Chapter 12

Employee Blogging and Social Media

§ 12:1 Introduction
§ 12:2 General Concerns with Employee Blogging and Social Networking
§ 12:3 Ownership of Business-Related Blogs and Social Media Content
§ 12:4 Laws and Regulations Governing Employee and Employer Liability
  § 12:4.1 National Labor Relations Act
    [A] Scope of Protected “Concerted Activity”
    [B] Lawful Social Media Policies
    [B][1] Recent NLRB Decisions
    [B][2] Recent Guidance from the NLRB’s Office of the General Counsel
    [C] Lawful Discipline for Violations of Social Media Policies
  § 12:4.2 Federal Trade Commission Guidelines for Employee Reviews of Company Products
  § 12:4.3 Negligent Supervision Liability for Employee Online Activity
  § 12:4.4 Whistleblowing, the First Amendment, and Retaliation
    [A] Whistleblower and Retaliation Laws
    [B] The First Amendment and Retaliation Jurisprudence
  § 12:4.5 Equal Employment Opportunity Laws
    [A] Social Media and Hiring Decisions
    [B] Discovery of Current Employees’ Protected Status or Protected Activity Through Social Media
    [C] Obligation to Rectify Complaints of Unlawful Conduct
    [D] Nondiscriminatory Investigation and Enforcement of Social Media Policies
  § 12:4.6 Restrictive Covenants
  § 12:4.7 State Laws Pertaining to Off-Duty Conduct
    [A] New York Labor Law
    [B] California Labor Law
  § 12:4.8 The Right to Privacy and the Stored Communications Act
§ 12:1 Introduction

Social networking websites such as Facebook, YouTube, Twitter, and MySpace have drastically increased the number of people participating in some mode of online forum. A social networking site is a website that provides a virtual community for people to interact for personal or business purposes, frequently featuring a profile that includes biographical data and functions that allow the user to upload pictures, videos, or other information while posting comments and thoughts. According to Facebook, as of September 2012 the social network has more than 1 billion monthly active users.\(^1\) Similarly, Twitter reported 500 million registered users.\(^2\) Twitter users “tweet” status updates and messages 230 million times per day.\(^3\)

Adding this to the population of people who use blogs shows that the overall online community is expanding exponentially. A blog (short for “weblog”) is a website featuring regular entries of commentary, descriptions of events, or multimedia. Most blogs are maintained by individuals, or a group of individuals, and they generally address specific topics or serve as personal diaries. There are more than 181 million identified blogs as of the end of 2011.\(^4\) While the percentage of bloggers under thirty years of age is dropping

Employee Blogging and Social Media § 12:2

with the increasing popularity of social networking, the combination of social networking and blogging surpassed email in popularity in 2009, with 67% of the worldwide population participating.  

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, the law is still developing in this area. State and federal employment statutes do not always explicitly regulate employees’ online activity, and the case law on the subject is not always consistent. Crafting a technology policy that addresses the challenges and potential issues presented by employee online activity is practically essential. Additionally, employers should stay apprised of further developments in this evolving area.

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

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

§ 12:3 Ownership of Business-Related Blogs and Social Media Content

One of the novel issues raised by the use of social media by businesses is ownership of content: Who owns the blog or social media—the employee or the employer?

For example, in a recently settled case in the Northern District of California, the company PhoneDog brought claims for misappropriation of trade secrets, intentional interference with prospective economic advantage, negligent interference with prospective economic advantage, and conversion against a former employee. PhoneDog v. Kravitz, No. 3:11-cv-03474 MEJ, 2011 U.S. Dist. LEXIS 129229 (N.D. Cal. Nov. 8, 2011). PhoneDog is an “interactive mobile news and reviews web resource” that “provides users with resources needed to research, compare prices, and shop from mobile carriers.” The employee worked for PhoneDog as a product reviewer and video blogger and used the Twitter account “@PhoneDog_Noah” for his employment with

---

7. For example, Taco Bell encountered a public relations nightmare when a uniformed employee posted on the company’s Facebook webpage a photo of himself licking a stack of tacos in one of the chain restaurant’s kitchens. *Taco Bell Worker Appears to Be Licking a Bunch of Taco Shells in This Facebook Picture*, HUFFINGTON POST (June 3, 2013, 9:43 AM), www.huffingtonpost.com/2013/06/03/taco-bell-worker-licking_n_3377709.html.
Employee Blogging and Social Media

PhoneDog. The employee submitted written and video content to PhoneDog, which was available to users through various media including the Twitter account. The employee also used the Twitter account to share information and promote PhoneDog’s services.

According to PhoneDog, when the employee ended his employment, PhoneDog requested the employee relinquish use of the @PhoneDog_Noah Twitter account. Instead, the employee changed the account handle to “@noahkravitz” and continued using the account. The employee claimed that “the [a]ccount, as all Twitter accounts are, is the exclusive property of Twitter and its licensors.” PhoneDog disagreed, stating that it had an “ownership interest in the [a]ccount based on the license granted to it by Twitter to use and access the [a]ccount.” PhoneDog claimed that, even if the employee created the account, PhoneDog owns it because the employee did so at the request and for the benefit of PhoneDog and used the account in the scope of his employment with PhoneDog. PhoneDog argued it had an intangible property interest in the account because the list of the account’s followers is “akin to a business customer list.” Ultimately, the case settled, so for now the questions about who owned the Twitter account remain unanswered.

A similar case in the Eastern District of Pennsylvania examined ownership of a LinkedIn account. Eagle v. Morgan, No. 11-4303, 2011 U.S. Dist. LEXIS 147247 (E.D. Pa. Dec. 22, 2011). Edcomm, Inc., which provides training to financial services companies, claimed that it had developed and maintained all connections and much of the content on the LinkedIn account through Edcomm personnel at its own expense and for its own benefit. Edcomm uses LinkedIn accounts to maintain connections and to contact instructors and specific personnel within its clients. Edcomm policy required employees to create and maintain LinkedIn accounts using their Edcomm email address, following a specific template chosen by the company, to include links to the company’s website on the page as well as Edcomm’s telephone number, and to use another Edcomm template to reply to individuals through the LinkedIn account. These accounts were monitored by Edcomm employees who corrected any violations of the policy and maintained the accounts of several employees for the benefit of Edcomm. Edcomm requested and retrieved Edcomm-related LinkedIn connections and content from departing employees’ accounts. Dr. Linda Eagle, a former employee, claimed that the LinkedIn account belonged to her. However, Edcomm claimed ownership of the account because it was used for Edcomm business and Edcomm personnel developed and maintained all connections and much of the content on her account.

The court rejected Edcomm’s claim that Dr. Eagle, by maintaining the LinkedIn account, had misappropriated Edcomm’s trade secret, because the LinkedIn account’s connections were either generally known in the wider business community or capable of being easily derived from public informa-
§ 12:4

EMPLOYMENT LAW YEARBOOK 2014

The court held a bench trial on the remaining claims in late November 2012. In March 2013, the court issued its findings of facts and conclusions of law. The court found in favor of Dr. Eagle on her claims for unauthorized use of name, invasion of privacy, and misappropriation of publicity (but not on her claims for identity theft, conversion, tortious interference with contract, or civil conspiracy). The court, however, found that Dr. Eagle failed to specify damages with reasonable certainty and, therefore, awarded her $0.00 in compensatory damages and $0.00 in punitive damages. The court noted that Dr. Eagle failed to point to a single contract, client, prospect, or deal that she had lost during the time she was without access to her LinkedIn account.

While questions of ownership of social media content await further guidance from the courts, employers can better protect themselves by addressing these issues in their social media policies and/or employee agreements, including who owns the account, its content, and the contacts and connections.

§ 12:4 Laws and Regulations Governing Employee and Employer Liability

While violations of company policy or breaches of loyalty often present clear cases, a number of statutes and legal theories may provide some protection to employees who use social media or blog on matters relating to their employment, as well as furnish defenses to employers in connection to such employee activity.

§ 12:4.1 National Labor Relations Act

[A] Scope of Protected “Concerted Activity”

Section 7 of the National Labor Relations Act, 29 U.S.C. § 157, provides:
Employees shall have the right to self-organization, to form, join, or assist labor organizations, to bargain collectively through representatives of their own choosing, and to engage in other concerted activities for the purpose of collective bargaining or other mutual aid or protection, and shall also have the right to refrain from any or all such activities except to the extent that such right may be affected by an agreement requiring membership in a labor organization as a condition of employment as authorized in section 8(a)(3) [section 158(a)(3) of this title].

Thus, section 7 of the NLRA affirms the right of employees to engage in “concerted activity,” which is the ability of employees to discuss benefits, wages, and other terms and conditions of employment among themselves 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 non-supervisory 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). Furthermore, section 8 of NLRA makes it an unfair labor practice for any private-sector employer to interfere with, restrain, or coerce employees in the exercise of their section 7 rights.

There are at least two types of situations where online communications intersect with the NLRA. First, if an employer fires or otherwise disciplines an employee for online comments that constitute “concerted activity” such as low wages, poor benefits, or long work hours, then that employee may have a viable claim against the employer under section 8 of the NLRA. Notably, however, employees’ social media posts that are unrelated to employment conditions are not protected by the NLRA. 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). Second, if the employer has a social media policy that interferes with its employees’ section 7 rights, then the policy itself may be unlawful. However, policies that do not burden protected communications about terms and conditions of employment and where the employer has a legitimate basis to prohibit the workplace communication are lawful under the NLRA.

[B] Lawful Social Media Policies

Concerned employers may have an incentive to limit employee usage of social media where it relates to their employment. An employer, for example, may elect to establish a rule forbidding employees from accessing social media websites while on duty. Such a policy, however, often does not exist in isola-
tion—it may likely include additional restrictions on the substance of social media communications. In turn, these constraints may unlawfully suppress protected activity and inadvertently cause an employer to contravene section 7 of the NLRA.

Although courts have not defined the contours of lawful and unlawful social media policies, the National Labor Relations Board (NLRB or the Board) and its Office of General Counsel have weighed in on this question over the past few years through agency decisions and various memoranda.

[B][1] Recent NLRB Decisions

In September 2012, the Board issued its first pair of decisions on the scope of protected social media communications.


In Costco, a three-member panel of the Board found that the employer’s electronic communications policy in its handbook violated the NLRA. Among the policy provisions reviewed, the Board analyzed Costco’s policy prohibiting employees from posting electronically statements that damage the company or any person’s reputation. The Board stated that the “appropriate inquiry” is whether the policy would “reasonably tend to chill employees in their exercise of their Section 7 rights[,]” which provides employees with the right to engage in concerted activity. The Board found that the policy’s broad prohibition on statements clearly encompassed concerted communications protesting Costco’s treatment of its employees. The Board also distinguished other lawful employer policies that were more tailored and prohibited clearly non-protectable communications such as malicious, abusive, or unlawful communications. Although the Board noted a previous decision that upheld a policy that prohibited “slanderous or detrimental” statements, the Board distinguished that policy because of its context: it included several other rules that prohibited egregious conduct such as “sabotage and sexual or racial harassment.” By contrast, the Board concluded that Costco’s overbroad policy had no such examples or context. Therefore, the Board found that the policy had a reasonable tendency to inhibit employees’ protected activity and thus violated the NLRA.

In *Karl Knauz*, a three-member panel of the Board affirmed the ALJ’s decision that an employer (a car dealership) may lawfully terminate an employee who posted pictures on Facebook of an auto accident at a Land Rover dealership also owned by the employer. However, a majority of the three-member panel found that the employer violated section 8 of the NLRA by maintaining a “courtesy” rule in its employee handbook. The courtesy rule stated:

> Courtesy is the responsibility of every employee. Everyone is expected to be courteous, polite and friendly to our customers, vendors and suppliers, as well as to their fellow employees. No one should be disrespectful or use profanity or any other language which injures the image or reputation of the Dealership.

Focusing on the last sentence, the Board found the courtesy rule unlawful because employees would reasonably construe its broad prohibition against “disrespectful” conduct and language to include employees’ protected statements about working conditions, protected statements seeking the support of others to improve working conditions, and criticism of the employer. The Board also found that ambiguous employer rules should be construed against the employer in order to further the NLRA’s goals.

One member of the panel dissented, stating that although the majority purported to use the correct standard, they failed to “faithfully apply it.” The dissent criticized the majority for isolating the last sentence of the “courtesy” rule without giving the preceding sentences any weight. The dissent also criticized the majority’s decision to construe ambiguous rules against the employer; the dissent argued that such construction should be limited to cases where the employer commits an explicit violation of section 7 (for example, a rule prohibiting employees from distributing literature to each other). The dissent concluded that reasonable employees would feel capable of exercising their section 7 statutory rights within the employer’s courtesy rule which was merely common sense behavioral guidance.

**[B][2] Recent Guidance from the NLRB’s Office of the General Counsel**

In an effort to provide additional guidance to employers with regard to the intersection of social media and the NLRA, the NLRB’s Office of the General Counsel (OGC) has issued three memoranda dated August 2011, January 2012, and May 2012. NLRB, Office of Gen. Counsel, Report of Acting General Counsel Concerning Social Media Cases, Memorandum OM 11-74 (Aug. 18, 2011), Memorandum OM 12-31 (Jan. 24, 2012), Memorandum OM 12-59 (May 30, 2012). The latter is available at
In each memorandum, the OGC discusses various employee scenarios and employers’ social media policies and ultimately opines whether it believes the employer’s acts and/or the employer’s social media policy to be lawful.

In the most recent memorandum, the OGC also included an example of a social media policy deemed to be lawful. The OGC opined that the rules in this sample policy sufficiently clarified and restricted their scope by including examples of clearly illegal or unprotected conduct. For instance, the policy’s rule prohibited “inappropriate postings that may include discriminatory remarks, harassment and threats of violence or similar inappropriate or unlawful conduct.” The OGC stated that the rule was lawful since it “prohibits plainly egregious conduct, such as discrimination and threats of violence, and there is no evidence that the Employer has used the rule to discipline Section 7 activity.”

As another example, the OGC considered the employer’s rule that employees avoid posts that “could be viewed as malicious, obscene, threatening or intimidating.” The policy further explains that prohibited “harassment or bullying” would include “offensive posts meant to intentionally harm someone’s reputation” or “posts that could contribute to a hostile work environment on the basis of race, sex, disability, religion or any other status protected by law or company policy.” The OGC opined that these are legitimate bases to prohibit such workplace communications, and that the policy did so without burdening protected communications about terms and conditions of employment.

As yet another example, the OGC considered the employer’s rule that employees maintain the confidentiality of trade secrets and private and confidential information. The OGC reaffirmed that employees have no protected right to disclose employer trade secrets. Moreover, the OGC noted that the rule provides sufficient examples of prohibited disclosures (namely, information regarding the development of systems, processes, products, know-how, technology, internal reports, procedures, or other internal business-related communications). To the OGC, the context and the examples were essential for employees to reasonably understand that the policy does not reach protected communications about working conditions.

In addition, it is important to highlight the OGC’s skepticism of “savings clauses” in employer social media policies. These clauses serve as disclaimers...

---

Employee Blogging and Social Media § 12:4.1

and typically inform employees that their workplace guidelines should not be construed or applied in a manner that interferes with their rights under the NLRA. The Board often finds these clauses insufficient to cure a policy’s ambiguities and to remove the chilling impact of those ambiguities upon section 7, at least in circumstances where they do not explicitly advise employees that they retain their rights to self-organize, to bargain collectively, or to engage in other concerted activities, among other things.9

Although these memoranda are not binding on employers, employers may want to consider the current views of the OGC, which has discretion to determine whether or not to bring a complaint against an employer. Moreover, the OGC appears to apply consistent principles in prosecuting a broad range of social media policies. For instance, in a 2012 advice memorandum released by the OGC pursuant to a Freedom of Information Act request, it was revealed that the OGC applied the same criteria to evaluate the legality of policies forbidding the use of an employer’s logo, trademark, or graphics as it did in evaluating the lawfulness of a policy prohibiting disclosure of confidential information.10 In one case, the OGC concluded that the employer’s ban on disclosing “nonpublic information” and “confidential information”—without further clarification of those phrases—was so vague that employees would reasonably construe it to bar discussion of working conditions or the terms or conditions of employment. Likewise, the OGC found that the blanket prohibition upon use of the employer’s logo or trademark would also be reasonably interpreted by employees to prohibit non-infringing, protected activities, such as producing leaflets or picket signs.11

In light of this guidance from the NLRB and OGC, employers should draft social media policies narrowly. If the employer wants to prohibit employees from posting certain information on social media, then it should focus on illegal conduct and conduct prohibited by other legitimate company

9. For an example of an accepted savings clause, see Advice Memorandum from Barry J. Kearney, Assoc. Gen. Counsel of the Office of the Gen. Counsel, to Daniel L. Hubbel, Reg’l Dir. Region 17 (Oct. 19, 2012) (savings clause helped to prevent an unreasonable interpretation of other ambiguous provisions where it provided that “[n]othing in Cox’s social media policy is designed to interfere with, restrain, or prevent employee communications regarding wages, hours, or other terms and conditions of employment”).


policies (for example, nondiscrimination and anti-harassment policies, policies requiring compliance with federal/state regulations, etc.). Employers should also provide specific examples, definitions, and any other context to make clear that the employer is not prohibiting conduct permitted under the NLRA.

[C] Lawful Discipline for Violations of Social Media Policies

Once an employer has drafted a social media policy, it may hold employees accountable for noncompliant conduct. However, an employer must be careful that the “noncompliant conduct” it seeks to discipline does not include protected “concerted activity” under the NLRA. To qualify as protected activity, employee action must be undertaken “for the purpose of collective bargaining or other mutual aid or protection.” 29 U.S.C. § 157. That is to say, complaints must be made on behalf of other employees or, at minimum, with the objective of inducing or preparing for collective action. Courts have not decided what qualifies as “concerted activity” in the social media context, though the NLRB has readily applied the phrase to a broad range of employee activities.


An employee tour guide was constructively discharged after he sent emails and posted messages in a Facebook group that criticized his employer’s practices and explained the advantages of union formation. It was undisputed that the employee sent his emails exclusively to former co-workers from a prior job and that he was unaware if any of his current co-workers had been members of the Facebook group in which he posted his criticisms. The Board nonetheless found that the employee had engaged in protected “concerted activity,” summarily applying an older decision’s holding that an employee who works alone in attempting to form, join, or assist a union is protected by section 7.


Hispanics United endorsed the view that merely agreeing with or “liking” a co-worker’s Facebook comment related to workplace issues is sufficient to convert an individual diatribe into “concerted activity.” Here, an employee expressed her displeasure at a co-worker’s repeated criticism by posting on Facebook that she “about had it!” and asking her “fellow coworkers[,] how do
u feel?” After several other employees commented in agreement, they were all discharged for violating an office policy against bullying and harassment. One member of the Board sought to affirm their discharge, recognizing that their communications, viewed holistically, demonstrated no intent to engage in group action—it was “mere griping, which the [NLRA] does not protect.”

Notwithstanding this observation, the other three members of the Board found the employees’ discharge unlawful under section 7, construing the initial posting as “soliciting [co-worker] views about [the] criticism” and the responsive commentary as “make[ing] common cause.” In their view, the co-workers’ discussions were “indispensable steps along the way to possible group action.”

While employers may generally discipline employees for conduct that falls beyond the NLRA’s scope, those situations—at least within the social media context—may be limited under the strict standards enforced by the NLRB.

§ 12:4.2 Federal Trade Commission Guidelines for Employee Reviews of Company Products

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. 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). However, the FTC appears to offer 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 procedures, but has not brought action against a company for the actions of a single employee who violated established company policy that covered the

12. See also Three D, LLC, d/b/a Triple Play Sports Bar & Grille, Nos. 34-CA-12915, et al. (N.L.R.B. Jan. 3, 2012) (finding act of “liking” was concerted activity because it expressed approval of employee complaints regarding payroll mismanagement).

13. See, e.g., Nat’l Labor Relations Bd. Advice Memorandum from Barry J. Kearney, Assoc. Gen. Counsel of Office of Gen. Counsel, to Dennis Walsh, Reg’l Dir. Region 4, Case 04-CA-094222 (May 8, 2013) (finding a Facebook communication was unprotected, individualized griping where employee posted that she merely recounted telling a supervisor to “back the freak off” and then typed “FIRE ME” and “Make my day”).
§ 12:4.3 Employment Law Yearbook 2014

conduct. 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.

§ 12:4.3 Negligent Supervision Liability for Employee Online Activity

Employers should remain vigilant in responding to any employee complaints regarding improper employee conduct on the Internet, including blogs or social networks. In certain circumstances, an employer may have a duty to supervise and take corrective action against employees who engage in unlawful or inappropriate activities at the workplace through their blogs or social networking sites. In an appalling set of circumstances, a New Jersey case addressed an employee who viewed child pornography, frequented adult-themed “Yahoo Groups,” and on several occasions exchanged illicit photos of his wife’s minor child with a pornography website while at work. The child and the mother sued the employer for negligent supervision, alleging that the employer should have monitored the employee’s Internet usage at work and had a duty to report him to the authorities. The Appellate Court of New Jersey held that because the employer was able to track the employee’s Internet usage (and indeed did so on a limited basis) and received credible complaints about the employee’s viewing pornography at work, it had a duty to investigate those actions and take prompt corrective action. Doe v. XYC Corp., 887 A.2d 1156 (N.J. Super. Ct. 2005).

§ 12:4.4 Whistleblowing, the First Amendment, and Retaliation

[A] Whistleblower and Retaliation Laws

As thoroughly discussed in chapter 11, 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. See chapter 11, supra, Whistleblowing and Other Retaliation Claims.

Blogging and social media impact whistleblowing and retaliation claims in at least two potential ways. First, the question exists whether posting information on a blog or social media site constitutes “blowing the whistle.” Generally, in order to invoke the protection of a whistleblower statute, the employee must first have made some report to an employer and/or a government agency. Similarly, anti-retaliation laws protect employees who report wrongdoing (such as discrimination and harassment) through internal channels. Blogging or posting about problems or violations of law, without more, may not be enough to be covered under this umbrella. Second, employees who blow the whistle may be undone by their own blogs or social media posts, undermining their credibility.\footnote{Hilary Russ, \textit{Nurses Registry Says Facebook Posts Should Kill FCA Suit}, LAW360 (July 26, 2011), www.law360.com/articles/260394/nurses-registry-says-facebook-posts-should-kill-fca-suit.}

The Tenth Circuit lately affirmed these principles in Debord v. Mercy Health Sys. of Kan., Inc., 2013 U.S. App. LEXIS 23733 (10th Cir. Nov. 26, 2013). In that case, the plaintiff contended that shortly after being hired in 2004 as a hospital technician, her supervisor began sexually harassing her by placing his hands on her body and making lewd comments or advances. The plaintiff, however, did not complain of her supervisor’s conduct until July of 2009 through a series of public messages on Facebook. In those postings, she called her supervisor a snake, exclaimed that he needed “to keep his creepy hands to himself,” and insinuated that he purposefully overpaid favored subordinates (herself, included). That supervisor saw the plaintiff’s postings and reported them to human resources, which sparked an investigation of the plaintiff’s claims. The plaintiff initially denied writing the Facebook messages, but later acknowledged her authorship.

The investigation concluded that the plaintiff’s claims were unsubstantiated, but while it proceeded, the plaintiff sent messages to other employees accusing her supervisor of destroying the evidence of his alleged misconduct. This development, along with the plaintiff’s previous transgressions, forced the hospital to discharge the plaintiff for disruptive, inappropriate, and dishonest behavior. The plaintiff brought suit alleging various theories under Title VII, including retaliation. Although she agreed that her employer stated lawful grounds for her termination, the plaintiff asserted that they were mere pretext and that the hospital’s real motivation was to punish her for complaining of sexual harassment.
§ 12:4.4  EMPLOYMENT LAW YEARBOOK 2014

The district court granted summary judgment against the plaintiff’s claims, and the Tenth Circuit unanimously affirmed. As the panel explained, the hospital presented convincing reasons for terminating the plaintiff, and her myriad arguments on appeal failed to raise a genuine dispute of material fact. Most notably, the plaintiff cited Kasten v. Saint-Gobain Performance Plastics Corp., 131 S. Ct. 1325 (2011), a case in which the U.S. Supreme Court held that the Fair Labor Standard Act’s anti-retaliation provision is triggered by an employee’s oral complaints, to support her contention that her employer’s decision to discharge her for the Facebook postings was per se unlawful because it was her method of reporting sexual harassment. The Tenth Circuit pointed out that the hospital terminated the plaintiff based on her dishonesty about writing the postings—and not for the act of airing her grievances on Facebook—but only after it repudiated the plaintiff’s reliance on Kasten. As the panel clarified, the Court reversed summary judgment against the employee in Kasten because he had orally addressed unlawful practices in accordance with the employer’s internal grievance resolution procedure; the Court, moreover, specifically observed that an employer needs notice of a complaint to discriminate upon it. The plaintiff’s Facebook postings here, in contrast, neither complied with her employer’s flexible grievance procedure, nor by themselves reached the hospital and gave it notice of any purported sexual harassment. Those postings, thus, could not qualify as protected reports or complaints.

Employers must remain aware of whistleblowers who misuse online forums as a sounding board for workplace gripes and should maintain a policy about publication of company affairs on the Internet. If an employer must discipline an employee for violating such a policy, the Debord opinion may provide it comfort in knowing that by also maintaining a reasonable policy for reporting complaints, the employer can help insulate itself from subsequent claims of retaliation.

[B] The First Amendment and Retaliation Jurisprudence

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. The breadth of online speech entitled to First Amendment protection has expanded significantly this year with the opinion of the U.S. Court of Appeals for the Fourth Circuit in Bland v. Roberts, 730 F.3d 368 (4th Cir. 2013). In Bland, the defendant sheriff of Hampton, Virginia, won his race for reelection in November 2009. During his new term, however, the sheriff declined to reappoint the six named plaintiffs as full-time employees. In 2011, these plaintiffs filed suit; several alleged
that the sheriff decided not to reappoint them based on their support of the sheriff’s opponent in the 2009 election via Facebook “likes” and comments, thereby infringing their First Amendment right to free speech.

The court ultimately decided that the sheriff enjoyed immunities against the plaintiffs’ claims for monetary damages, but not before it addressed the merits of the plaintiffs’ First Amendment arguments and found that Facebook “likes” constitute protected speech. The circuit panel opined that:

On the most basic level, clicking on the “like” button literally causes to be published the statement that the User “likes” something, which is itself a substantive statement. In the context of a political campaign’s Facebook page, the meaning that the user approves of the candidacy whose page is being liked is unmistakable. That a user may use a single mouse click to produce that message that he likes the page instead of typing the same message with several individual key strokes is of no constitutional significance.

The panel further held that “liking” a page also qualifies as symbolic expression. It reasoned that the thumbs-up symbol generated by one plaintiff’s “like” in association with the opponent’s campaign page conveyed the plaintiff’s support of the opponent’s candidacy as clearly as actual text would have. According to the court, “liking a political candidate’s campaign page communicates the user’s approval of the candidate and supports the campaign by associating the user with it. In this way, it is the internet equivalent of displaying a political sign on one’s front yard.”

Notwithstanding this development, there is some support for employers who discipline employees for legitimate business reasons. For example, in the unpublished decision Richerson v. Beckon, 337 F. App’x 637 (9th Cir. 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 entitled “What It’s Like on the Inside,” which included several highly personal and critical comments about her employer, union representatives, and fellow teachers. After the blog was discovered, several teachers and other school employees complained to the school district’s human resources director about it. 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. Richerson sued the district, alleging that her duties were reassigned in retaliation for the exercise of her First Amendment free speech rights.

The Ninth Circuit affirmed summary judgment in favor of the school district and held 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 undermined her ability to enter into trusting relationships as an instructional coach and injured the school’s legitimate interests, the balance tipped in favor of the school district.16

The Eleventh Circuit recently extended this line of reasoning to Facebook activity in Gresham v. City of Atlanta, 2013 U.S. App. LEXIS 20961 (11th Cir. Oct. 17, 2013). The plaintiff in that matter had criticized another police officer in her department for unethically interfering with an investigation. She posted those sentiments on Facebook, but the plaintiff’s action violated a rule in her department requiring that criticisms of fellow officers be directed through official department channels. The plaintiff was placed on disciplinary investigation as a result, rendering her ineligible for several open promotions. The plaintiff filed an action claiming that she was not promoted in retaliation for her First Amendment speech on Facebook.

The Eleventh Circuit disagreed, holding that the plaintiff’s speech failed the \textit{Pickering} balancing test. The panel began its opinion by highlighting the government’s legitimate interest in maintaining discipline and good working relationships among employees, and noting that comments concerning officer performance and integrity can impact confidentiality and a department’s effi-

---

16. At least two courts have recently dealt with a similar issue in the Facebook context. In the first case, a teacher expressed her frustration with her first-grade students on Facebook and suggested that they would benefit from a “scared straight program.” \textit{In re Tenure Hearing of O'Brien}, 2013 N.J. Super. Unpub. LEXIS 28 (N.J. Super. App. Div. Jan. 11, 2013). The court rejected the teacher’s contention that her comments addressed a matter of public concern, and held that even if they did, the school district’s interest in maintaining the confidence of parents in the district’s teachers outweighed the teacher’s right to express her comments. The second case produced a different result despite nearly identical facts. The teacher in that matter, like the one in \textit{O'Brien}, posted a comment on Facebook insinuating that she wanted her students to face a fate similar to one child who had drowned during a beach field trip. \textit{Rubino v. City of New York}, 2012 N.Y. Misc. LEXIS 468 (Sup. Ct. Feb. 1, 2012). A hearing officer found the teacher’s posting as unbecoming behavior and recommended termination. The New York Supreme Court disagreed, however, holding that termination was disproportionate to the offense, particularly in light of the teacher’s unblemished fifteen-year employment with the city. The court also found the penalty was inconsistent with the “spirit of the First Amendment,” though it declined to address the teacher’s free speech argument. It is worth noting, however, that the New York Appellate Division affirmed the decision without giving deference to the lower court’s First Amendment rationale. \textit{Rubino v. City of New York}, 2013 N.Y. App. Div. LEXIS 3188 (N.Y. App. Div. 1st Dep’t, May 7, 2013).
Employee Blogging and Social Media § 12:4.5

cient operation. According to the court, those legitimate interests outweighed the plaintiff’s interest in expressing her frustrations on Facebook, particularly since it was not calculated to prompt public discussion about her concerns. Furthermore, because the department’s policy was a lawful means to promote its legitimate interests, the department had acted appropriately in response to the plaintiff’s undisputed violation of that policy. Finally, the court laid to rest the plaintiff’s argument that the department’s failure to produce evidence of disruption tilted the *Pickering* analysis in her favor. The opinion noted that her public employer had no such burden to provide proof of actual disruption, and in fact, pronounced that “the reasonable possibility of adverse harm will generally be enough to invoke the full force of judicial solicitude for a police department’s internal morale and discipline” (citing Waters v. Chaffin, 684 F.2d 833, 839 (11th Cir. 1982)).

§ 12:4.5 Equal Employment Opportunity Laws

Employees who blog or post on social media sites remain protected by EEO statutes (for example, Title VII of the Civil Rights Act, state fair employment laws, etc.). The risk with the increase of social networking and other online activity is that conduct giving rise to discrimination or harassment claims can now occur through many new forums.

[A] Social Media and Hiring Decisions

Many employers now use Facebook, MySpace, LinkedIn, and other social networking sites as part of the vetting process for new hires. Browsing these sites may allow employers to gather additional information about applicants and better understand whether they fit a company’s culture. Using these sites involves various risks, however, because they may inadvertently expose an

17. Another thorny situation of a government employee exercising his free speech arose when a deputy attorney general in Indiana tweeted that riot police in Wisconsin should “use live ammunition” to handle protesters at the state capitol. He also later stated, “[y]ou’re damn right I advocate deadly force. Against thugs physically threatening legally-elected state legislators & governor?” The Office of the Indiana Attorney General reviewed the tweets and decided to terminate the employee in February 2011, justifying its actions by stating, “[w]e respect individuals’ First Amendment right to express their personal views on private online forums, but as public servants we are held by the public to a high standard, and we should strive for civility.” As of October 2013, no lawsuit has been filed regarding this matter. See *Ind. Official Who Urged “Use Live Ammunition” on Wis. Protesters Loses Job*, NBC News (Feb. 23, 2011), www.msnbc.msn.com/id/41736625/ns/us-news-life/t/ind-official-who-urged-use-live-ammunition-wis-protesters-loses-job/.
employer to information about a potential hire’s protected characteristics. That mere knowledge could form the basis of a lawsuit. By way of example, if an employer learns of a candidate’s religious affiliations, it may find itself defending a Title VII claim for failure to hire even where no animus toward the applicant’s religion motivated the employer’s decision.

Furthermore, even if their social network screening procedures are proper, employers may be required to disclose any results from the search obtained or used in employment decisions under the Federal Fair Credit and Reporting Act (FCRA) or a state equivalent, if a third party is used to conduct the screening. See 15 U.S.C. § 1681 et seq.; see also California’s Investigative Consumer Reporting Agencies Act, CAL. CIV. CODE § 1786 et seq.; New York’s Fair Credit Reporting Act, N.Y. GEN. BUS. LAW § 380 et seq.

One way for an employer to protect itself is to thoroughly document all hiring decisions, stating the reason for a particular decision at the time it is made. Another way to reduce the risk of discriminatory hiring claims is to have an employee with no authority 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. Another option is to engage a third party to review the online activity of potential employees. By outsourcing the checks, the third party will not only find the information the employer seeks, but also filter out any protected class information. Before using a third party, however, employers should keep in mind that fair credit reporting laws may apply if the third party falls within the definition of a “consumer reporting agency.” If so, then the third party may have certain licensing, training, and disclosure requirements.18

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

1. 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.

---

Employee Blogging and Social Media § 12:4.5

- Employers’ representatives should not “friend” applicants in order to gain access to their nonpublic social networking profiles.¹⁹
- Employers that are considering making an employment decision based on information found in social media should consult with counsel prior to doing so.²⁰

[B] Discovery of Current Employees’ Protected Status or Protected Activity Through Social Media

As with hiring new employees, the practice of viewing personal information about current employees through social networks and blogs carries risks. Religious affiliations, political views, medical status, sexual orientation, and other protected information may all be accessible on an employee’s social network page. While employees generally cannot claim a reasonable expectation of privacy if they “friend” an employer who sees the information or publicly post the information, employers are still prohibited from making employment decisions based on this protected information even if it is widely available. For example, information about an employee’s criminal past, short of a conviction, or medical or financial problems that could potentially impact job performance are often shielded from any adverse employment decisions.

Furthermore, the discovery by an employer of an employee’s medical condition (for example, on Facebook) may arguably put the employer on notice that the employee is protected under the Americans with Disabilities Act and should be offered reasonable accommodation.

The potential for a negative inference also exists where an employer learns of an employee’s protected activity before executing a lawful adverse employ-

¹⁹. 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 Ass’n Prof’l Guidance Comm., Opinion 2009-02 (Mar. 2009), www.philadelphiabar.org/WebObjects/PBAReadOnly.woa/Contents/WebServerResources/CMSResources/Opinion_2009-2.pdf. 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 Ass’n Comm. on Prof’l Ethics, Ethics Opinion 843 (Sept. 10, 2010), www.nysba.org/AM/TemplateRedirect.cfm?template=/CM/ContentDisplay.cfm&Section=Ethics_Opinions&ContentID=55951.

ment action. For example, the court in Deneau v. Orkin, LLC, No. 11-00455-B, 2013 U.S. Dist. LEXIS 70933 (S.D. Ala. May 20, 2013), held that the plaintiff established a prima facie case of retaliation under Title VII where she was discharged only a few days after she posted a comment on her Facebook page asking, “anyone know a good EEOC lawyer? need one now,” and the employer’s managers were aware of the posting prior to her termination. 21

[C] Obligation to Rectify Complaints of Unlawful Conduct

As mentioned above, employers may not have a strict obligation to monitor the online conduct of their employees, but they do have a duty to act when they know of or receive complaints of unlawful harassment or discrimination related to their workplace.

With regard to harassment, in an earlier case involving airline employees’ blogs, Blakey v. Cont’l Airlines, 751 A.2d 538 (N.J. 2000), the Supreme Court of New Jersey, overruling two lower New Jersey courts, 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. 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. 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.

Courts have been inclined to require similar action by employers for complaints of harassment or discrimination arising from social media forums, despite the employer’s lack of control in these situations. In Amira-Jabbar v. Travel Servs., Inc., 726 F. Supp. 2d 77 (D.P.R. 2010), a former employee recited an incident on Facebook to support a hostile work environment cause of action. After a company outing, the plaintiff’s co-worker posted a photo on the social network that precipitated an allegedly racist remark in the comments section. The court granted the employer’s motion for summary

21. See also Gaskell v. Univ. of Ky., 2010 U.S. Dist. LEXIS 124572 (E.D. Ky. Nov. 23, 2010) (denying motion for summary judgment on plaintiff’s Title VII claim of religious discrimination where defendant’s discovery of plaintiff’s religious views through his personal website raised a triable issue as to whether those religious beliefs were a motivating factor in not hiring plaintiff).
judgment. The court first held that the isolated instances of harassment cited by plaintiff, including the Facebook comment, simply could not sustain a hostile work environment claim. The court further held that the employer could not be liable for the actions of plaintiff’s co-workers because it had satisfied its duty upon receiving the plaintif’s complaint: The employer conducted an investigation of the wrongful acts, reviewed anti-harassment policies with employees, and blocked every work computer’s access to Facebook.

[D]  Nondiscriminatory Investigation and Enforcement of Social Media Policies

In addition to the above, employers who investigate and reprimand employees for personal blogs or social networking sites must be sure to conduct such investigations and take responsive actions in a nondiscriminatory manner to avoid 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 with the Equal Employment Opportunity Commission and a multi-million-dollar lawsuit against Delta. Although the employer contended that the termination was due to the employee’s misuse of the company’s uniform, the plaintiff alleged that other employees, primarily men, posted photographs of themselves in uniform on the Internet without incident. Simonetti v. Delta Airlines, Inc., No. 05-2321 (N.D. Ga. filed Sept. 7, 2005). Ultimately, the case was dismissed for administrative reasons.

§ 12:4.6  Restrictive Covenants

Another legal question related to the use of social media in hiring and recruiting is whether contact through social networks violates non-competition agreements and other restrictive covenants. This is another example of the intersection between new technology and traditional legal theories that the courts are just beginning to address. In TEKsystems, Inc. v. Hammernick et al., No 0:10-cv-00819 (D. Minn. Mar. 16, 2010), a company brought an action against its former employee in the U.S. District Court for the District of Minnesota regarding whether a former recruiter for TEKsystems violated her post-employment non-competition agreement by contacting contract employees she recruited to TEKsystems about potentially working for her new employer, Horizon Integration. The case settled in 2010 prior to any decision.

The Eastern District of Michigan has also addressed non-compete agreements. In Kelly Servs., Inc. v. Marzullo, 591 F. Supp. 2d 924 (E.D. Mich. 2008), Kelly Services found out, by reading the LinkedIn profile of former
employee Marzullo, that 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. As a result, the court did not find that the confidentiality and non-solicitation agreements were violated.

Two years later, the U.S. District Court for the Eastern District of Michigan examined whether individuals who were part of a network of hundreds of thousands of independent business owners (IBOs) and sold products for Amway Corporation had violated a non-solicitation rule by encouraging other IBOs to compete with Amway. Amway Global v. Woodward, 744 F. Supp. 2d 657 (E.D. Mich. 2010). The court upheld an arbitrator’s decision that the defendant IBOs did solicit other IBOs to join a competitor, most notably through a blog entry describing one IBO’s reasons for making the switch and stating, “[i]f you knew what I knew, you would do what I do.” In finding that this conduct violated the non-solicitation agreement between the IBOs and Amway, the court found that the substance of the message and the medium through which it was transmitted were determinative of whether the communication was a solicitation. The court further reasoned that communications qualifying as solicitations do not lose that status merely because they are made on the Internet. Further, the possibility that no one would actually read the online solicitation does not affect its status as a solicitation.

§ 12:4.7 State Laws Pertaining to Off-Duty Conduct

Some states, notably New York and California, have off-duty conduct statutes. CAL. LAB. CODE §§ 96(k), 98.6; N.Y. LAB. LAW § 201-d. In addition to New York and California, similar statutes have been enacted in Colorado and North Dakota. COLO. REV. STAT. § 24-34-402.5(1); N.D. CENT. CODE § 14-02.4-03. These laws limit the ability of an employer to deny employment to, or 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.

[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 televi-
sion, 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).

However, 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. 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.


Given the narrow scope of the statute, it is unclear whether blogging or social networking without more would be protected under the statute as a recreational activity. Therefore, 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
§ 12:4.7 EMPLOYMENT LAW YEARBOOK 2014

California’s Labor Commissioner to pursue these claims on an employee’s behalf. CAL. LAB. CODE §§ 96(k), 98.6.

Although the language of section 96(k) appears broad, it 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.” Barbee v. Household Auto. Fin. Corp., 113 Cal. App. 4th 525, 533–34 (2003); see also Grinzi v. San Diego Hospice Corp., 120 Cal. App. 4th 72 (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).

Whether or not blogging and social networking are protected under California’s “lawful conduct” statute therefore turns on whether employee discipline or termination would impinge on constitutional rights. Perhaps the most obvious right, 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, 111 Cal. Rptr. 2d 336, 26 Cal. 4th 1013, 1031 (Cal. 2001). However, privacy rights are enforceable against private actors and could affect employer liability.

Although section 96(k) was not expressly at issue, there is at least one example of a California court upholding an employer’s decision to terminate an employee based on his off-duty conduct. In San Diego Unified Sch. Dist. v. Comm’n on Prof’l Competence, 124 Cal. Rptr. 3d 320 (Cal. Ct. App. 2011), a school district suspended and served a notice to terminate a dean of students for soliciting sex on Craigslist via a posting that included explicit and pornographic pictures of himself. The dean removed the ad upon notification and argued that he did not intend students to see it and that parents should be monitoring their children’s Internet activities. Both the Commission on Professional Competence and the trial court (who reviewed the commission’s decision) found no cause for dismissal existed because, although “this sexually explicit ad was vulgar and inappropriate and demonstrated a serious lapse in good judgment,” the school district failed to prove any nexus between the ad and the employee’s employment. However, the California Court of Appeal reversed. Although the court found that the employee did not use school time, resources, or equipment to post the ad and that the employee did not intend any student to view it, the court determined that the employee’s actions demonstrated “evident unfitness to teach” and that he had engaged in immoral conduct under California Education Code section 44932, either of which was enough to warrant termination by itself. Although section 96(k)
was not expressly at issue, this case provides some support for an employer’s
decision to terminate an employee based on his or her off-duty conduct
involving social media use.

§ 12:4.8 The Right to Privacy and the Stored
Communications Act

Although more thoroughly discussed in chapter 8, both federal and state
law define when employees have a reasonable expectation of privacy in their
use of social media and blogs. Additionally, 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 under the federal Stored Communications Act (SCA), a statute that
has spawned a new realm of litigation with the growing use of social media in
business.

In Pietrylo v. Hillstone Rest. Grp., No. 06-5754 (FSH), 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 Hill-
stone 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 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 autho-
rized was supported by evidence that the employee who turned over the log-
in and password information was coerced into providing the information.

A New Jersey federal district court has found that the SCA also applies to
privately held data maintained on Facebook. Ehling v. Monmouth-Ocean
a registered nurse, had posted a comment on her Facebook wall implying that
paramedics who arrived at the scene of a museum shooting should have let the
felon die. The plaintiff had made her account visible to only her friends, but
unbeknownst to the plaintiff, one of those Facebook “friends”—a co-
worker—transmitted snapshots of her postings to management. The plaintiff
was suspended as a result. She filed suit two years later, alleging that the
employer improperly accessed her Facebook account in violation of the SCA and her right to privacy, in addition to other causes of action.

The employer successfully moved to dismiss those claims. While the court found that the plaintiff’s efforts to maintain the private nature of her Facebook account entitled it to protection under the SCA, the alleged wrongful conduct for which she sought redress fell within an exception precluding her employer's liability. As the court pointed out, the plaintiff authorized her co-worker’s access to her Facebook wall with the intent of communicating her updates. And because the co-worker voluntarily provided screenshots to her employer, the employer did not violate the SCA. Indeed, the very fact that her employer was merely a “passive recipient[ of information” was also fatal to her claim for invasion of privacy.

Maremont v. Susan Fredman Design Grp., Ltd., No. 10-C-7811, 2011 U.S. Dist. LEXIS 140446 (N.D. Ill. Dec. 7, 2011), yet another case involving similar causes of action, highlights the hurdles that employees must overcome to wage a successful privacy-related claim. The plaintiff in Maremont alleged that her employer made business-related postings to her personal Twitter and Facebook accounts while she remained on medical leave. The plaintiff had stored her access information for those accounts on the employer’s servers, but she never gave anyone explicit authority to access her accounts, and the employer failed to stop posting on them despite her request to do so.

The plaintiff later sued her employer under various theories, including violations of the SCA and breach of privacy. On cross-motions for summary judgment, the court allowed the plaintiff’s SCA claim to move forward, finding unanswered questions with respect to whether plaintiff suffered actual injury as a result of the employer’s SCA violation and the extent to which the employer had been authorized to post on her social media accounts. As for plaintiff’s privacy claim, it was dismissed. The court noted that the plaintiff had approximately 1,250 subscribers to her Twitter and Facebook postings—a broad online following, which left no dispute that the contents of her accounts were public; plaintiff, therefore, did not identify any private content breached by her employer.

To address these privacy issues, 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 and social media postings are unlikely to be the subject of any privacy protection, stored or archived material on a work computer could potentially qualify.

For further discussion of how privacy rights may impact social media use, see chapter 8, Employee Privacy Law.
§ 12:4.9 New Laws Prohibiting Employers’ Access to Employees’ Social Media Accounts

Whether an employer can demand access to an employee’s, or potential employee’s, social networking profile or blog has been the subject of recent debate and legislative activity.

In 2009, 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. Following widespread, nationwide opposition to the practice, the city eliminated the hiring practice.

In 2011, a job applicant applying for a position with the Maryland Department of Corrections was required to undergo a background investigation. Part of that investigation included providing the department with the applicant’s Facebook log-in and password to permit the interviewer to review the applicant’s Facebook profile and postings. While the Maryland Department of Public Safety and Correctional Services (DPSCS) denied that a log-in and password were required for employment, the applicant stated he was informed the requirement was department policy. The ACLU sent a letter to the DPSCS requesting this practice be suspended indefinitely. In response, the DPSCS agreed to temporarily suspend the process of asking applicants for social media information, agreed that an applicant’s refusal to provide log-in and password information would not be grounds for disqualification, but reserved the right to inquire about a candidate’s Facebook account.

Prompted by the nationwide publicity of these and other cases, several states, including California, passed legislation in 2012 and 2013 that bars employers from requesting that current and/or prospective employees provide account information for social media site access. The California statute, for

example, specifically prohibits an employer from requiring or requesting an employee or applicant for employment to disclose a user name or password for the purpose of accessing personal social media in the presence of the employer, or to divulge any personal social media. In addition, the statute prohibits an employer from discharging, disciplining, threatening to discharge or discipline, or otherwise retaliating against an employee or applicant for not complying with a request or demand by a violating employer. However, employers may request social media reasonably believed to be relevant to an investigation of allegations of employee misconduct or an employee violation of law. Other states have opted to promulgate statutes with similar provisions banning demands for user name or password information; additional proscriptions against employer requests to be added as a social media contact; or broad language prohibiting coerced access by an employer generally. The Vermont legislature, meanwhile, has elected to commission a study of social network privacy in the workplace before taking further action.

Similar legislation was introduced on the federal level to regulate employer access to employee and applicant account information. The Password Protection Act of 2012 was introduced in the U.S. Senate to prohibit employers from compelling or coercing disclosure of private user information to gain access to private social media accounts as a condition of employment. The bill also sought to prohibit employers from discriminating or retaliating against a prospective or current employee due to a refusal to comply with an employer’s request for access. Likewise, the Social Networking Online Protection Act was introduced in the House to prohibit employers and universities from requiring employees or students to provide access information to personal email or social media accounts. Both bills expired after being referred to committees, but have since been reintroduced. It remains to be

seen whether these incarnations will muster as much support as their state counterparts.

Facebook has also weighed in and is warning employers not to ask job applicants for their passwords and threatening legal action to enforce its policy against sharing passwords.\footnote{34}

\section*{§ 12.5 Utilizing Social Media in Litigation}

\subsection*{§ 12.5.1 Scope of Discoverability of Blogs and Social Media}

Based on the wealth of information available on blogs and social networking sites, it comes as no surprise that these sites have discoverable information. Employers in litigation should consider sending a preservation notice to opposing counsel that includes a request to preserve such information and include such information in their own data preservation policies. For example, company-issued computers, phones, or other devices may contain a user's blog and/or social networking information.

Courts, however, are still sorting out the extent to which blogs and social networking information are discoverable in litigation. Many courts take an expansive view and find social networking sites are generally discoverable, notwithstanding any "private" or restricted settings. For example, in 2010, 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. Romano v. Steelcase, Inc., 907 N.Y.S.2d 650 (N.Y. Sup. Ct. 2010). The plaintiff alleged in a personal injury action that her injuries prevented her from participating in certain activities and affected her enjoyment of life. However, public pictures on social media sites showed her participating in an active social life and traveling to other states, contrary to her assertions that her injuries prohibited travel. Defendant moved to compel production of the "private" or restricted portions of her social networking sites. In granting the request, the court dismissed plaintiff’s privacy concerns because social networking sites have policies that state the information is in public space, and indeed the “very purpose” of social networking sites is to share information with others.\footnote{35}


\footnote{35. 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 plaintiffs’ motion for protective order regarding their Facebook, MySpace, and
Some cases take a more restrictive approach and find that social media sites with restricted access are not discoverable. See Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965 (C.D. Cal. 2010) (finding Facebook and MySpace messages with restricted access were not discoverable due to their private nature).

Other courts take a more nuanced approach to discovery of social networking sites, carefully scrutinizing whether the underlying information is relevant. For example, in Mailhoit v. Home Depot USA, Inc., No. CV-11-03892, 2012 WL 3939063 (C.D. Cal. Sept. 7, 2012), the defendant in an employment lawsuit sought several categories of social media communications related to plaintiff, including social networking posts about plaintiff’s emotions, posts to place plaintiff’s own communications “in context,” employment-related posts, and all pictures on her profile or tagged during the relevant time period. Although the court recognized that social networking sites are generally subject to discovery, the federal rules still required “a threshold show that the information is reasonably calculated to lead to the discovery of admissible evidence.” Therefore, the court found three of the four categories overbroad but approved the defendant’s request for employment-related social media communications, specifically communications between plaintiff and any current or former employee of Home Depot, or which in any way refers to her employment at Home Depot or the lawsuit.  

Meetup.com content); Zimmerman v. Weis Mkts., Inc., 2011 Pa. Dist. & Cnty. Dec. LEXIS 187 (Pa. Ct. C.P. May 19, 2011) (finding that because plaintiff voluntarily posted all of the pictures and information on social media sites to share with other users, he had no reasonable expectation of privacy; social networking site is, by definition, the “interactive sharing of your personal life with others”); McMillen v. Hummingbird Speedway, Inc., 2010 Pa. Dist. & Cnty. Dec. LEXIS 270 (Pa. Ct. C.P. 2010) (unrealistic for a person to believe that disclosures made to others on social media sites would be considered confidential and remain private because the goal of the sites is to connect with others); Patterson v. Turner Constr. Co., 931 N.Y.S.2d 311 (N.Y. App. Div. Oct. 27, 2011) (finding that discovery of relevant posting on plaintiff’s online Facebook account was not protected from discovery simply because privacy settings were used to restrict access); Largent v. Reed, No. 2009-1823 (Pa. Ct. C.P. Nov. 8, 2011) (finding plaintiff’s Facebook account was discoverable due to pictures and status updates contradicting her injury claims; “only the uninstructed or foolish could believe that Facebook is an online lockbox of secrets”).

See also Tompkins v. Detroit Metro. Airport, 278 F.R.D. 387 (E.D. Mich. 2012) (acknowledging that material posted on Facebook is neither privileged nor protected by a right to privacy, but finding that the defendant does not have a “generalized right to rummage at will through information”); McCann v. Harleysville Ins. Co. of N.Y., 78 A.D.3d 1524 (N.Y. App. Div. 2010) (upholding the denial of a motion to compel Facebook information, because the defendant failed to establish
Mailhoit appears to be part of a common, if not prevailing, trend in which judges approach social media discovery on a case-by-case basis, often demanding that parties submit tailored requests for production or employing creative methods for resolving disputes. The court in EEOC v. Original Honeybaked Ham Co. of Ga., 2012 U.S. Dist. LEXIS 160285 (D. Colo. Nov. 7, 2012), for example, initiated a procedure whereby social media content was reviewed in camera by a forensic expert for relevance before being produced. The employer in that matter sought to uncover electronic communications shared among the class members, many of which were made using social media channels such as Facebook. While the court viewed the claimants’ volitional conduct in “creating relevant communications and sharing them with others” as raising a “strong argument” in favor of production, it also acknowledged the privacy concerns implicated by the employer’s broad requests. An in-camera inspection, thus, provided a compromise to achieve the parties’ competing interests.

§ 12:5.2 Methods of Discovering Blogs and Social Media

During litigation, employers are likely to be more successful obtaining social networking information from individual users rather than third-party providers. This is because some courts interpret the Stored Communications Act to find that it may not enforce subpoenas to third-party providers. A basis for relevancy of the evidence and instead was seeking to conduct a fishing expedition into plaintiff’s Facebook account); Offenback v. L.M. Bowman, Inc., 2011 WL 2491371 (M.D. Pa. June 22, 2011) (granting the defendant access to relevant information on the plaintiff’s Facebook and MySpace pages during an in camera review; questioning whether it was necessary for it to review the online “private” information).

37. See, e.g., Reid v. Ingerman Smith, 2012 U.S. Dist. LEXIS 182439 (E.D.N.Y. Dec. 27, 2012) (electing not to require full disclosure of all materials contained in plaintiff’s social media accounts because not all of the information would be relevant); Giachetto v. Patchogue-Medford Union Free Sch. Dist., 293 F.R.D. 112 (E.D.N.Y. May 6, 2013) (holding that routine status updates on social networking sites were not relevant to plaintiff’s claim for emotional distress, but that postings related to the emotional distress alleged were relevant and discoverable); Robinson v. Jones Lang LaSalle Ams., Inc., 2012 U.S. Dist. LEXIS 123883 (D. Or. Aug. 29, 2012) (granting a motion to compel in part to facilitate discovery of social media activity that could demonstrate the degree to which plaintiff experienced alleged emotional distress); Caban v. Plaza Constr., 41 Misc. 3d 1205(A) (Sup. Ct. N.Y. Sept. 24, 2012) (denying with prejudice motion seeking a compressed file of plaintiff’s social media accounts subject to a new demand with more specific identification of relevant social media data).
providers for user information. See, e.g., Crispin, 717 F. Supp. 2d 965 (finding that Facebook and MySpace are electronic communications services providers under the Stored Communications Act). However, employers can still rely on traditional forms of discovery to obtain user’s social networking information, and some providers are enabling employers to do so. For example, Facebook announced a feature called “Download Your Information,” where users can download all information ever uploaded into their Facebook account, including their profile, friend list, notes, events, photos and videos, wall posts, and sent and received messages and comments. This “Download Your Information” feature should allow employers in litigation to request Facebook information easily by requesting all documents accessible through the user’s “Download Your Information” feature. Furthermore, because of the simplicity of the download feature, employers should be able to successfully resist arguments that retrieving such data is overly burdensome.

Facebook also recently unveiled its “Timeline” feature, which allows users to (1) keep a historical record of everything they have done on Facebook, and (2) compile a catalog of everything the user is interested in. This new feature further increases Facebook’s potential as a discovery engine for attorneys and others interested in the information. The enhancements to users’ profiles allow Facebook and its users to compile a mini encyclopedia about users and the users’ interests. The Timeline information will enable users to flip through wall posts and other actions and will be organized by year. Moreover, users can go back into their timeline and fill in past details and events, and users’ friends can see comprehensive summaries of their friends’ profiles. Notably, any additions made retroactively to a picture or previous status will appear under the prior year in Timeline. For example, if a user comments in 2012 on a picture initially posted in 2002, the new comment from 2012 will appear in 2002 on Timeline. Though metadata will show when the new information was actually posted, this may result in increased time and cost to attorneys analyzing the Facebook posts in an effort to prevent litigants from

38. Download Your Information from Facebook, YouTube (June 5, 2011), www.youtube.com/watch?v=Gk16FRAdUJk.
42. Sullivan & Newman, supra note 40.
43. Ryan, supra note 41.
posting comments retroactively in an effort to improve their case. This further increases the wealth of information available on social networking sites that may be subject to discovery.

§ 12:5.3 The Importance of Prompt Discovery Notices

Social media provides such significant leverage in litigation that a party that fails to preserve relevant data may be subject to considerable penalties. The personal injury plaintiff in Gatto v. United Air Lines, Inc., 2013 U.S. Dist. LEXIS 41909 (D.N.J. Mar. 25, 2013), learned this lesson after neglecting to recover his deactivated Facebook account. Per court order, the plaintiff in that case had agreed to change the password on his Facebook account in order to give the defendants access to his profile. When the defendants subsequently used the furnished password, Facebook alerted the plaintiff that an unfamiliar IP address had accessed his account. As a result, plaintiff’s counsel contacted defense counsel, who confirmed that they—and not an unauthorized user—were responsible for the warnings.

Despite receiving affirmation that his account had not been compromised, the plaintiff still deactivated his Facebook profile on the basis of those alerts. By the time plaintiff’s counsel advised defense counsel of this development, Facebook’s purported practice of automatically deleting accounts fourteen days after deactivation had already taken effect, rendering the plaintiff’s former account irretrievably lost. Asserting that the lost account contained relevant data that contradicted the plaintiff’s claims and deposition testimony, the defendants filed a motion for sanctions that included a trial instruction for the jury to draw an adverse inference against the plaintiff for failing to preserve his Facebook account.

The court held that the plaintiff’s failure to preserve his Facebook account warranted the adverse inference (or “spoliation instruction”) because:

1. the account was within his control;
2. the destroyed evidence was relevant to the parties’ claims or defenses;
3. it was reasonably foreseeable that his account would be discoverable; and
4. the evidence in the account had actually been suppressed.

Notably, in reaching this conclusion, the court found it immaterial whether or not the plaintiff had unintentionally deprived the defendants of evidence. According to the court, the spoliation inference serves a remedial function that remains operative so long as the suppressed evidence was relevant. Moreover, the court held that even if the plaintiff did not intend to deprive the defendants of relevant data, it was undisputed that he acted intentionally when
he deactivated his Facebook account and failed to reactivate it within fourteen
days.

Gatto highlights the duty of plaintiffs to preserve their social media
accounts, as well as the need of employers to serve related discovery requests
promptly. Once an employee is put on notice of his obligation to preserve
relevant evidence, any subsequent misconduct in suppressing information will
provide employers with grounds for seeking sanctions.

§ 12:5.4 Limitations on Attorney Research Using Blogs
and Social Networking Sites

While social networking provides new avenues for discovery and research,
attorney ethical restraints remain in place. States prohibit attorneys from using
dishonesty, fraud, deceit, or misrepresentation to discover information from
blogging or social networking sites. For example, the Philadelphia Bar Associa-
tion did not allow an attorney to ask a third party to “friend” the witness in
order to gain access to the individual’s social network profile, but did allow the
attorney to do so because it would not constitute “dishonesty, fraud, deceit, or
York State Bar Association took a similar view in allowing lawyers to access
material only if the profile was available to all members of the social network
“public” and the lawyer neither “friends” the party nor directs someone else
to do so. N.Y. State Bar Ass’n, Ethics Op. 843 (Sept. 20, 2010). The New
York Bar Association opinion was aimed at preventing the use of deception to
obtain information such as attempting to “friend” a witness or adversary
under false pretenses.

Similarly, recent decisions have granted attorneys permission to investigate
jurors and potential jurors using the Internet and social media sites so long as
they do not communicate with them. For example, the New York City Bar
Association issued an ethics opinion addressing when an attorney may
research potential or sitting jurors through social media websites. The
opinion provides that attorneys may conduct research on jurors, but may not
make any communication with them. The opinion defines prohibited
conduct in the context of social media to include any communication that
makes a juror or potential juror aware of the attorney’s viewing or attempted
viewing of the juror’s personal social media page. Even an unintentional
contact may qualify as a violation. Further, while an attorney may view public

44. N.Y. City Bar Ass’n, Formal Op. 2012-2: Jury Research and Social Media (2012),
available at www.nycbar.org/ethics/ethics-opinions-local/2012opinions/1479-
formal-opinion-2012-02.
information on jurors, attorneys may not engage in, or employ others to engage in, deceptive practices when researching to gain more information on jurors.

§ 12:5.5 Publicizing Litigation Proceedings via Blogs and Social Networks

With the advent of blogs and social networking sites, neither employees nor employers can rely on court proceedings with incendiary allegations remaining anonymous. With technology today anyone can quickly share court documents and testimony to the entire world, just by sitting in the audience with a smartphone. For example, even though the Northern District in California prohibited cameras in the courtroom for the Proposition 8 trial, numerous sources were tweeting the exact words from the proceedings in real time. Likewise, on appeal, documents posted on PACER are quickly disseminated to groups all across the country within a matter of minutes.

Similarly, blogs and social networking sites present special risks for employers who are currently in trial. Jurors may publish highly sensitive information presented in court, make disparaging comments about counsel and clients, attempt to improperly contact witnesses, attorneys or judges, and/or prematurely post verdicts. Parties should consider such risks before any case goes to a jury trial and prepare specific jury instructions prohibiting jurors from using social networks improperly during jury service.45 Furthermore, the publicity risks of a full-blown trial, whether positive or negative, have grown exponentially with social networking.
