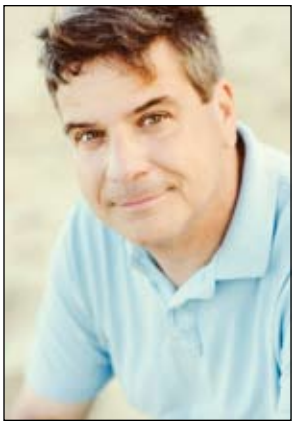
Hiring And Firing In The Facebook Age (With Sample Provisions)



William C. Martucci

Jennifer K. Oldvader

William C. Martucci and **Jennifer K. Oldvader** are national litigators in the National Employment Litigation and Policy Group at Shook, Hardy & Bacon, L.L.P. ,in Washington, D.C. and in Kansas City, Missouri. Mr. Martucci and Ms. Oldvader practice nationally on behalf of corporate employers in employment litigation, complex class action (employment discrimination and wage & hour) litigation, EEOC litigation, and unfair competition litigation. ***Chambers USA America's Leading Lawyers for Business*** stated that "Bill Martucci is worth having on any dream team for employment litigation and policy issues." **Justin Smith,** a 2009 Summer Associate at Shook, Hardy & Bacon assisted with this article.

William C. Martucci, Jennifer K. Oldvader, and Justin D. Smith

Easy access to a lot of information about employees can prove to be a double-edged sword for employers.

THERE ONCE was a time before the Internet. A time when private thoughts were preserved only in private diaries. A time when job complaints were uttered only in small groups of private conversations. A time when conversations were recorded only by the memories of those present. Those days are in the distant past.

Now information flows freely at the click of a mouse. Employees can complain about their jobs almost instantly through tweets or posts to Facebook or MySpace They can chronicle their lives in a publicly accessible manner by blogging; or upload obscene or embarrassing photos via any number of social networking sites. Technology connects — and exposes — us like never before.

These uses of the Internet continue to grow at astronomical rates. A new blog is created every 1.5 seconds. Twitter has grown by more than 1,000 percent in the last year. Time spent on Facebook has increased just under 700 percent in the last year to 13.9 billion minutes a month, by more than 100 million different monthly visitors. A new information medium is all that likely could slow down this rapid expansion of online activity.

This exponential growth has significant consequences for the workplace. When employees regularly access social networking sites at work (and multiple surveys indicate a large percentage of workers are), employers may experience a significant drag on productivity. There are also risks that employees may reveal trade secrets, harass their co-workers, criticize their supervisors, or simply discuss politically- or morally-charged topics in a manner that may be linked with the company. With all of these possibilities and more, it is not surprising that, in a 2007 nationwide survey from the American Management Association and ePolicy Institute, one-third of employers reported that they had fired an employee for misusing the Internet.

What is surprising, perhaps, is how few employers have responded by adopting appropriate Internet and/or Social Networking Use Policies. In a 2009 study by Deloitte LLP, 23 percent of employees reported that their employer had no policy about using social networks while at work. Another 24 percent did not know if there was a policy or not, and 11 percent knew a policy was in place, but did not know what it was. Thus, more than half of employees did not know what conduct was permissible online.

This article begins by addressing the employment law risks presented by social networks and blogs, including the risks inherent in using information found on such sites to make employment decisions. The remainder of the article is dedicated to providing best practice tips for drafting an appropriate Internet and Social Networking Usage Policy.

HIRING IN THE FACEBOOK AGE • Thanks to Google, Facebook, and a host of other social networking media, employers have access to more information when making hiring decisions than ever before. According to a Ponemon Institute study, one in three hiring managers search Google for information on job applicants. One in five search social networks. Overall, approximately one-third of Google and social network searches lead to rejections of the applicant, and the uncovered information influences more than 60 percent of employers when making the hiring decision.

Some employers now require applicants to disclose any blogs, aliases, or social networking use on their job applications. For example, the Obama administration required applicants to disclose any blog posts, aliases used when writing online, and links to their Facebook pages. Other employers ask for disclosure during the interview. According to a spokesman for the Missouri State Teachers Association, at least one Missouri superintendent interviewing teacher applicants asked if they had a Facebook or MySpace page. If the applicant said yes, the superintendent would propose looking at the page right then.

Danger: Invasion Of Privacy

Despite the wealth of information made available by the Internet, employers must proceed with caution before searching Google and social networks for information on job applicants, ensuring that any such searches conform with applicable laws. For example, if an employer accesses an applicant's "private" social networking account, the potential employee could make a common law invasion of privacy claim. To prevail on such a claim, a plaintiff must generally prove that the information obtained by the employer was in fact private. Information posted on a MySpace or Facebook page, accessible to the world at large, would likely not be considered private. *See Sandler v. Calcagni,* 565 F. Supp. 2d 184, 196 (D. Me. 2008); *Moreno v. Hanford Sentinel, Inc.,* 91 Cal. Rptr. 3d 858, 862 (Cal Ct. App. 2009). However, when the applicant has limited the accessibility of the information to only "invited" friends or guests, and the employer somehow circumvents this accessibility limit, the applicant may have a stronger claim. *See Pietrylo v.*

Hillstone Restaurant Group, 2009 WL 3128420 (D.N.J. June 16, 2009).

Danger: Discrimination

Unlawful discrimination is perhaps a more viable claim. Title VII prohibits employers from refusing to hire an applicant based upon his or her race, color, religion, sex, or national origin. 42 U.S.C. §2000e et seq. The Age Discrimination in Employment Act, 29 U.S.C. §623 et seq., affords the same protection based upon a person's age, as does the Americans with Disabilities Act for those with disabilities, 42 U.S.C. §12112 et seq. State law might provide further protections. Many employers go to great lengths to keep information regarding an applicant's membership in certain protected classes away from their decision makers, even if the information is otherwise maintained for affirmative action purposes. However, one simple Google search could undermine any such efforts made by a company. By visiting an applicant's Facebook page or using Google, an employer very well could learn the applicant's race, gender, age, or the existence of a disability from pictures or other posted information. Making an employment decision based on this information could result in liability for unlawful discrimination.

Keep Good Records

To avoid such liability, or the appearance of improper decision making, it is vital that all searches be well documented. Employers should keep records of all sites visited and search terms employed. It is equally important that employers have appropriate equal opportunity and anti-discrimination policies and that the relevant decision makers are adequately trained on such policies. Employers choosing to use online searches in connection with hiring decisions should also ensure that such searches are run uniformly — either for each and every applicant or for all applicants to whom a conditional offer of employment has been made.

Job-Related Searches Only

Furthermore, online searches should be limited to job-related information. Should an employer use information found via an online search to disqualify an applicant, an employer must be able to articulate a job-related rationale for the disqualification. If the information is not related to the job at stake, or the employer can articulate no such rationale, the employer may be evermore vulnerable to claims of discrimination.

Background Checks

The Fair Credit Reporting Act, 15 U.S.C. §1681 et seq., must also be considered. Under the Fair Credit Reporting Act, an employer must notify an applicant in writing and receive their consent if there will be a background check conducted by a third-party. This requirement likely applies if the employer hires a third-party to search Google or social networks for information on an applicant, though there are not yet court decisions on this issue.

Other Dangers

Finally, performing searches of applicants on social networking sites may violate the site's terms of service. For example, Facebook's terms of service require users collecting information to obtain consent and post a privacy policy explaining for what purpose the information will be used. Another provision prohibits creating an account under someone else's name or with false personal information. There has been speculation that a violation of these terms of service may give rise to a tort or contract claim, but that action is likely not enforceable by a party other than Facebook. It is also at least plausible that an employee may have a claim under the Federal Computer Fraud and Abuse Act, 18 U.S.C. §1030, although such a claim would require proof that the employer exceeded access and obtained information from a "protected computer" involving an interstate or foreign communication. Addition-

ally, an employer should never try to "hack" a social network page or blog, for that action could result in liability under the Stored Communications Act, 18 U.S.C. §§ 2701 et seq. *See Konop v. Hawaiian Airlines, Inc.,* 302 F.3d 868 (9th Cir. 2002), *cert. denied,* 537 U.S. 1193 (2003).

FIRING IN THE FACEBOOK AGE • As a practical matter, recent surveys of employers indicate that more than half monitor the at-work Internet use of employees to uncover access to social networking sites. This monitoring is generally permissible as long as the employer has a publicized Internet policy informing employees their usage will be watched. Furthermore, it is well established that employers can fire employees for activity or lack thereof while on the job. What is much less certain is whether and when employers can fire employees for comments made on a blog or social network site while off duty.

Despite the uncertainty, stories abound of employees fired for their online conduct. To relate just a few of the tamer examples: An employee was fired for blogging about how she hated her job and ridiculing company awards. Another employee was fired for implying that he did nothing at work besides surfing the Internet and blogging. Cisco rescinded their job offer from a young woman who wrote on Twitter that she would "have to weigh the utility of a fatty paycheck against the daily commute to San Jose and hating the work." A 16-year-old girl was fired for her Facebook status describing her job as boring. A Charlotte superintendent recommended firing a teacher who claimed on Facebook to be "teaching in the most ghetto school in Charlotte." Yet another teacher was expected to lose her job for a Facebook status saying, "I'm feeling p----- because I hate my students."

Even a brief review of the myriad of online examples reveals that employees have been fired for online conduct that ranges from complaining about their company or supervisors to harassing coworkers, disclosing company trade secrets, writing on controversial topics, or posting inappropriate material. The employment at-will doctrine, which allows an employer to fire an employee for any reason or no reason at all, would generally allow employers to take action against employees based on the content of their blogs or social network sites. However, this traditional common law doctrine has been greatly eroded in recent decades and is limited in this context by several potentially applicable employment laws.

Off-Duty Conduct Statutes And Privacy Laws

Some states have enacted off-duty conduct statutes, which prohibit employers from discharging employees who engage in lawful activities outside of work. *See, e.g.,* Cal. Lab. Code §§96(k), 98.6 (protects employees from adverse employment consequences for "lawful conduct occurring during nonworking hours away from the employer's premises."); Colo. Rev. Stat. §24-34-402.5(1) (employer cannot fire for "lawful activity off the premises of the employer during nonworking hours"); N.Y. Lab. Law. §201-d(2)(c) (protects employees from adverse employment consequences for "legal recreational activities outside work hours, off of the employer's premises and without use of the employer's equipment or other property"); N.D. Cent. Code §14-02.4-01 (prohibits discrimination for "participation in lawful activity off the employer's premises during nonworking hours"). Many of these states make exceptions, however, allowing an employer to discipline employees for off-duty conduct if it creates a conflict of interest or directly relates to employment activities. In interpreting these exceptions, courts have generally granted employers a great deal of discretion. However, employers should consult state law to determine if their state has enacted an off-duty conduct statute, and if so, under what circumstances employees can be fired for off-duty conduct.

As mentioned above, employees fired because of online conduct may also be able to state a common law invasion of privacy claim should they be able to prove that their employer accessed "private" online information. For instance, in *Pietrylo,* supra, a Houston's restaurant employee formed a private, by invitation-only discussion group called "Spec-Tator" on his MySpace page. Spec-Tator was intended to be a place where his fellow employees could vent about their jobs. However, after one member of Spec-Tator provided members of Houston's management with her access information, and they viewed the page's content, two employees — the creator of the group and another employee — were fired. Soon after, the two employees filed a lawsuit, alleging, among other things, a common law invasion of privacy claim.

While a jury ultimately found for the company on the privacy claim, an inspection of the jury's verdict form shows that the jury did indeed find that the Spec-Tator was a private, secluded place. The claim ultimately failed, however, when the jury found that the plaintiffs did not have a reasonable expectation of privacy in the group. It should be noted that this claim did survive summary judgment, with the district court specifically reserving both of the foregoing issues for the jury.

The *Pietrylo* plaintiffs did not walk away empty-handed, however. The jury found in their favor on their claim under the federal Stored Communications Act, 18 U.S.C. §§ 2701-11, as well as the state-law version of the Act, N.J. Stat. Ann. 2A: 156A-27. These acts make it an offense to intentionally access stored communications without authorization or in excess of authorization. Both statutes provide an exception to liability "with respect to conduct authorized ... by a user of that service with respect to a communication intended for that user." Thus, the plaintiffs' claims hinged on whether the employee who provided her Spec-Tator access information did so voluntarily or instead felt pressured or coerced into providing such information. The verdict indicates that the jury found that the employee felt coerced, and that she, therefore, did not authorize Houston's to access Spec-Tator. The jury awarded $17,000 in compensatory and punitive damages on these claims.

The National Labor Relations Act

Depending on the comments made on a blog or social network, the National Labor Relations Act (NLRA) might apply. NLRA Collective Bargaining section 7 gives employees the right to organize unions, collectively bargain, and "to engage in other concerted activities for the purpose of collective bargaining or other mutual aid or protection." *See* 29 U.S.C. § 157.

"Concerted" has been defined as "engaged in with or on the authority of other employees, and not solely by and on behalf of the employee himself." *See* Meyers Indus., 268 N.L.R.B. 493, 497 (Jan. 6, 1984), *cert. denied,* 474 U.S. 948 (1985). Employees therefore must work together in order for their activity to qualify as concerted. There must also be a nexus between the activity and the "employees' interests as employees." *See Eastex Inc. v. N.L.R.B.,* 437 U.S. 556, 567 (1978). "Mutual aid or protection" requires employees to be acting with the purpose of improving the terms and conditions of their employment or their positions as employees "through channels outside the immediate employee-employer relationship." *Id.* at 565. This includes discussions about "wages, benefits, working hours, the physical environment, dress codes, assignments, responsibilities, and the like." *New River Indus., Inc., v. N.L.R.B.,* 945 F.2d 1290, 1294 (4th Cir. 1991). Publicly criticizing the working conditions of nurses at a hospital, *Community Hosp. of Roanoke Valley, Inc. v. N.L.R.B.,* 538 F.2d 607, 610 (4th Cir. 1976), or complaining to coworkers about the negative effects of a new vacation policy have been classified as protected actions. *Timekeeping Sys., Inc.,* 323 N.L.R.B. 244, 250 (Feb. 27, 1997). This provision does not protect criticism unrelated to the mutual

aid or protection of employees, such as distributing flyers criticizing the quality of an employer's television broadcasts, or circulating a petition calling for the resignation of a foreman who had disciplined employees. *See, e.g., N.L.R.B. v. Local 1229, Int'l Bhd. of Elec. Workers,* 346 U.S. 464, 476-77 (1953); *Joanna Cotton Mills Co. v. N.L.R.B.,* 176 F.2d 749, 751-53 (4th Cir. 1949).

According to NLRA §8(a)(1), 29 U.S.C. §158(a)(1), employers cannot "interfere with, restrain, or coerce employees" who exercise the rights in section 7. An employer violates §8(a)(1) if:

- The employer knew of the concerted nature of the employee's activity;
- The concerted activity was protected by the NLRA; and
- The adverse employment action was motivated by the employee's protected concerted activity.

Meyers Indus., supra, 268 N.L.R.B. at 497. Violations may result in the employer paying back wages to the employee less whatever has been earned by the employee in the interim. 29 U.S.C. § 160(c). According to the National Labor Relations Board, the average back pay award in 2007 was only $3,935.

For purposes of blogging and social networking, the applicability of the NLRA will hinge on whether the activity was concerted. The activity may qualify as concerted if the employee notified other employees about the blog or social network, discussed aspects of the work environment, and permitted other employees to respond and comment. Employers must proceed cautiously when multiple employees engage in criticisms of the employer on a blog or social network.

Title VII And Other Anti-Discrimination Laws

Like it did in the applicant context, Title VII may protect employees disciplined for online activity if that activity reveals a protected characteristic. For example, an employee-blogger who posts about his recent religious conversion may be able to allege that his dismissal was a result of his religious beliefs and therefore violated Title VII. In such a situation, the employee may be able to state a prima facie case of religious discrimination if he could show that: the employer read his blog; the blog made the employer aware of his new faith; and subsequent to becoming aware of his faith, the employer fired him. Of course, establishing that the employer actually read the blog could prove very difficult.

Title VII may also come into play where a discharged employee can show that others who engaged in the same activity were not dismissed. A case in point is the Complaint filed in the Northern District of Georgia in 2005 by Ellen Simonetti — also known as the "Queen of the Sky." *See Simonetti v. Delta Airlines, Inc.* 2005 WL 2897844 (N.D. Ga. Sept. 7, 2005). Ms. Simonetti was fired after posting mildly provocative pictures of herself in her Delta uniform on her blog. She then filed suit, alleging that male employees who engaged in similar activity did not face any adverse employment action.

Other Potentially Applicable Laws

If the company is publicly traded, employers must avoid violating the whistleblower provisions of federal securities statutes. Employees who provide information to the federal government, Congress, or a supervisor, relating to securities violations or shareholder fraud are protected from adverse employment actions. 18 U.S.C. §1514A. Violation of this statute may result in up to 10 years in prison. If the information posted by an employee to a blog or social network alerts the authorities to a potential securities or fraud charge, employers should think twice before retaliating against that employee.

Other federal statutes may also offer employees "whistleblower" or anti-retaliation protections from discipline related to their online conduct. The Family and Medical Leave Act, for example, protects employees who oppose workplace practices

made illegal by the FMLA. This opposition could very well come in a blog or social networking post.

Finally, public employers must be also be cognizant of First Amendment limitations on their ability to discipline employees who speak out on matters of public concern. For private employers, free speech normally is not an issue since the First Amendment only applies to state action and not to private conduct. *See Lloyd Corp., LTD v. Tanner,* 407 U.S. 551, 567 (1972). In Connecticut, however, state law prohibits employers from discriminating against employees who exercise their rights to free speech under the federal or state constitution, unless the activity substantially or materially interferes with the employee's job performance or relationship with the employer. *See* Conn. Gen. Stat. §31-51q. A handful of other states protect employees who engage in political speech or activity, such as running for office or campaigning for a candidate. See Conn. Gen. Stat. §31-51q; D.C. Code §2-1402.11(a); La. Rev. Stat. Ann. §23:961; N.Y. Lab. Law §201-d(2); S.C. Code Ann. §16-17-560; Wash. Rev. Code Ann. §42.17.680(2). Connecticut employers or employers of politically active employees should not base employment decisions on this protected speech.

DEVELOPING AN APPROPRIATE SOCIAL NETWORK AND BLOG POLICY • Even if employers ban use of social networks in the workplace, a policy still is needed for use of blogs and social networks after working hours. Implementing a policy on the use of blogs and social networks can protect against loss of company trade secrets and injury to the company name, protect against possible harassment of co-workers, and may allow the employer to track what is being said about the company. However, a policy also might risk overregulating employees, lower employee morale, and subject the company to bad press.

Corporate policies already enacted range from the broad to the narrow. For instance, Sun Microsystems' Guidelines on Public Discourse state: "Many of us at Sun are doing work that could change the world. Contributing to online communities by blogging, wiki posting, participating in forums, etc., is a good way to do this. You are encouraged to tell the world about your work, without asking permission first, but we expect you to read and follow the advice in this note." On the other hand, the New York Times has developed the following policy: "[L]eave blank the [Facebook] section that asks about your political views…don't editorialize…keep an eye on what appears [on your social network page]."

Before implementing a policy, employers must realize the resistance employees have to regulation. According to a Ponemon Institute survey, more than eight out of 10 workers older than 50 believe their privacy would be violated if they were disciplined for what they wrote on a blog after hours, regardless of whether the content was work-related or not. Only inserting microchips into the arms of employees to give security clearance to trade secrets was considered a greater invasion of privacy. In addition, a Deloitte LLP survey revealed that 53 percent of employees believe their social network page is none of their employer's business, and 61 percent say they will not change their online activity even if their boss is watching. Despite this resistance, an appropriate, well-crafted policy is necessary to help insulate employers from the various risks inherent in employee online activity.

The employer can draft a new policy or incorporate guidelines into an existing IT policy. The policy should cover any form of online communication and conduct, from blogs to social networks, from Twitter to chat rooms and message boards. When drafting a policy, employers should consider including the following provisions:

There is no expectation of privacy when using an employer computer system. If permitted, an employee's use of blogs and social networks during working hours must not interfere with work activity.

An employee must not reveal confidential, proprietary information, or any other type of trade secret.

An employee must not reveal personal information of other employees or customers.

An employee must not violate the company's anti-discrimination policy and/or code of conduct. Employees should treat other Internet users with respect, and conduct themselves appropriately at all times. If the policy is specifically for social networks and blogs, it should be read in conjunction with disciplinary rules and procedure, and any existing IT policy.

An employee must not make libelous, defamatory, or harassing statements in online postings.

An employee must not use employer logos/uniforms/brands in online postings. Potential civil and criminal penalties for copyright violation also should be explained.

An employee must not state, or in anyway imply, that the employee represents the company. If the employee identifies the company, the employee must include a disclaimer explaining that the views expressed do not represent those of the company.

Conduct is prohibited that creates a conflict of interest or otherwise harms the employer's business interests.

An employee should follow all applicable federal, state, and local laws.

An employee may be subject to disciplinary action if this policy is violated. Some behavior should be identified as gross misconduct.

Questions about appropriate conduct should be directed to a manager or supervisor.

In addition, a well-crafted policy will reflect the employer's culture and attitude toward employee use of social networks and blogs. Take, for example, IBM's Social Computing Guidelines. Considering the company's position as a leader in computing technology, it would seem odd for it to issue any hard line policies on social networking. Thus, the company has chosen to draft a policy that embraces and encourages, while specifically regulating, social networking and blogging. The policy states: "IBM is increasingly exploring how online discourse through social computing can empower IBMers as global professionals, innovators and citizens. These individual interactions represent a new model: not mass communications, but masses of communicators. Therefore, it is very much in IBM's interest — and, we believe, in each IBMer's own — to be aware of and participate in this sphere of information, interaction and idea exchange[.]" However, the policy also goes on to remind employees to follow IBM's business conduct guidelines and to provide employees with eleven other guidelines for their social networking activity.

CONCLUSION • Blogs and social networks possess great potential for employers. Employers can use these forms of communication to advertise, recruit, gather background information on applicants, train and mentor employees, connect and communicate with employees, and quickly share information throughout a company. Indeed, in one instance, the online complaint by a spouse about an employee's working conditions led the company to begin making changes. Employers who can harness this powerful medium might receive many positive benefits for their companies and their employees.

Two out of three people on the Internet around the world visit a social network or blog, Web sites where Internet users spend one out of every 11 minutes online. There once was a time before the Internet, but that time has long since passed. We are living in the Facebook Age, and corporate employers must adjust if they want to effectively address the challenges of the Internet world.