IN THE BUSINESS OF YOUR SUCCESS℠

ADP TOTALSOURCE®

Rising Above the Risks of Social Media:

Responsibilities and Policies in the Workplace

October 16, 2012

HR. Payroll. Benefits.

jackson|lewis

Preventive Strategies and Positive Solutions for the Workplace®

Contents

About This Guide

Facebook, Twitter, and email may be more addictive than alcohol or smoking

That is what a recent study says about social media, a form of online communication that is certainly no longer considered a fad. With more than 1 billion users on Facebook and Twitter alone, social media may be the biggest cultural and economic shift since the industrial revolution. Simply put, social media is the dominant form of communication today.

Chances are that some of your employees are on social media right now.

Not surprisingly then, millions of employees communicate daily via social media. In fact, chances are that some of your employees are on social media right now. And employers are just as likely to be using social media —investigating job applicants' Facebook, LinkedIn, and Twitter profiles during the recruitment and hiring stages. Employers are also increasingly turning to social media for information about the conduct of current employees.

These changes have not gone unnoticed by the federal government, state governments, and the court systems. They have become increasingly active in this constantly evolving area of the law. They have been busy proposing and creating new laws and rules, as well as reinterpreting old ones, all in an effort to catch up with social media's impact on the workplace.

These rapid changes have caught some employers off guard. Are you prepared? **The purpose of this special report is to provide employers with timely information to prepare for, and plan for, the substantial impact that social media is having in the workplace.**

The Numbers Are Staggering

Facebook dominates social media traffic. It has more than 900 million monthly active users, and it is estimated to reach one billion users by August 2012. That is an amazing number — approximately 14 percent of the world's population. Twitter, which is also prevalent, has nearly 500 million registered users and is still growing at an astounding rate.

Hiring managers are using social media to evaluate candidates' character and personality outside the confines of the traditional interview process.

Employees' private and workplace lives easily intersect on social media, where boundaries become blurred. Of the millions of employees who use social media sites, one recent survey revealed that 39% have befriended a colleague or business contact on Facebook or LinkedIn; 14% have posted a status update or tweeted about their work; 22% have posted a status update or tweeted about a work colleague; and 28% have posted photos of colleagues or business activities. Yet, a recent survey by the Society for Human Resources Management shows that 69% of employers surveyed do not track employee use of social media on company-owned computers or devices.

Employers are also actively using social media. For example, nearly 40 percent of employers use social networking sites to research job candidates, according to a recent survey from CareerBuilder. The survey reveals that hiring managers are using social media to evaluate candidates' character and personality outside the confines of the traditional interview process. When asked why they use social networks to conduct background research, hiring managers listed the following reasons: to see if the candidate presents himself/herself professionally (65 percent); to see if the candidate is a good fit for the company culture (51 percent); to learn more about the candidate's qualifications (45 percent); to see if the candidate is well-rounded (35 percent); and to look for reasons not to hire the candidate (12 percent).

A third of hiring managers who currently research candidates via social media said they have found information that has caused them not to hire a candidate. The reasons range from evidence of inappropriate behavior to information that contradicted their listed qualifications: candidate posted provocative/inappropriate photos/information (49 percent); there was information about candidate drinking or using drugs (45 percent); candidate had poor communication skills (35 percent); candidate bad-mouthed previous employer (33 percent); candidate made discriminatory comments related to race, gender, religion, etc. (28 percent); and candidate lied about qualifications (22 percent).

Lastly, according to the survey, employers are also looking for information that could potentially give a job seeker an advantage. A third of hiring managers said they have found something that has caused them to hire a candidate, including the following: good feel for candidate's personality (58 percent); conveyed a professional image (55 percent); background information supported professional qualifications (54 percent); well-rounded, showed a wide range of interests (51 percent); great communication skills (49 percent); candidate was creative (44 percent); and other people posted great references about the candidate (34 percent).

Point being, the use of social media in the workplace is here to stay. While employers cannot prevent all of the legal risks associated with social media, they can manage them.

The Rising Tide: Federal and State Legislative Developments

For years, there really was no law that specifically addressed an employer's right to use social media to collect information about applicants or current employees. That is quickly changing.

Federal legislative developments

On March 22, 2012, U.S. Senators Charles Schumer and Richard Blumenthal called on the U.S. Equal Employment Opportunity Commission and the U.S. Department of Justice to investigate whether employers violate any privacy, fraud, or anti-discrimination laws by demanding access to job applicants' Facebook accounts before making a hiring decision.

The next day, March 23, 2012, Facebook publicly joined the discussion. The Company's Chief Privacy Office posted the following blog entry on the Company's website:

> *In recent months, we've seen a distressing increase in reports of employers or others seeking to gain inappropriate access to people's Facebook profiles or private information. This practice undermines the privacy expectations and the security of both the user and the user's friends. It also potentially exposes the employer who seeks this access to unanticipated legal liability.*
>
> *The most alarming of these practices is the reported incidents of employers asking prospective or actual employees to reveal their passwords. If you are a Facebook user, you should never have to share your password, let anyone access your account, or do anything that might jeopardize the security of your account or violate the privacy of your friends. We have worked really hard at Facebook to give you the tools to control who sees your information.*
>
> *As a user, you shouldn't be forced to share your private information and communications just to get a job. And as the friend of a user, you shouldn't have to worry that your private information or communications will be revealed to someone you don't know and didn't intend to share with just because that user is looking for a job. That's why we've made it a violation of Facebook's Statement of Rights and Responsibilities to share or solicit a Facebook password.*
>
> *We don't think employers should be asking prospective employees to provide their passwords because we don't think it's the right thing to do. But it also may cause problems for the employers that they are not anticipating. For example, if an employer sees on Facebook that someone is a member of a protected group (e.g., over a certain age, etc.) that employer may open themselves up to claims of discrimination if they don't hire that person.*

The Social Networking Online Protection Act would prohibit employers from requiring such information or to deny employment or penalize candidates or employeess for refusing to provide such information.

One month later, on April 27, 2012, federal legislators introduced proposed legislation to bar current and prospective employers from requiring job candidates and employees to submit their user names and passwords for social networking sites. The Social Networking Online Protection Act, introduced by U.S. Representative Eliot Engel, would prohibit employers, schools, and universities from requiring such information or to deny employment or penalize candidates, employees, or students for refusing to provide such information.

"The American people deserve the right to keep their personal accounts private," said U.S. Representative Jan Schakowsky, a co-sponsor of the bill. "No one should have to worry that their personal account information, including passwords, can be required by an employer or educational institution, and if this legislation is signed into law, no one will face that possibility."

"Social media sites have become a widespread communications tool — both personally and professionally — all across the world," Engel said in a statement. "However, a person's so-called 'digital footprint' is largely unprotected. Passwords are the gateway to many avenues containing personal and sensitive content — including email accounts, bank accounts, and other information." The legislation is still pending.

State legislative developments

States are also active in this area. On May 2, 2012, Maryland became the first state to make it illegal for employers to demand user names, passwords, or other means to access any personal account or service through an electronic communication device (computer, phone, PDA, etc.), such as social media sites Facebook or LinkedIn, belonging to employees or job applicants. The new law becomes effective October 1, 2012. The law applies to any employer engaged in business in Maryland, as well as any unit of state or local government. It is also illegal for employers to discharge, discipline, or otherwise penalize employees or applicants who refuse to comply with requests for such information. In addition, employers may not fail or refuse to hire applicants who object to similar requests.

Other states are likely to follow suit. California is considering legislation that would make it illegal for companies to request or require employees and job candidates to disclose their social media user names and passwords. The proposed legislation would also prohibit colleges and universities from requiring the information from students. If a company refused to hire a job applicant because of information obtained on a social networking website, the applicant could bring a lawsuit.

Maryland became the first state to make it illegal for employers to demand user names, passwords or other means to access any personal account.

Illinois is considering legislation that would make it illegal for an employer to request a password or related account information from an employee or prospective employee in order to access that person's social networking site. The proposed legislation specifies that it does not limit an employer's right to maintain lawful workplace policies governing the use of its electronic equipment or monitor that use without requiring an employee to provide any social networking passwords. The proposed legislation also would not bar an employer from getting information about a prospective employee or current employee that is in the public domain.

New York is considering legislation that would make it illegal for an employer or employer's agent, representative, or designee to require any employee or applicant to disclose any log-in name, password, or other means for accessing a personal account or service through an electronic communications device. Moreover, an employer or its representative may not fire, discipline, or otherwise penalize a worker for refusing to cough up passwords or other information used to access personal social networking sites. Refusal to provide a password or access to a social media site cannot be used as a reason to refuse to hire a candidate for a job. Violators are subject to a $300 fine the first time around and a $500 fine for each subsequent violation, according to the proposed legislation.

Michigan and Minnesota are also considering legislation that would make it illegal for employers to require applicants to disclose their passwords to social networking sites.

So far, none of these proposed laws would restrict an employer's ability to find and use information that is publicly available on social media. Nonetheless, employers need to closely monitor these developments and ensure compliance with the laws that are passed in the upcoming months.

The Rising Tide: Federal Regulatory and Enforcement Activity

In addition to legislative activity at the federal and state levels, there has been regulatory and enforcement activity by various agencies of the federal government, including the Equal Employment Opportunity Commission and the National Labor Relations Board.

Employee complaints are nothing new, but social media sites like Facebook have given workers a new avenue for their gripes. While online venting may not sit well with employers, as discussed below, employers should be cautious about taking disciplinary action over arguably insulting posts and tweets.

National Labor Relations Board

If you plan to skip this section because you do not have any unionized employees, you are making a mistake. Employers who ignore the National Labor Relations Act (Act) do so at their own peril. When it comes to social media in the workplace, the National Labor Relations Board (Board) is a powerful enforcer of rights for unionized and non-unionized employees alike. The Board has been more active — and successful — in this area than any other federal agency.

While online venting may not sit well with employers, employers should be cautious about taking disciplinary action over arguably insulting posts and tweets.

By way of background, the Board enforces the Act. When the Board says that an employee has engaged in "protected concerted activity" on social media or otherwise, the Board is referring to an employee's conduct that is protected by Section 7 of the Act. Section 7 protects employees who engage in "concerted activities for the purpose of collective bargaining or other mutual aid or protection." Importantly, the Act does not just protect employees who engage in union activities or work in a unionized environment. It also protects other forms of employee conduct undertaken for their "mutual aid or protection" including, for example, a group of nonunion employees complaining to management about their wages or working conditions, participating in a strike or work stoppage, or attempting to enlist public support to improve their terms or conditions of employment.

The Board's Acting General Counsel, Lafe Solomon, spoke at a legal conference on November 3, 2011. He said the appearance gave him "a chance to explain to the 93 percent [of private-sector workers] who are not represented by unions the National Labor Relations Act" and principles of protected concerted activity under the Act. Mr. Solomon said the Board is receiving hundreds of unfair labor practice charges from individuals asserting that employers violated their NLRA rights by punishing them due to their use of social media . Like other charges filed with the Board's regional offices, he said, some will not to have merit. Nonetheless, he said it is a positive development that more workers are "waking up" to rights that are guaranteed by the Act, but have been unfamiliar to the general public.

August 2011 Board Report

On August 18, 2011, Mr. Solomon released a report summarizing 14 recent cases the Board considered involving employees' use of social media, including, Facebook, Twitter, YouTube, text messages, video, images, podcasts, and other multimedia communications. Without providing express

guidelines in the August 18 report on how an employer, whether unionized or not, can establish and enforce a lawful social media policy, the report discusses recent cases from the Board to shed light on activities the Board likely will or will not consider protected under the Act.

Out of the 14 cases discussed, the Board found in four that an employee's posts on Facebook or Twitter constituted "protected concerted activity;" in five cases, that an employee's posts on Facebook or Twitter did not warrant protection under the Act; in four cases, that some provisions of the employers' social media policies were overly broad and unlawful; and in one case, that the employer's media and press interview policy was lawful and valid.

Protected concerted activity

Many conversations that start in the workplace continue in social media. It is important for employers to understand that an employee's social media use likely may be considered protected concerted activity when the comments or posts involve shared concerns over terms and conditions of employment. Posts can be considered protected when they derive from or are a direct "outgrowth" of an earlier discussion among coworkers about their terms and conditions of work. Facebook or Twitter posts directed to coworkers to invite or induce further action also are likely to be considered protected concerted activity. Further, a post that is offensive or laced with profanity or sarcasm still may warrant protection under the Act if the content is derived from shared concerns about the terms and conditions of employment.

In one case, the employer, an ambulance service, terminated an employee for posting negative remarks about her supervisor on Facebook. The employer's Internet and blogging policy prohibited employees from making disparaging remarks when discussing the company or supervisors and from depicting the company in any media without its permission. From her personal computer outside of working hours, the employee posted a criticism about her supervisor which drew responses from her coworkers. The coworkers also wrote negative remarks about the supervisor, some of which included profane language. After the employer found out about the post, the employee was terminated for violating the employer's Internet policies. The Board found that the employee had engaged in a protected activity by exercising her right to discuss supervisory actions with coworkers.

It is important for employers to understand that an employee's social media use likely may be considered protected concerted activity when the comments or posts involve shared concerns over terms and conditions of employment.

Activities not protected by the Act

Social media posts that do not involve a discussion with other employees and are not directed to other employees, that do not discuss the terms and conditions of employment, or that include offensive or inappropriate comments directed toward an employer's clients are not likely protected under the Act. In one case, a bartender was terminated for posting a message on Facebook regarding his employer's tipping policy. Pursuant to the policy, waitresses were not allowed to share tips with bartenders. The employee had a conversation on Facebook with a non-coworker family member, complaining about the lack of raises and tips. The employee described the employer's customers as "rednecks" and stated that he hoped they would choke on glass as they drove home from the bar. The Board found the employee's posts were not made in concert with other employees, but solely on his own behalf, even though they concerned the terms and conditions of his employment.

Additionally, the Facebook conversation did not grow out of another conversation with a coworker, nor did any of his coworkers respond to his postings.

In a separate case, the Board found a journalist's termination was lawful. He was fired for tweeting unprofessional comments about his employer, local homicides, and criticisms about a local television station. The Board found that the posts were inappropriate and offensive and did not relate to the conditions of his employment or seek to involve other employees in issues related to employment. Therefore, they did not involve a protected activity.

Overly broad social media policies

In several cases, the Board found the employer's social media policy overly broad. These cases have provided employers with guidance on drafting a lawful policy. In one case, the employer's social media policy prohibited employees from using any social media that may violate, compromise, or disregard the rights and reasonable expectations as to privacy or confidentiality of any person or entity. It also prohibited any communication or post that constitutes embarrassment, harassment, or defamation of the employer, any other employee, officer, board member, and representative or staff member. The Board found these provisions overly broad, concluding that employees could reasonably construe the policy to prohibit protected conduct. The Board highlighted that the policy also provided no guidance as to what the employer considered to be private or confidential. Further, the policy included several broad terms, but no definitions or limits that would exclude protected activity from their reach.

The Board found several other social media policies overly broad, with terms and prohibitions that reasonably would be construed as prohibiting protected activity. In these policies, the employers prohibited employees, on their own time, from blogging about company business, posting anything that they would not want their manager or supervisor to see, and posting pictures or comments involving the company or its employees that could be construed as inappropriate.

Another provision the Board found overly broad included restrictions on revealing (including through photographs) personal information regarding coworkers, company clients, partners, or customers without their consent, without any limitation or examples of what is covered. The Board also found this provision could reasonably be construed as a restraint on protected activity.

Additionally, the Board found that forbidding employees from discussing the terms and conditions of employment or sharing information about themselves or fellow employees with each other or nonemployees violates the Act. It also concluded that prohibiting employees from using the employer's logos and photographs of the employer's store, brand or product, without written authorization, was unlawful. It found this ban was overly broad in that it could prevent an employee from posting pictures of employees carrying a picket sign depicting the employer's name, peacefully handbilling in front of a store, or wearing a t-shirt displaying the employer's logo in connection with a protest over terms and conditions of employment, all which are protected activities.

January 2012 Board Report

On January 24, 2012, Mr. Solomon issued a second report on more recent social media cases that have been decided by the Board. The January 24, 2012 report discusses social media policies and chronicles additional actions taken by the Board on unfair labor practice charges involving the use of social media by employees.

The January 2012 report reviews 14 charges, several of which allege that the language of the employer's social media policy violated the Act. For example, in one case the social media policy required employees who had identified themselves as employees of the employer on social media sites to state, each time they posted, that their comments contained only their personal opinions and did not necessarily reflect the employer's opinions. The Board found that provision unlawful because:

. . . requiring employees to expressly state that their comments are their personal opinions and not those of the employer every time that they post on social media would significantly burden the exercise of employees' Section 7 rights to discuss working conditions and criticize the employer's labor policies, in violation of Section 8(a)(1).

Employers should use great caution when writing social media policies.

The same policy also required employees to obtain approval to identify themselves as the employer's employees on social media sites. The Board also found this provision unlawful because:

personal profile pages serve an important function in enabling employees to use online social networks to find and communicate with their fellow employees at their own or other locations .... [T]his policy, therefore, [is] particularly harmful to the Section 7 right to engage in concerted action for mutual aid or protection and [is] unlawfully overbroad.

Another provision of that policy prohibited use of the company's name or service marks outside the course of business without prior approval of the employer's law department. The Board found this provision unlawful, stating:

Employees have a Section 7 right to use their employer's name or logo in conjunction with protected concerted activity, such as to communicate with fellow employees or the public about a labor dispute. We concluded that this provision of the policy could reasonably be construed to restrict employees' Section 7 rights to use the employer's name and logo while engaging in protected concerted activity...

Employers should use great caution when writing social media policies. These policies are receiving great scrutiny by the Board, and provisions that may appear harmless on their face, such as those noted above, may not be.

Recent Board Comments

On March 1, 2012, the Board's regional director in Fort Worth, Texas reminded attendees at a legal conference that it would be a violation if the employer takes action, in response to a Facebook or other social media communication, that would "reasonably chill" employees in the exercise of their Section 7 rights under the Act.

The regional director said that social media is a "hot, hot subject," with more than 100 cases involving Facebook postings filed with the Board between 2009 and 2011. The standard that the Board applies in Facebook and other social media cases are rules that have evolved over 70 years of case law. "We are not saying that an employee can say or do anything; it has to be in concert with other employees and it must be protected. It can't be so egregious or it will lose protection under the NLRA," the regional director said.

In social media cases, the regional director reminded attendees that the Board will apply its standard analysis for protected concerted activity. She explained that the Board generally looks at four factors when deciding whether employee speech amounts to protected concerted activity—the place of the discussion, the subject matter, the nature of the employee's outburst, and whether the outburst was provoked by the employer's unfriendly practice.

Equal Employment Opportunity Commission

Employers that use social media to make employment decisions "need to be consistent" in order to avoid claims of disparate treatment or disparate impact under Title VII of the 1964 Civil

Rights Act, according to a trial attorney with the EEOC who spoke at an August 26, 2011 workshop.

The EEOC attorney advised employers to set clear guidelines on using social media to research potential job candidates. He said this is necessary because employers are privy to a great deal of information "in cyberspace" about applicants to which they previously did not have access. By way of example, the trial attorney mentioned that a job candidate could have posted details on a social networking site about being a breast cancer survivor or a paraplegic. "How do we control employers' legitimately trying to find out information about prospective employees while not violating the law?" he queried. He said, "If you wouldn't ask for it during an interview, don't search for it online." "It could possibly get you in trouble."

> "If you wouldn't ask for it during an interview, don't search for it online."

The EEOC has also addressed the intersection between social media and genetic information. Congress enacted the Genetic Information Nondiscrimination Act of 2008 (GINA) to prohibit discrimination based on genetic information and restrict the requesting and disclosure of such information. GINA not only prohibits employers from discriminating against employees and job applicants but also prohibits employers from acquiring employees' genetic information. In early 2011, the EEOC released regulations that make it illegal to conduct "an Internet search on an individual in a way that is likely to result in a covered entity obtaining genetic information." Fortunately, in the regulations, the EEOC concluded that the sharing of information over Facebook, Twitter, and other social networking sites is analogous to discussing such matters around the water cooler — with management overhearing it. Such a scenario falls within the "inadvertent acquisition" exception to GINA's prohibition on the employer's acquisition and possession of employees' genetic information.

Securities and Exchange Commission

Financial advisors may not advertise using client endorsements or testimonials. The increase in the use of social media connections, such as "like" buttons, increases the potential to cross regulatory lines, because such connections can be viewed as an endorsement. In addition, given the particular facts and circumstances, such connections could also be viewed as testimonials.

On January 4, 2012, the Securities and Exchange Commission (SEC) issued guidelines for financial advisors. The SEC found that firms tend to have overlapping policies and procedures that apply to advertisements, client communications, and electronic communications, which were confusing because they often do not specifically identify social media.

The SEC suggested reviewing internal compliance programs to determine if social media use is addressed and ensure that the rules are currently being followed. The factors they focus on include:

- Usage guidelines: Base restrictions upon the risk to the firm, which sites are approved, and which functionalities are approved.
- Content standards: Suggest clear guidelines for content or use of preapproved content.
- Monitoring: Determine how to appropriately monitor use and the frequency of monitoring.
- Firm resources: Determine if there are available resources for compliance and monitoring.
- Participation: Determine the appropriateness of a site.
- Training: Get training on how to appropriately use social media, consider requirement of certification.

- Personal/professional sites: Determine if the use is through a firm-sponsored profile or through an individually created profile. Review the potential risks for profiles that are part of a corporate enterprise.
- Information security: Review and address potential information security risks with social media use.
- Recordkeeping and document retention: Determine whether or not recordkeeping is being adhered to based on the Advisers Act if it applies to the content and that documentation is accessible as determined by federal securities laws.

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 coworkers, 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.

When employees use social media, however, to harass coworkers, 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.

Potential theories of employer liability for employees' misuse of social media

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 coworkers, 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 coworkers 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 legal claim 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. Employees may also act more deliberately, such as a disgruntled employee revealing a company's trade secrets and other proprietary information on a blog.

According to FTC Guidelines 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.

Reporting requirements for child pornography. Several 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. 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) Guidelines. According to FTC Guidelines 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. 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.

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.

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. As discussed above, the Act 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 Act; 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 or Facebook page, an employer must determine if the employee has engaged in protected concerted activity.

Legal off-duty activities. Watch out for unique state laws. Some states have "lawful conduct" laws that may protect an employee or applicant's legal off-duty activities. Thus, in some states, an employer may be prohibited from terminating an employee who, for example, posts pictures of himself intoxicated at a party on social media (assuming the employee is over 21 years old). In contrast, the employer may have more leeway where the conduct is illegal. The following states have lawful conduct laws:

Some states have "lawful conduct" laws that may protect an employee or applicant's legal off-duty activities.

California: *Provides that no employee shall be discharged or otherwise discriminated against for lawful off-duty conduct. The law entitles any employee who is discharged, threatened with discharge, demoted, suspended, or discriminated against in any manner in the terms and conditions of his or her employment to reinstatement and reimbursement for lost wages and work benefits.*

Colorado: *Makes it illegal for an employer to terminate an employee because that employee engaged in any lawful activity off the employer's premises during nonworking hours unless the restriction 1) relates to a bona fide occupational requirement or is reasonably and rationally related to the employment activities and responsibilities of a particular employee or a particular group of employees; or 2) is necessary to avoid, or avoid the appearance of, a conflict of interest with any of the employee's responsibilities to the employer.*

Illinois: *Prohibits workplace discrimination on the basis of the use of lawful products except where the employer is a nonprofit organization that, as one of its primary purposes or objectives, discourages the use of one or more lawful products by the general public.*

Minnesota: *Prohibits an employer from refusing to hire a job applicant or disciplining an employee for using lawful consumable products, if the products are used off the employer's premises outside of working hours. Provides for an exception related to a bona fide occupational requirement that is reasonably related to the employment activities or responsibilities of a particular employee or group of employees or where it is necessary to avoid a conflict of interest or the appearance of a conflict of interest.*

Montana: *Provides that an employer may not refuse to employ, license, or discriminate against an individual with respect to compensation, promotion, or the terms, conditions, or privileges of employment because the individual uses a lawful product off the employer's premises during nonworking hours, unless such use 1) affects an individual's ability to perform job-related employment responsibilities or the safety of other employees; 2) conflicts with a bona fide occupational qualification that is reasonably related to the individual's employment; 3) conflicts with a professional service contract where the unique nature of the services provided authorizes the employer to limit the use of certain products; or 4) is prohibited by a nonprofit organization employer that, as one of its primary purposes or objectives, discourages the use of one or more lawful products by the general public.*

Nevada: *Makes it unlawful for an employer to fail or refuse to hire a prospective employee or to discharge or otherwise discriminate against an employee concerning his compensation, terms, conditions or privileges of employment, because he engages in the lawful use of any product outside working hours and off the employer's premises if that use does not adversely affect his ability to perform his job or the safety of other employees.*

New York: *Makes it unlawful for an employer to make hiring or firing decisions, or otherwise discriminate against an employee or prospective employee because of that individual's legal use of consumable products or legal recreational activities outside of work hours, off of the employer's premises, and without use of the employer's equipment or other property. There is an exception for protected activity that creates a material conflict of interest related to the employer's trade secrets, proprietary information or other proprietary or business interest.*

North Carolina: *Prohibits an employer from refusing to hire a prospective employee, or discharging or otherwise discriminating against any employee with respect to compensation, terms, conditions, or privileges of employment because the employee or prospective employee lawfully uses lawful products off the employer's premises during nonworking hours and such use does not adversely affect the employee's job performance or the person's ability to properly fulfill the responsibilities of his position or the safety of other employees.*

Wisconsin: *Prohibits any employer, labor organization, employment agency, licensing agency, or any other person from engaging in any act of employment discrimination on the basis of the use or nonuse of lawful products off the employer's premises during nonworking hours.*

Laws related to political activities and affiliations. Many states, including California, prohibit employers from regulating employee political activities and affiliations or influencing employees' political activities. Taking action against an employee for objectionable political speech could violate these restrictions.

Discrimination claims. 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. 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.

Whistleblower statutes. 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 "providing information, causing 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." 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.

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 a human resources professional knowledgeable in this area to manage the risks inherent in any adverse employment decision.

Monitoring and Regulating Employees' Use of Social Media

Supreme Court finds government employer's search reasonable

In a unanimous decision, the U.S. Supreme Court held that the City of Ontario's review of transcripts of an employee's text messages sent and received on a City-issued pager was a reasonable search under the Fourth Amendment. *City of Ontario, Calif. v. Jeff Quon, et al.*, No. 08-1332 (June 17, 2010).

The Court avoided deciding whether public employees have a reasonable expectation of privacy in text messages sent on employer-owned equipment under the Fourth Amendment and what particular standard ought to apply in making that determination. It acknowledged that rapid changes in communications and the means by which information is transmitted, as illustrated by advancements in technology and what society views as proper behavior, created significant challenges to setting legal standards for the workplace that would survive the test of time. The Court noted, "Prudence counsels caution before the facts of the instant case are used to establish far-reaching premises that define the existence, and extent, of privacy expectations enjoyed by employees when using employer-provided communications devices."

So, the Court assumed, without deciding, that the employee had a reasonable expectation of privacy in his text messages and the case could be decided on narrower grounds, i.e., whether the search was reasonable under well-defined Fourth Amendment standards.

Under the Fourth Amendment, a government employer is permitted to conduct a workplace search without a warrant where it is (i) "justified at its inception" and (ii) reasonable in scope. A search is "justified at its inception" where it is conducted for a "noninvestigatory, work-related purpose" or for the "investigation of work-related misconduct." A search is reasonable in scope where the measures used are reasonably related to the objectives of the search and not excessively intrusive under the circumstances.

All employers, public and private, must be prepared with comprehensive computer and electronic equipment usage policies.

Applying these standards, the Court held that the City's review of Quon's text message transcripts was reasonable. According to the Court, the search had a clear noninvestigatory, work-related purpose at its inception—to evaluate whether the monthly character limit was sufficient for the City's needs and to ensure that employees were not paying out-of-pocket for work-related expenses.

The extent of an expectation of privacy, the Court reasoned, is relevant to assessing whether the scope of a search is reasonable. Moreover, "employer policies concerning communications will of course shape the reasonable expectations of their employees, especially to the extent that such policies are clearly communicated," the Court said.

All employers, public and private, must be prepared with comprehensive computer and electronic equipment usage policies. The Court noted that these policies will help shape an employee's expectation of privacy. Further, it is critical that practices and policies be consistent, reflect current technologies, and be clearly communicated.

Employers also should consider requiring employees to acknowledge in writing that they received and reviewed these and similar policies and procedures, particularly as new technologies are introduced. Because this area of the law continues to evolve, as evidenced by the Court's refusal to expand its holding beyond the narrow confines on this case, a well-drafted and communicated policy will be critical in addressing an employee's expectation of privacy in connection with electronic communication and preserving the employer's ability to review and monitor those communications.

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." 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. 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. 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.

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.

Strategies for Regulating Electronic Communications

Whether employees are communicating with friends outside the company or with coworkers 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.

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.

In compliance with the decisions of the National Labor Relations Board discussed above, employers may take several actions. Employees should be warned that postings regarding: (1) proprietary and confidential company information; (2) discriminatory statements or sexual innuendos regarding coworkers, management, customers, or vendors; and (3) maliciously false statements regarding the company, its employees, customers, competitors, or vendors will not be tolerated and will subject the individual to discipline. Confidential and proprietary information of the Company must be appropriately defined to avoid running afoul of recent NRLB decisions.The policy should specify that these prohibitions apply to postings and blogging occurring at any time, on any computer.

Again, in compliance with the decisions of the National Labor Relations Board discussed above, 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). Employers can also implement a policy that reduces the level of privacy employees expect in their work computer systems, email, 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.

Question of Social Media Account Ownership Need Not Be a Problem for Employers

Forward-thinking companies also embrace social media, networking sites and blogs for, among other things, branding, client development and service, research, and marketing. While the benefits could be significant, social media use is not without challenges for employers.

One hot area is disputes between employers and departing employees over the ownership of social media accounts. Such disputes are on the dockets of several federal district courts throughout the country.

One hot area is disputes between employers and departing employees over the ownership of social media accounts. Such disputes are on the dockets of several federal district courts throughout the country. Employers in these cases are asserting ownership over company Twitter and LinkedIn profiles claiming, among other things, that they contain "trade secrets." Employees dispute these contentions by pointing out that there is nothing "secret" about social media profiles and that employers have no inherent property interests in Twitter and LinkedIn accounts.

In *PhoneDog v. Kravitz,* 2011 U.S. Dist. LEXIS 129229 (N.D. Cal., Nov. 8, 2011), for example, a federal court in California denied a motion to dismiss where the employer sought damages for each Twitter follower that a departing employee took with him. The employee was given use of and maintained a Twitter account for the employer's business during his employment. When he left, he changed the Twitter account handle and continued to use the account. PhoneDog and its former employee do not have a written agreement pertaining to ownership of the disputed Twitter account. The company alleged several claims against the departing employee, including misappropriation of trade secrets, conversion, and tortious interference with prospective advantage.

Another example is *Eagle v. Morgan,* 2011 U.S. Dist. LEXIS 147247 (E.D. Pa., Dec. 22, 2011). A federal court in Pennsylvania denied a motion to dismiss a suit over an employee's LinkedIn account. The disputed LinkedIn account was developed by company personnel and used for company business. As in *PhoneDog,* the parties do not have a written agreement as to ownership of the account.

These cases may be headed into prolonged and extensive litigation. They may have been avoided had the parties entered into clearly written agreements at or near the inception of the employment relationship. Such an agreement was upheld in *Ardis Health, LLC v. Nankivell,* 2011 WL 4965172 (NRB) (S.D.N.Y., Oct. 19, 2011). A federal court in New York granted a preliminary injunction requiring an employee to give her employer access to social media sites pursuant to obligations under the parties' written Nondisclosure and Rights to Work Product Agreement.

Employers who profit from their employees' use of social media should carefully analyze these issues. In many cases, a properly drafted agreement delineating the property interests in employee work product will save employers from time-consuming and expensive litigation over ownership of social media accounts.

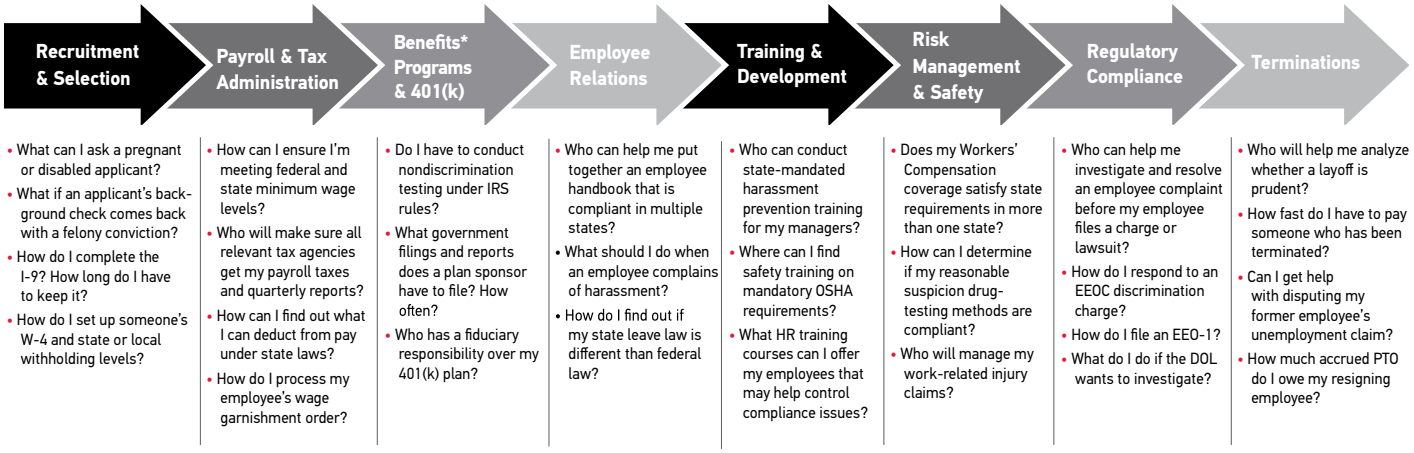
Conclusion

As you can see, the law of social media is constantly in flux. With frequent changes in the laws and regulations by the federal government, state governments and courts, it is difficult to keep up all of the new rules, determine how they affect you, and stay in compliance. ADP TotalSource® is well versed in legal developments, and it stays on top of new rules that affect your business. ADP TotalSource timely updates clients about new developments of significance and offers clear action plans that allow clients to focus on their business objectives.

The ADP TotalSource® Solution

Compliance Support in the HR Value Chain

The regulatory compliance support that ADP TotalSource provides to its clients is not just one link in our HR Value Chain – it is integral to every link in the chain, from hiring to firing and everything in between. With an array of products and services in their tool belts, our professionals stand ready to help you implement a strong HR infrastructure that will allow you to proactively address employee-related issues and use best practices that will help you minimize potential employer liability.



For more information on Regulatory Compliance Management Programs from ADP TotalSource call (800) 447-3237 or visit www.adptotalsource.com.

*The health insurance option and related services are not available in select markets.
ADP TotalSource does not provide guidance or services for client-sponsored plans.

HR.Payroll.Benefits.

About ADP TotalSource

A part of ADP's Employer Services Division, ADP TotalSource provides employers with a comprehensive Human Resources outsourcing solution that helps reduce the costs and complexities related to employment and human resources management. For companies and HR departments that seek to return the focus to their core processes, ADP TotalSource removes administrative and regulatory burdens, allowing more effort to be expended on strategic initiatives. Our affordable outsourcing opportunities have the ability to significantly reduce operating costs and streamline business operations, paving the way for growth and competitive gains. To learn more about how ADP TotalSource can help your business call **1-800-HIRE-ADP (800-447-3237)** or visit us online at **www.adptotalsource.com.**

About Jackson Lewis

Jackson Lewis is a strategic alliance partner with ADP TotalSource. For more than 50 years, Jackson Lewis has placed a high premium on preventive strategies and positive solutions in the practice of workplace law. With nearly 700 attorneys practicing in 48 offices nationwide, Jackson Lewis has a national perspective and sensitivity to the nuances of regional business environments. **www.jacksonlewis.com.**

Notes

Notes

Notes

IN THE BUSINESS OF YOUR SUCCESS℠

jackson lewis
Preventive Strategies and Positive Solutions for the Workplace®

HR. Payroll. Benefits.

MKT190 0812 Printed in the USA ©2012 ADP, Inc.