



jackson|lewis
Preventive strategies.
Positive solutions.

Social Media and the Workplace: Managing the Risks

All We Do Is Work.
Workplace Law. In four time zones
and 45 major locations coast to coast.

www.jacksonlewis.com

JACKSON LEWIS

SERVING THE DIVERSE NEEDS OF MANAGEMENT

Jackson Lewis is one of the largest law firms in the country dedicated exclusively to representing management on workplace issues. The Firm has successfully handled cases in every state and is admitted to practice in all Circuit Courts of Appeal and in the United States Supreme Court. With 45 offices and more than 600 attorneys, the Firm has a national perspective and sensitivity to the nuances of regional business environments.

Since 1958 we have represented a wide range of public and private businesses and non-profit institutions in a vast array of industries. When issues arise, we devise optimal solutions that minimize costs and maximize results. Whether we are counseling on legal compliance or litigating a complex case, we assist our clients in achieving their business goals.

In addition, we help employers create policies and procedures promoting positive employee relations. We have built our practice and earned our national reputation over the years by helping companies reduce workplace-related litigation by educating management on legal trends, judicial developments, and statutory and regulatory compliance in the rapidly evolving area of workplace law. Our state-of-the-art preventive law programs utilize the Firm's expertise and unmatched experience to evaluate employment trends and related litigation, minimizing the risk of exposure in future lawsuits.

This Special Report is designed to give general and timely information on the subjects covered. It is not intended as advice or assistance with respect to individual problems. It is provided with the understanding that the publisher, editor or authors are not engaged in rendering legal or other professional services. Readers should consult competent counsel or other professional services of their own choosing as to how the matters discussed relate to their own affairs or to resolve specific problems or questions. This Special Report may be considered attorney advertising in some states. Furthermore, prior results do not guarantee a similar outcome.

Copyright: © 2010 Jackson Lewis LLP

Social Media and the Workplace: Managing the Risks

Social media applications such as blogs, social networking, and video sharing have surged in popularity over the past few years, and, in one form or another, are now used by employees in almost every workplace. According to its own statistics, Facebook, the most popular social networking site in the U.S., has over 400 million active users, who, in total, post more than 60 million status updates each day and upload more than 3 billion photos each month.¹ The average Facebook user spends more than 55 minutes per day on the site.²

Though some assume employees' social media use is solely problematic for employers, forward-thinking companies across the globe are embracing social networking sites and blogs for, among other things, branding, client development and service, research, recruiting, and to improve employee engagement and facilitate multi-office workplaces. Using Facebook as an example, more than 700,000 local businesses have active pages on the site.³ Recognizing this trend, Facebook provides a number of business-related applications, including document sharing, networking tools, and blog promotion.⁴ As more and more companies turn to web-based social media applications for business purposes, employees will be increasingly likely to use these technologies in the workplace.

Employees' social media use, however, also poses risks for employers. Social media has been defined as "a group of Internet-based applications that... allow the creation and exchange of user-generated content."⁵ This capacity exposes employers to a number of hazards. Some examples include employees sharing confidential company information with a virtual community of contacts through a social networking site such as Facebook, MySpace, or Twitter, disparaging their employers and co-workers on a blog, or posting embarrassing videos recorded in the workplace on YouTube. Regardless of whether employees are posting at home or during working hours, employers may face legal liability when employees misuse social media.

As we become more dependent on social media for business purposes, questions surrounding employees' and employers' respective rights and responsibilities abound. This white paper is intended to provide an overview of the various laws and other issues that come into play with respect to social media use in the workplace.⁶ It is divided into three parts: (1) employees' misuse of social media, including theories of employer liability; (2) monitoring and regulating employees' social media use; and (3) basing hiring decisions on information obtained from social media.

¹ Facebook Press Room, <http://www.facebook.com/press/info.php?statistics> (last visited Mar. 3, 2010).

² *Id.*

³ *Id.*

⁴ See Josh Peters, *30+ Apps for Doing Business on Facebook*, MASHABLE, Jan. 22, 2009, <http://mashable.com/2009/01/22/business-facebook-apps/>.

⁵ Wikipedia, *Social Media*, http://en.wikipedia.org/wiki/Social_media#cite_note-0 (last visited Jan. 15, 2010) (citing Andreas M. Kaplan and Michael Haenlein, *Users of the world, unite! The challenges and opportunities of social media*, BUSINESS HORIZONS, Vol. 53, Issue 1, January-February 2010, at 59-68).

⁶ An analysis of the **benefits** of social media in the workplace is beyond the scope of this paper, which is designed to help employers manage the risks.

I. Employees' Misuse of Social Media

Employees may intentionally or inadvertently use social media—whether on-the-job or at home—in a way that poses risks for their employers. While at work, employers may suffer because employees spend too much time on social networking sites, instant messaging with friends, or just surfing the internet. Though these activities may decrease productivity, they may not necessarily result in any additional harm. When employees use social media, however, to harass co-workers, criticize the company or its clients, reveal confidential information, endorse products or services without proper disclosure, or engage in criminal conduct, employers face far greater risks. It is important to keep in mind that employees often create these types of problems not because they are acting maliciously, but instead because they are acting—or posting—without thinking.

A. Potential Theories of Employer Liability for Employees' Misuse

Some of the legal risks employers face when employees misuse social media include:

Hostile Work Environment and Discrimination Claims. Social networking sites and blogs provide employees with additional avenues for engaging in inappropriate conduct. Employees may vent workplace frustrations by posting discriminatory statements, racial slurs, or sexual innuendos directed at co-workers, management, customers, or vendors. If a supervisor has posted discriminatory statements regarding an employee's protected status on his or her Facebook page, for example, and the employee is later terminated or subjected to an adverse employment action, the supervisor's discriminatory statements could be used as evidence that the employment action was motivated by discriminatory animus in a subsequent lawsuit or administrative claim.

Defamation Claims. Employers may face liability for defamation based on electronic communications disseminated by employees. Employee bloggers, for example, can create unrest in the workplace by posting rumors, gossip, and offensive false statements about co-workers and supervisors. Negative comments made by management about a departing employee may also create liability. Consider the following example: An employee leaves Company A to take advantage of more promising opportunities with Company B. Prior to starting with Company B, her supervisor at Company A posts false and damaging comments regarding her abilities and work habits on a blog. An employee at Company B stumbles upon these comments, and Company B withdraws its employment offer based on the false information. As a result of the comments posted in the blog, the former employee may have a cause of action against Company A and the supervisor for defamation or interference with prospective economic relations.

Improper Disclosure of Confidential or Other Protected Information. Employees may inadvertently reveal—or enable others to piece together— proprietary or confidential information on a blog or social networking site, instantly disseminating extremely sensitive company—or client— information with the simple click of a button. For example, consider a corporate attorney working on a merger and acquisition who updates her Facebook status to read: “So glad the deal is done. I need some sleep!” Someone who knows that the attorney handles mergers and acquisitions and represents a particular client may piece together that something important is about to happen. If that person decides to buy a significant amount of stock in one of the companies, the attorney and his or her law firm can end up in trouble. Employees may also act more deliberately, such as a disgruntled employee revealing a company's trade secrets and other proprietary information on a blog.

Reporting Requirements for Child Pornography. Some states, including Arkansas, Illinois, Michigan, Missouri, North Carolina, Oklahoma, South Carolina, and South Dakota, have mandatory reporting statutes that require information technology workers to report child pornography found on computers they are servicing.⁷ In cases of child pornography or other illegal electronic conduct, employers must take particular care to preserve the evidence for legal authorities and to not destroy any equipment, emails, or files that make contain such evidence.

Federal Trade Commission (FTC) Guides. According to newly revised FTC Guides addressing the use of “endorsements and testimonials in advertising,” employers may face liability when employees comment on their employer’s services or products on social media without disclosing the employment relationship.⁸ Potential liability may exist even if the comments were not sponsored or authorized by the employer.

In addition to these legal risks, employees may purposely or inadvertently harm an employer’s *reputation* using social media. Employees can harm their employer’s reputation by posting controversial or inappropriate comments or pictures on their own blogs or websites, which in some way make reference to their employer or can be connected to the employer based on the individual’s status as an employee. For example, in some instances employees may post statements or videos revealing unlawful conduct outside of work. If individuals viewing the posts or videos have knowledge of the individual’s employer, or the employer is somehow referenced, the conduct may be imputed to the employer. In some instances, employees may be liable for this type of conduct, under theories of *interference with prospective economic relations*, *interference with contract*, *intentional infliction of emotional distress*, *publication of private facts*, and other *speech-based torts*.

B. Disciplining Employees Who Misuse Social Media

There are a myriad of scenarios that may prompt an employer to discipline an employee for his or her social media use. The most obvious situation is an employee who engages in illegal web-based activity while at work. Another common scenario is an employee who spends the majority of his or her on-duty time using Facebook or surfing the internet. Other situations may include employees who criticize a supervisor or client, post distasteful photos or videos, or call in sick and then post contrary information. Some real life examples include the following:

- A Texas disc jockey was fired for blogging about his homosexual dating habits on the company’s MySpace page and his personal website;
- An Orlando Sheriff’s deputy was fired after he posted comments about swimming nude, drinking heavily, female breasts, and other topics on MySpace;
- A California automobile club fired 27 employees who made objectionable comments on MySpace, including remarks about co-workers’ weight and sexual orientation;

⁷ See Ark. Code § 5-27-604, 325 Ill. Comp. Stat. 5/4.5, Mich. Comp. Laws § 750.145c(9), Mo. Rev. Stat. § 568.110, N.C. Gen. Stat. § 66-67.4, Okla. Stat. tit. 21 § 1021.4, S.C. Code § 16-3-850, and S.D. Codified Laws § 22-22-24.18. In addition, the Appellate Division of the Superior Court of New Jersey has held “that an employer who is on notice that one of its employees is using a workplace computer to access pornography, possibly child pornography, has a duty to investigate the employee’s activity, lest it result in harm to innocent third-parties.” *Doe v. XYZ Corp.*, 2005 N.J. Super. LEXIS 377 (Dec. 27, 2005).

⁸ FTC Guides Concerning the Use of Endorsements and Testimonials in Advertising, 16 CFR §255 (2009).

- The Philadelphia Eagles fired an employee for posting a critical message about the team on his Facebook page. The employee wrote, “I am f---ing devastated about [Brian] Dawkins signing with Denver... Dam Eagles R Retarded!!”; and
- A Washington employer fired a manager for posting sexual photos of himself with minor children on Facebook.

Before deciding to take an adverse employment action against an employee based on his or her social media use, employers should consider whether there are legal constraints preventing or limiting such action. Some of the legal constraints employers must consider include:

The National Labor Relations Act. The NLRA affords employees (even those who are not unionized) the right to engage in “concerted activity,” including the right to discuss the terms and conditions of their employment—and even to criticize their employers—with co-workers and outsiders. Not all concerted activities are protected by the NLRA; only those activities that are engaged in for the purpose of collective bargaining or other mutual aid or protection are covered. Thus, before disciplining an employee who, for example, has complained about the employer on his or her blog, an employer must determine if the employee has engaged in protected concerted activity.

Could the employee be protected under a whistleblower statute? Federal and state whistleblower laws may protect employees who complain about company conditions affecting public health and safety, as well as employees who report potential securities fraud violations. For example, the Sarbanes-Oxley Act of 2002 (SOX) prohibits employers from terminating employees for “provid[ing] information, caus[ing] information to be provided, or otherwise assist[ing] in an investigation regarding any conduct which the employee reasonably believes constitutes a violation of ... any rule or regulation of the Securities and Exchange Commission, or any provision of Federal law relating to fraud against shareholders.”⁹ The investigation, however, must be conducted by, among others, a person with supervisory authority over the employee. An employee who reports alleged securities fraud on a company blog monitored by management to detect improper activities within the workplace could be protected, for example, under SOX.

Was the communication related to political activities or affiliations? Many states, including California, prohibit employers from regulating employee political activities and affiliations or influencing employees’ political activities.¹⁰ Taking action against an employee for objectionable political speech could violate these restrictions.

Was the employee engaging in “legal off-duty activity” protected by state law or illegal activity? Some states have “lawful conduct” laws that may protect an employee or applicant’s legal off-duty activities. For example, under California law, an employee is protected from “demotion, suspension, or discharge from employment for lawful conduct occurring during nonworking hours away from the employer’s premises.”¹¹ Thus, in some states, an employer may be prohibited from terminating an employee who, for example, posts pictures of himself intoxicated at a party (assuming the employee is over 21 years old). In contrast, the employer may have more leeway where the conduct is illegal (assuming the employee is under 21 in the example provided). However, even where conduct appears to be illegal, the employer may still need to take additional steps to investigate and consult with counsel

⁹ 18 USCS § 1514A.

¹⁰ See, e.g., Cal. Lab. Code §§ 1101, 1102 (2006).

¹¹ Cal. Lab. Code §§ 96(k), 98.6; see also, e.g., 820 Ill. Comp. Stat. § 55/1-120 (limited to “use of lawful products”); Minn. Stat. § 181.938 (limited to “lawful consumable products”); N.Y. [Labor] Law § 201-d; Wisc. Stat. § 111.321.

before taking any action. For example, in California, employers are prohibited from excluding someone from employment based solely on an arrest, marijuana convictions more than two years old or convictions that have been expunged or dismissed. Thus, even postings relating to seemingly “illegal conduct” may not be utilized by the employer in some circumstances. The law is far from clear in this area, and employers should consider each situation independently.

Does the employee have a potential discrimination claim? Employers are prohibited from unlawfully discriminating against employees on account of protected characteristics, including race, age, sexual orientation, marital status, disability, and even genetic information.¹² If an employer learns from an employee’s Facebook status, for example, that the employee is pregnant, the employer cannot fire the employee on account of the pregnancy. Employers should also keep in mind that an employee terminated for inappropriate social media use may later assert that the employer’s actions were discriminatory.

Ultimately, hiring, disciplining, and firing are all critical parts of the employment relationship, and what is appropriate social media use in one workplace may not be in another. An employer relying on web-based information to make these decisions should be aware of potential legal repercussions and consult with legal counsel to manage the risks inherent in any adverse employment decision.

II. Monitoring and Regulating Employees’ Social Media Use

“What are the legal boundaries of an employee’s privacy in this interconnected, electronic-communication age, one in which thoughts and ideas that would have been spoken personally and privately in ages past are now instantly text-messaged to friends and family via hand-held, computer-assisted electronic devices?” That is the question posed by a federal district court in a case that the U.S. Supreme Court has agreed to review.

In *City of Ontario v. Quon.*, the Supreme Court will determine whether, under the Fourth Amendment to the U.S. Constitution, the California Police Department’s employees should expect privacy for personal text messages they send and receive on police pagers where the Department’s official “no-privacy” policy may conflict with its informal policy of allowing some personal use of pagers.¹³ The underlying suit was filed by police Sgt. Jeff Quon, his wife, his girlfriend, and another police sergeant after one of Quon’s superiors audited his messages and found that many of them were sexually explicit and personal in nature. The U.S. Court of Appeals for the Ninth Circuit sided with the police officer, ruling that Quon had a “reasonable expectation of privacy” regarding messages stored on the service provider’s network, and the government’s search was unreasonable under the circumstances.

While the Fourth Amendment only applies to the government—and not private sector employers—the outcome in *Quon* may affect electronic communications policies and practices across the country, whether by public or private employers.

¹² The U.S. Equal Employment Opportunity Commission has not yet issued final regulations regarding how the Genetic Information Nondiscrimination Act’s provisions will apply to social networking sites.

¹³ *Quon v. Arch Wireless Operating Company Inc.*, 445 F.Supp.2d 1116 (C.D. Cal. 2006), *aff’d in part, rev’d in part*, 529 F.3d 892 (9th Cir. 2008), *reh’g denied*, 554 F.3d 769 (9th Cir. 2009), *cert. granted*, *City of Ontario v. Quon et al.*, U.S. No. 08-1332 (12/14/09).

A. Monitoring Employees' Social Media Use: Privacy Concerns

Considering the significant potential liability and other risks employers face from employees' social media use, how far can employers go in monitoring these communications? Although the Fourth Amendment to the U.S. Constitution prohibits unreasonable searches and seizures by the government, it does not apply to private sector employers. While private sector employees have no inherent constitutional right to privacy, employer conduct is limited by common-law principles and federal and state privacy laws, including:

TORT: "Intrusion upon the plaintiff's seclusion or solitude." Private sector employees have common law "privacy rights" which are enforced through tort claims based on invasion of privacy theories. The most applicable theory to employer-monitoring of electronic communications is "intrusion upon the plaintiff's seclusion or solitude."¹⁴ Under this theory, an employee must prove: (1) an intentional intrusion, physical or otherwise, (2) upon the plaintiff's solitude or seclusion or private affairs or concerns, (3) which would be highly offensive to a reasonable person. An employer may successfully defend against such claims by establishing that the employee did not have a reasonable expectation of privacy in the electronic communications.¹⁵ Courts are generally more inclined to rule in the employer's favor where the employee voluntarily uses an employer's network and/or computer and consented to be monitored or was advised of the employer's written electronic communications policy.

Federal Wiretap Act and the Electronic Communications Privacy Act (ECPA) of 1986, amending the Federal Wiretap Act of 1968. ECPA imposes criminal and civil penalties against any person who intentionally intercepts an electronic communication with certain specific exceptions, including an "ordinary course of business" exception.¹⁶ The *Stored Communications Act ("SCA")*, part of the ECPA, covers stored electronic communications. In one recent case, a federal court in New Jersey rejected the employer's attempt to throw out a jury verdict against managers at a Houston's restaurant who intentionally and without authorization accessed a private, invitation-only chat group on MySpace in violation of the federal SCA.¹⁷

State Law. Various states protect a person's right to privacy through statutes or state constitutions. Some states prohibit electronic monitoring of employee communications without two-party consent. Employers should check the relevant state privacy laws before monitoring employees' social media use.

B. Strategies for Regulating Electronic Communications

Whether employees are communicating with friends outside the company or with co-workers and business partners regarding work-related projects, employers should have clear policies regarding the use of social media both in and outside the workplace. Employees—who may not realize they can expose employers to risk by posting information on blogs and private social networking sites during work or non-work hours—should be informed of potential risks and aware of the employer's expectations.

¹⁴ RESTATEMENT (SECOND) OF TORTS § 652 (1965).

¹⁵ For example, in *Thygeson v. U.S. Bancorp*, 2004 U.S. Dist. LEXIS 18863 (D. Or. Sept. 15, 2004), the court held an employee had no reasonable expectation of privacy in the internet websites he accessed while using his work computer. In that case, the plaintiff was a former employee who was fired for excessive internet use and storing sexually inappropriate e-mails, from his web-based account, on the company network. The plaintiff sued, claiming the company invaded his privacy. The court rejected the plaintiff's claim because the company only gathered information available on its own network and had a policy regarding personal computer use and monitoring.

¹⁶ 18 U.S.C. § 2511(2)(a)(1)(2006).

¹⁷ *Brian Pietrylo, et al. v. Hillstone Restaurant Group d/b/a Houston's*, No. 06-5754 (FSH) (D.N.J. Sept. 25, 2009).

The precise contours of an employer’s social media use policy will depend on the organization, its culture and approach to social technologies, and the nature of work performed. For instance, a social media use policy for educators may be very different from a policy aimed at employees who are encouraged to use social media for developing client relations. However, there are some basic issues employers should address when implementing a social media policy.

Employees should be warned that postings regarding: (1) proprietary and confidential company information; (2) discriminatory statements or sexual innuendos regarding co-workers, management, customers, or vendors; and (3) defamatory statements regarding the company, its employees, customers, competitors, or vendors will not be tolerated and will subject the individual to discipline. Social media use policies should also make clear that if the employee mentions the company with which he or she is affiliated, he or she must also include a disclaimer stating that any opinions expressed are the employee’s own and do not represent the company’s positions, strategies, or opinions. The policy should specify that these prohibitions apply to postings and blogging occurring at any time, on any computer.

Employers should also consider amending their handbook policies to provide a detailed explanation of what is considered “acceptable use” (*i.e.*, business use only, limited personal use, or unlimited personal use).¹⁸ Employers can also implement a policy that reduces the level of privacy employees expect in their work computer systems, e-mail, and internet use. Indeed, courts have routinely considered whether an employer has an electronic communications policy in determining whether an employee had a reasonable expectation of privacy. While such a policy will not necessarily insulate an employer from all potential liability, it will reduce employees’ expectations of privacy and provide the employer with more discretion to take action against employees who engage in misconduct.

Other provisions employers may chose to incorporate into a social media policy include the following:

- Employees are expected to comport themselves professionally both on and off duty;
- Managers are prohibited from using any informal review systems on social networking sites (*i.e.*, LinkedIn);
- Company policies governing the use of corporate logos and other branding and identity apply to electronic communications, and only individuals officially designated may “speak” (whether orally or in writing) on the company’s behalf;
- Employees must comply with all other company policies with respect to their electronic communications (such as rules against conduct that may result in unlawful sexual harassment, etc.);

¹⁸ After the NLRB’s decision in *The Guard Publishing Company, d/b/a The Register-Guard*, 351 NLRB No. 70 (Dec. 16, 2007), employers can restrict the subject matter of employee e-mails sent through their networks. In that decision, the NLRB ruled that an employer does not violate the NLRA by maintaining a policy prohibiting employees from using the employer’s e-mail system for “non-job-related solicitations.” In its ruling, the Board also held that an employer may permit employee personal e-mail usage unrelated to Section 7 activity, but prohibit any use of the e-mail system for union solicitation. It said that, without violating the NLRA, “an employer may draw a line between charitable solicitations and noncharitable solicitations, between solicitations of a personal nature (*e.g.*, a car for sale) and solicitations for the commercial sale of a product (*e.g.*, Avon products), between invitations for an organization and invitations of a personal nature, between solicitations and mere talk, and between business-related use and non-business-related use.” Employers must still, however, consider NLRA protections as well as state off-duty laws when implementing blogging and social networking policies. It is also possible that the *Register Guard* decision will be overturned.

- The company's systems may not be used for any illegal activity, including downloading or distributing pirated software or data;
- The company reserves the right to take disciplinary action against an employee if the employee's electronic communications violate company policy;
- A statement that the policy is not intended to interfere with rights under the NLRA;
- A reporting procedure for violations of the policy;
- Designate a management representative within the organization as the point of contact for policy violations or questions concerning the policy to ensure consistent application; and
- Notice that monitoring will occur in order to reduce an employee's expectation of privacy.

A social media policy should be written with the assistance of counsel for distribution to all employees in employee handbooks, policy manuals (as a stand-alone policy), paycheck reminders, and annual or more frequent e-mail reminders. Employers may also consider requiring employee acknowledgments for receipt of all of the above. All policies must be accompanied by actual monitoring and uniform enforcement.

III. Can Employers Base Hiring Decisions on Information Obtained from Social Networking Sites or Blogs?

Employers are increasingly turning to social media for information about job applicants. So long as the employer does not violate state or federal discrimination laws, nothing currently prohibits an employment decision based on information an applicant places in the public domain.¹⁹ Nevertheless, employers should balance the need to obtain information against the risks associated with acting on such information if it reveals an applicant's protected characteristics.

When using social media to vet job candidates, an employer may inadvertently become aware of an applicant's protected characteristics, such as race, age, sexual orientation, marital status, disability, and even genetic information protected under federal law. Some states also prohibit discrimination on account of sexual orientation, political affiliation, and off-duty conduct. If the employer decides not to hire the applicant, he or she could sue the employer, alleging that the decision was discriminatory. This is the precise reason many employers have stopped requiring applicants to submit certain information with their resume or application; searching social networking sites may reveal such information and open the employer to the very risk it tried to avoid.

¹⁹ The Federal Fair Credit Reporting Act (FCRA) requires employers to obtain consent before conducting background checks through consumer reporting agencies. If an employer decides not to hire an applicant based on information in a consumer report obtained from a social networking site, the employer must notify the applicant that its decision was based on that information. Some state fair credit reporting laws are more stringent than federal law.

Other issues include learning about an applicant's arrest history, conviction, or workers' compensation claim. Similarly, federal law prohibits employers from discriminating against an applicant based on the employee's current or prior filing for bankruptcy. Employers must be careful of state and federal laws that prohibit employment discrimination on account of such information.

Employers should also avoid circumventing a potential employee's privacy settings by pretending to be someone else in order to gain access to a restricted network.

One practical option is to have someone who is not a decision maker at the company conduct the search in order to filter out protected information. This person can then provide the "scrubbed" information in document form to a decision maker for review.

Another risk of using social media and other information obtained on the internet to screen applicants is that the information discovered may be inaccurate or misleading. For example, a website seemingly run by, or affiliated with, a job applicant may not actually be related to, or even known by, the applicant. Additionally, false information may be posted on blogs and other social networking sites. Reputable news sources are continually coming under fire for relying upon, without fully checking, internet-based postings. Employers should keep this in mind when turning to the internet for information about job applicants.

* * *

Social media use presents a multitude of opportunities—and risks—for employers. As more and more companies turn to social media for business purposes, it will become imperative for employers to provide employees with clear guidelines detailing what is and what is not acceptable use. Employers, too, will need to understand the limits of using social media for hiring, promotion, and termination decisions.

For additional information, please contact:

JoAnna Brooks | Partner

Jackson Lewis LLP

199 Fremont Street, 10th Floor

San Francisco, CA 94105

(T) 415-394-9400 | (F) 415-394-9401

brooks@jacksonlewis.com | www.jacksonlewis.com

Chad P. Richter | Partner

Jackson Lewis LLP

10050 Regency Circle, Suite 400

Omaha, NE 68114

(T) 402-391-1991 | (F) 402-391-7363

richterc@jacksonlewis.com | www.jacksonlewis.com

All we do is
wor**rk**

Workplace law. In four time zones and 45 major locations coast to coast.

jackson | lewis

Preventive Strategies and
Positive Solutions for the Workplace™

www.jacksonlewis.com