'fairly easy to access by third parties'"); *Muick v. Glenayre Elecs.*, 280 F.3d 741, 743 (7th Cir. 2002) (holding that any reasonable expectation of privacy computer employee had in his work computer was eliminated when employer announced that it could inspect the computer); *United States v. Bailey*, 272 F. Supp. 2d 822 (D. Neb. 2003) ("An employee cannot claim a justified expectation of privacy in computer files . . . where computer uses were notified that network

While communications that take place over a company network are not subject to a reasonable expectation of privacy, those that take place over outside networks may be. If a company laptop is used at home to post information on a personal blog and no company policy addresses employer access to the laptop, information on that laptop could be the subject of a privacy claim, depending on the circumstances.<sup>16</sup>

Furthermore, employers should be cautioned that to the extent that employees' outside postings on blogs or social networking sites are invitation-only and password protected, unauthorized access of these postings may result in liability. In *Pietrylo v. Hillstone Rest. Grp.*, 2009 WL 3128420 (D.N.J. Sept. 25, 2009), two employees established an invitation-only and password-protected chat group on MySpace for employees of Hillstone to vent their grievances about their employer. Upon request of one of Hillstone's managers, an employee who had been given access to the chat group turned over her account log-in and password information. After accessing the site several times, management fired the two employees who created the group. The employees filed suit claiming that the employer violated the federal Stored Communication Act (SCA) and invaded their right to privacy. The jury returned a verdict for the employees finding that although the employees' common-law right to privacy was not invaded, the employer had violated the SCA by accessing the password-protected MySpace postings without authorization. The jury also found that the employer had acted maliciously, and awarded punitive damages. In upholding the jury verdict, the trial court held that, even though the managers were provided log-in and password information from another employee, the jury's finding that the employer's access was not authorized was supported by evidence that the employee who turned over the log-in and password information was coerced into providing the information.

The rise in social networking sites also increases the risk for discrimination and retaliation by an employer. If an employer is "friended" by an employee,

---

administrators and others were free to view data downloaded from the internet.".) *But cf. In re Asia*, 322 B.R. at 257 (use of the employer's email system does not waive the attorney-client privilege where it is not clear if a company computer policy banning personal emails existed); *Convertino*, 64 F. Supp. at 110 (the employee has a reasonable expectation of privacy in the employer's email system because "[t]he DOJ maintains a policy that does not ban personal use of company email").

16. *Curto v. Med. World Commc'ns, Inc.*, 99 Fair Empl. Prac. Cas. (BNA) 298, 2006 WL 1318387 (E.D.N.Y. May 15, 2006) (finding emails an employee sent while working at home to her attorney on a company issued laptop via the employee's personal email account were privileged).

which then allows the employer to view the employee's page, these risks accompany the access to information. Religious affiliations, political views, medical status, sexual orientation, and other protected information may all be accessible on an employee's social network page. While these employees cannot claim a reasonable expectation of privacy if they friend an employer who sees the information, the law still precludes employers from making employment decisions based on this information even if it is widely available. For example, information about a criminal past, short of a conviction, or medical or financial problems that could potentially impact job performance are shielded from any adverse employment decisions. Furthermore, the discovery by an employer of an employee's medical condition (for example, on Facebook) puts the employer on notice that the employee is protected under the Americans with Disabilities Act and should be offered reasonable accommodation. Finally, an employee may feel compelled to accept a boss's or supervisor's friend request, and this could be considered coercion.<sup>17</sup>

The combined challenges of blogging and social networking and the potential for employer liability provide good reasons for employers to review their acceptable-use policies. Because technology has advanced, company policies must advance.

### **[A] Liability for Hiring Decisions**

Many employers now use Facebook, MySpace, LinkedIn, and other social networking sites as part of the vetting process for new hires. As long as the information they use is in the public domain, employment decisions can be based on this information. However, an employer may inadvertently discover protected information such as race, religion, or disabilities by investigating an applicant on a social networking site. If the applicant is not hired, the applicant may sue the employer alleging discrimination on one or more of these characteristics.

One way for an employer to protect itself is to thoroughly document all hiring decisions, stating the reason a particular decision was or was not made at the time it is made. Another way to combat these potential allegations is to have an employee with no authority to make hiring decisions review the applicant's online profile and provide a summary to the hiring authority that has been filtered to redact or omit protected information about the candidate. In this way, the employer can use information on the social networking site, but will not be exposed to the protected characteristics.

---

17. Caulfield, *supra* note 8; Baldas, *supra* note 8.

Other suggestions to avoid liability when using social media in hiring include the following:

- Employers should screen applicants in a uniform manner by creating a list of the social media they will search for each applicant and the lawful information about each applicant desired from the social media search. If all applicants cannot be screened using the lawful criteria because an employer does not have the time, resources, or inclination to do so, employers must be consistent, objective, and nondiscriminatory in selecting subsets of applicants to screen.
- Employers' representatives should not "friend" applicants in order to gain access to their nonpublic social networking profiles.<sup>18</sup>
- Employers that are considering making an employment decision based on information found in social media should consult with counsel prior to doing so.<sup>19</sup>

### **[B] Federal Trade Commission Issues**

Under the Federal Trade Commission (FTC) Guides regarding "endorsements and testimonials in advertising," an employer may be liable when employees comment on their employer's goods or services on social media without disclosing the employment relationship.<sup>20</sup> However, the FTC may be offering employers a safe harbor. If the employer has an appropriate policy governing social media participation by employees, clearly articulates that policy to its employees, and consistently enforces the policy, the employer may be protected from liability. The FTC claims it has brought enforcement actions against companies that fail to establish or maintain appropriate internal

- 
18. Related to this issue of "friending" applicants or even employees, two bar associations have discussed whether it is ethical for an attorney to access an adverse witness's social network profile. The Philadelphia Bar Association did not allow an attorney to ask a third party to "friend" the witness in order to gain access, but did allow the attorney to do so because it would not constitute "dishonesty, fraud, deceit, or misrepresentation." Phila. Bar Assoc., Opinion 2009-02 (Mar. 2009). The New York State Bar Association took a narrower view in allowing lawyers to access material if the profile was available to all members of the social network and the lawyer neither "friends" the party nor directs someone else to do so. N.Y. State Bar Assoc., Ethics Opinon 843 (Sept. 20, 2010).
  19. Renee M. Jackson, *Social Media Permeate the Employment Life Cycle*, NAT'L L.J., Jan. 11, 2010, available at [www.law.com/jsp/nlj/PubArticleNLJ.jsp?id=1202437746082&Social\\_media\\_permeate\\_the\\_employment\\_life\\_cycle&slreturn=1&hbxlogin=1](http://www.law.com/jsp/nlj/PubArticleNLJ.jsp?id=1202437746082&Social_media_permeate_the_employment_life_cycle&slreturn=1&hbxlogin=1).
  20. FTC Guides Concerning the Use of Endorsement and Testimonials in Advertising, 16 C.F.R. § 255.5 (2009). See generally 16 C.F.R. § 255 (2009).

procedures, but has not brought action against a company for the actions of a single employee who violated established company policy that covered the conduct.<sup>21</sup> If company policy allows employees to blog or post on social networks, but requires the post to disclose the employment relationship, or that the statement is the employee's and is not attributable to the employer, then the company appears to be shielded from liability potentially created by the online entry.

### § 12:3.7 **Privacy and Discoverability of Online Information**

Social networking sites such as MySpace and Facebook create another wrinkle in analyzing an employee's online content. Because sites provide different levels of privacy settings, it is unclear what is public information and what is private.

According to the Central District of California in *Crispin v. Christian Audigier, Inc.*,<sup>22</sup> webmail and private messaging on social networking sites are inherently private, and stored messages are not readily accessible to the public. Facebook wall postings and MySpace comments depend on the user's privacy settings. If the settings are for restricted access, then the postings and comments are private. The court determined that these communications were not discoverable due to their private nature.

However, the Southern District of Indiana found in *EEOC v. Simply Storage Management, LLC*<sup>23</sup> that a person's expectation and intent that her communications be maintained as private is not a legitimate basis for shielding those communications from discovery. While the requesting party is not entitled to access all non-relevant material on a site, merely locking a profile from public access does not prevent discovery either. The court determined that relevant, as defined by the court, private social networking site information could not be shielded from discovery because of the person's expectation and intent that the communications remain private.

- 
21. Megan J. Erickson, *Potential Employer Liability for Employee Endorsements Under FTC Guidelines*, Erickson's SocialNetworkingLawBlog.com, May 3, 2010, [www.socialnetworkinglawblog.com/2010/05/potential-employer-liability-for.html](http://www.socialnetworkinglawblog.com/2010/05/potential-employer-liability-for.html); AGC of America, *Social Networking Policy May Protect Employers From Federal Trade Commission Violations*, Feb. 17, 2010, [http://newsletters.agc.org/hr\\_labor/2010/02/17/social-networking-policy-may-protect-employers-from-federal-trade-commission-violations/](http://newsletters.agc.org/hr_labor/2010/02/17/social-networking-policy-may-protect-employers-from-federal-trade-commission-violations/).
  22. *Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965 (C.D. Cal. 2010).
  23. *EEOC v. Simply Storage Mgmt.*, 270 F.R.D. 430, 110 Fair Empl. Prac. Cas. (BNA) 49 (S.D. Ind. May 11, 2010).

State appellate courts in Minnesota and California have also weighed in on the issue. In *Yath v. Fairview Clinics, NP*,<sup>24</sup> the court of appeals in Minnesota found that a MySpace page was public because anyone could view it. Similarly, the California Court of Appeals for the Fifth District in *Moreno v. Hanford Sentinel, Inc.*<sup>25</sup> found a MySpace page to be public, even though the author's last name was not included on the page. The court found that the picture of the author in addition to her first name was enough to determine her identity. More recently, a New York state court ordered a plaintiff to turn over access to her entire Facebook and MySpace pages even though she had used strict privacy settings.<sup>26</sup>

### § 12:3.8 *Pending Issues*

The question of whether an employer can demand access to an employee's, or potential employee's, social networking profile or blog is another contentious issue. Recently, the city of Bozeman, Montana, came under fire for a policy that asked, but did not require, all job applicants to provide log-in information and passwords to social networking profiles because the public had a right to know who the city hired. The city's stance also stated that this information would be helpful for certain positions, such as child care or law enforcement.<sup>27</sup> Following widespread, nationwide opposition to the practice, the city eliminated the hiring practice.<sup>28</sup> In Mississippi, a claim alleging invasion of privacy has been filed in the Southern District of Mississippi stemming from an incident in September 2007 where a cheerleading coach demanded

- 
24. *Yath v. Fairview Clinics, NP*, 767 N.W.2d 34 (Minn. Ct. App. 2009).
  25. *Moreno v. Hanford Sentinel, Inc.*, 172 Cal. App. 4th 1125 (Ct. App. Cal. 5th Dist. 2009).
  26. *Romano v. Steelcase, Inc.*, 2010 WL 3703242 (N.Y. Sup. Ct. Sept. 21, 2010) (the court ordered the plaintiff to execute a consent form authorizing Facebook and MySpace to provide access and did not directly require the social networking sites to provide access without the executed consent). *See also* *Bass v. Miss Porter's Sch.*, 2009 WL 3724968 (D. Conn. Oct. 27, 2009) (ordering the production of the plaintiff's entire Facebook profile); *Ledbetter v. Wal-Mart Stores, Inc.*, 2009 WL 1067018 (D. Colo. Apr. 21, 2009) (denying plaintiff's motion for protective order regarding his Facebook, MySpace, and Meetup.com content).
  27. Ki Mae Heussner, *Montana City Asks Job Applicants for Online Passwords*, ABCNews.com, June 19, 2009, <http://abcnews.go.com/Technology/JobClub/story?id=7879939&page=1>.
  28. Martha Neil, *Mont. Town Rescinds Rule Requiring Job Seekers to Reveal Social Web Passwords*, ABAJournal.com, June 23, 2009, [www.abajournal.com/news/article/mont.\\_town\\_rescinds\\_rule\\_requiring\\_job\\_seekers\\_to\\_reveal\\_social\\_web\\_passwor/](http://www.abajournal.com/news/article/mont._town_rescinds_rule_requiring_job_seekers_to_reveal_social_web_passwor/).

the log-in information and passwords of the high school's cheerleaders.<sup>29</sup> The case has not yet gone to trial.

The question of whether contact through social networks violates non-compete clauses and other restrictive covenants will also soon be addressed by the District Court of Minnesota. In *TEKsystems, Inc. v. Hammernick et al.*,<sup>30</sup> a former recruiter for TEKsystems contacted contract employees she recruited to TEKsystems about potentially working for her new employer, Horizon Integration. This case is scheduled to go to trial by August 1, 2011.<sup>31</sup>

Another pending issue will be examined when the NLRB addresses whether an employee's Facebook comments constituted concerted, protected activity. A complaint issued October 27, 2010, alleges that Dawnmarie Souza, an employee of American Medical Response of Connecticut, Inc. (AMR) was illegally terminated after posting negative remarks about her supervisor on her Facebook page.<sup>32</sup> The complaint also claims that Souza was denied union representation during an investigatory interview and that AMR's employee blogging and Internet-use policy is overly broad. The complaint stems from an incident the fall of 2009 in which AMR asked Souza to prepare an incident report concerning a customer complaint about Souza. Souza requested union representation but was denied by AMR. After going home, Souza posted negative remarks about her supervisor on her Facebook page. The remarks, which drew supportive response from co-workers and further negative comments about the supervisor, included referring to her supervisor as a "17," which was AMR's code for a psychiatric patient, and said he was being a "scumbag as usual." When co-workers asked Souza what happened, Souza stated "Frank being a dick." Souza was terminated soon after.

The NLRB alleges that AMR's termination of Souza was unlawful because her actions were concerted, protected activity and that the reason for

---

29. *Jackson v. Pearl Pub. Sch. Dist.*, 2009 WL 2474930 (S.D. Miss. Aug. 6, 2009).

30. *TEKsystems, Inc. v. Hammernick et al.*, No 0:10-cv-00819 (D. Minn.).

31. The Eastern District of Michigan addressed noncompete agreements and LinkedIn in 2008. *Kelly Servs., Inc. v. Marzullo*, 591 F. Supp. 2d 924 (E.D. Mich. 2008). In that case, Kelly Services found out, by reading his LinkedIn profile, that its former employee, Marzullo, had violated his non-competition agreement by working for a competitor in the Texas market. However, unlike TEKsystems, there was no evidence of contact with customers or sharing of trade secrets that prevented the court from finding that the confidentiality and non-solicitation agreements were violated. TEKsystems will go further and address the issue of contact through LinkedIn.

32. Complaint and Notice of Hearing, *American Medical Response of Connecticut, Inc. and International Brotherhood of Teamsters, Local 443*, Case No. 34-CA-12576 (Oct. 27, 2010).

the termination was that Souza “assisted the Union.” The NLRB also alleges that AMR’s Internet policy is overly broad and that it restricts an employee’s concerted, protected activity in violation of section 7 of the NLRA. Specifically, the NLRB claims that the following paragraph from AMR’s Blogging and Internet Posting Policy interferes with employees’ exercise of the right to engage in concerted, protected activity:

Employees are prohibited from making disparaging, discriminatory or defamatory comments when discussing the Company or the employee’s superiors, co-workers and/or competitors.

NLRB General Counsel Lafe Solomon claims that employees are allowed to discuss conditions of their employment with co-workers—at a water cooler, restaurant, or on social media. Solomon and the NLRB believe that Souza’s actions fall within this scope of protected conversation. Interestingly, AMR learned of Souza’s comments from AMR customers and not through another employee or supervisor.

AMR defends against the wrongful termination complaint by stating that Souza was not terminated only for her Facebook comments, but that AMR received written complaints from a hospital administrator, two nurses, and a patient complaining of Souza’s rude and unprofessional behavior. AMR claims that the Facebook comments violate not only the Internet policy, but also AMR’s collective bargaining agreement.

An advisory memorandum issued by the NLRB in December 2009 provides guidance regarding the lawfulness of AMR’s Internet policy. On December 4, 2009, the NLRB issued an advisory memorandum regarding Sears Holdings’ Social Media Policy. The language at issue restricted employees’ “disparagement of company’s or competitors’ products, services, executive leadership, employees, strategy, and business prospects.” The NLRB stated that the policy could not reasonably be interpreted to prohibit section 7 protected activity. Applying *Lutheran Heritage Village—Livonia*, 343 N.L.R.B. 646 (2004), the NLRB applied a two-step inquiry to determine if the employer violated section 8(a)(1). First, the rule is clearly unlawful if it explicitly restricts section 7 activity. If the restriction is not explicit, the policy violates section 8(a)(1) only if

- (1) employees would reasonably construe the language to prohibit section 7 activity,
- (2) the rule was promulgated in response to union activity, or
- (3) the rule has been applied to restrict the exercise of section 7 rights.

The NLRB stated that phrases cannot be read in isolation and that it would not find a violation simply because a rule could conceivably be read to restrict section 7 activity. The Board indicated it would look to the rule's context to determine the "reasonableness" of a particular construction. In the Sears example, the Board stated that, while the "disparagement" language quoted above could chill the exercise of section 7 language if read in isolation, as a whole, the policy's context provided guidance to preclude a reasonable employee from construing the rule as a limit on section 7 conduct. The majority of activities precluded by the policy (for example, discussing confidential or proprietary information of the company or clients, partners, vendors, and suppliers; discussing private information such as launch or release dates; company intellectual property; explicit sexual references or references to illegal drugs) were clearly not protected by section 7. The policy's preamble also stated that it was designed to protect the employer, not restrict the flow of useful and appropriate information.

The NLRB delayed a hearing on this case to allow the parties to reach a settlement, which they did on February 7, 2011. As part of the settlement, AMR agreed to revise its rules to ensure that employees are not restricted from discussing wages, hours, and working conditions with co-workers and others while not at work, and that employees would not be disciplined for such discussions.

## § 12:4 Practice Pointers

To maximize the protection from possible negative effects from employee online activity, employers should adopt clear policies governing employee conduct and obligations and directly address the issue of harmful or embarrassing Internet activity and content. What Internet policy is appropriate varies depending on the culture and needs of the employer. However, most Internet policies should contain at least the following provisions:

- (1) Blogging, social networking, and other personal Internet activity may not be done on company time or with the use of company computers.
- (2) Employees must comply with all of the company's policies, including, but not limited to, the code of conduct and the discrimination and harassment policies.
- (3) Blogs and social networking sites are individual interactions, not corporate communications, and employees must not represent or imply that they are expressing the opinion of the company. Online posts should include a disclaimer that the views expressed are those of the

individual and not the employer. Employees are personally responsible for the contents of their online profiles and blogs.<sup>33</sup>

- (4) Never disclose any confidential, trade secret, or proprietary information of the company.
- (5) A request that employees keep company logos or trademarks off their blogs and profiles and not mention the company in commentary, unless for business purposes.
- (6) A prohibition on using company email addresses to register for social media sites.
- (7) An instruction not to post or blog during business hours, unless for business purposes.
- (8) A prohibition on posting false information about the company or its employees, customers, or affiliates.<sup>34</sup>
- (9) A clear statement that misuse of social media can be grounds for discipline, up to and including termination.

Employers should send a message to employees: Respect yourself, your co-workers, and your company. Employers must impress upon employees not to put anything on the Internet that will embarrass, insult, demean, or damage the reputation of the company, its products and customers, or any of its employees. By establishing clear policies and keeping abreast of applicable law and its developments, problems with personal Internet use can be minimized to the greatest extent possible.

- 
33. The importance of a provision of this kind is underscored by a pair of cases in which Cisco Systems and one of its lawyers were sued for defamation for postings on the lawyer's blog allegedly accusing two other attorneys of criminal conduct in connection with a case against Cisco. *See Ward v. Cisco*, No. 2007-2502 (Tex. Dis. Ct. filed Nov. 7, 2007); *Albritton v. Cisco*, No. 2008-481-CCL2 (Tex. County Ct. filed Mar. 3, 2008). Soon after the suits were filed, Cisco revised its blogging policy to require all employee bloggers to include a disclaimer on their blogs that the views expressed therein are their own and not those of the company.
  34. At a Brixx Pizza in Charlotte, N.C., a waitress was fired for apparently truthfully making a post on her Facebook page that mentioned Brixx by name and complained about the tip left by "cheap" customers who stayed an hour after the restaurant closed.