



Are You Building a House of Cards? Social Networking in the Office

BY ELIZABETH J. MCNAMEE AND KIM S. MAGYAR

Social media and next generation internet tools are changing how people interact and communicate — even in or about the workplace. Web applications that used to passively provide information for viewing now allow and encourage interactive information-sharing and collaboration. Often called Web 2.0, these new applications — including social networking sites, blogs, video-sharing sites, wikis, discussion forums, file-sharing and other user-generated media — allow a company's employees, vendors and customers to readily share information about the company and its products or services.¹ In this article, we will define social media and address its use in the workplace. We will analyze the more common legal concerns related to employee, as well as company, use of social media. And finally, we will provide considerations to take into account when drafting and implementing a social media/social networking policy.

Social media defined

Information shared through social media is designed to be disseminated through social interaction, often using web-based technologies. Social media sites allow users to interact with each other as contributors to the content, transforming the traditional broadcast media monologue (e.g., a press release or a news story) into a dialogue. Engaging in social media is inexpensive; it's accessible. Virtually anyone with internet access and a computer can publish, access, modify or comment on information about anyone or anything.

Statistics reflect the pace at which social media use is assimilating into popular culture. A span of 38 years passed before radio reached an audience of 50 million. Television crossed the 50 million mark in 13 years, yet the internet reached this same benchmark in only four years. By comparison, Facebook reached more than 100 million users in less than nine months. On Twitter, the combined number of people following Ashton Kutcher and Ellen Degeneres is greater than the population of several countries, including Ireland and Norway.² Similarly, information is being exchanged at as rapid a pace. On average, 1.5 million pieces of content are shared every day on Facebook alone. On YouTube, 24 hours of video is uploaded to its site every minute. Furthermore, social media applications for cell phones mean that users can share experiences and information anywhere, at anytime, with nearly anyone.

The population no longer views social media as tools relegated to kids and bloggers seeking to assimilate with others who have similar interests. According to a recent survey, 78 percent of lawyers and 71 percent of in-house counsel have joined an online social network, and 23 percent of lawyers and 20 percent of in-house counsel use their online social networks for professional purposes.³

Although new social media sites are launched daily, Facebook, LinkedIn, You-



ELIZABETH J. MCNAMEE is senior employment counsel at TSA Stores, Inc. dba The Sports Authority, where she oversees employment-related litigation for the company nationwide. She provides counsel to the company's corporate, field and distribution centers' human resources teams, and advises company management on employment/labor-related issues. McNamee can be contacted at emcnamee@thesportsauthority.com.



KIM S. MAGYAR is an attorney with Snell & Wilmer, L.L.P.'s Phoenix Labor and Employment Group. Her practice generally focuses on management-side employment matters and litigation, and she regularly counsels her clients regarding employment law issues, including social media concerns. Magyar can be contacted at kmagyar@swlaw.com.

Tube and Twitter are arguably the most popular, and all have found their way into the workplace. These four social media sites and more are commonly used for advertising, branding, marketing, and employee recruiting and screening. Each site offers its own unique and distinct features. Facebook is the largest online network, with over 400 million active users (defined as users that have returned to the site in the last 30 days). Facebook seeks to help people communicate more efficiently with their friends, family and coworkers. Its mission is to give people the power to share and make the world more open and connected. LinkedIn is a professional networking site with more than 65 million members. It seeks to connect the world's professionals to make them more productive and successful. According to its site, executives from all Fortune 500 companies are LinkedIn members, and a new member joins LinkedIn approximately every second. YouTube declares itself the "World's most popular online video community." Users can upload, view and share video. Twitter is a micro-blogging and social networking service that allows users to send and read free text-based messages of 140 characters or less, known as "Tweets."

Organizations are still ascertaining how these and other social media sites should be used in the workplace. For example, a Deloitte LLP workplace study revealed that while 60 percent of business executives say they have the "right to know" how employees portray themselves and their employer online, nearly 53 percent of employees contend that their "social networking pages are none of an employer's business."⁴ Nevertheless, there is no denying that social media sites are regularly used in the workplace. The same study showed that 55 percent of employees visit social networking sites at least once weekly, and 21 percent admit doing so during work hours (a number almost certain to be underreported). Thirty percent of executives use social networking as part of their business and operations strategy and 53 percent of employees believe that new Web 2.0 tools are "better than those provided by my employer."⁵ The potential risks to employers are also real and potentially significant. Indeed, the Deloitte study revealed that 74 percent of employees say it's easy to damage a company's reputation using social media.

Social media legal hazards

Regardless of whether social media use takes place during work hours or afterward, or whether it is authorized or sanctioned by the employer, employers may face liability under many different legal theories. These include, but are

not limited to, the following: failure to pay wages for time worked under the Fair Labor Standards Act; discrimination and harassment under Title VII; violation of the National Labor Relations Act; invasion of privacy; defamation; wrongful termination; and false or deceptive advertising under the Federal Trade Commission guidelines.

FLSA

The Fair Labor Standards Act (FLSA), 29 USC §201, and many corresponding state laws, generally require employers to pay their non-exempt, hourly employees⁶ a minimum wage plus a premium for hours worked in excess of 40 hours per workweek — otherwise known as “overtime.” Currently, the federal minimum wage is \$7.25 per hour, but it can be higher based on state-specific law. As already stated, overtime is generally required if an employee works more than 40 hours in a workweek, but it can also

The protected class information that the employer inadvertently learns, which the employer does not want to know, cannot be “unlearned.”

be required if the time worked exceeds a certain number of daily hours, pursuant to state-specific law.

The FLSA’s relevant terms are defined broadly — an “employee” is “any individual employed by an employer;” and “employ” means “to suffer or permit to work.” Under these broad definitions, employers must provide compensation, including overtime, to non-exempt employees who engage in work-related activities. This would include employment-related social media activities. Employers should be particularly mindful of tracking time spent in these activities outside normally scheduled working hours.

Furthermore, the Department of Labor’s regulations make clear that it is management’s duty “to exercise its control and see that the work is not performed if it does not want it to be performed.”⁷ It is management’s duty to control employees’ work hours through a combination of clear policies and vigorous enforcement, including appropriate disciplinary action.

The Department of Labor has warned employers that management simply “cannot sit back and accept the benefits” without compensating employees for their work, even

if the work is not requested or assigned by the employer. Consider the scenario where a non-exempt marketing assistant uses his iPhone to send an after hours Tweet about a presentation recently provided by the employer. This simple act could be construed as “work” under the FLSA, such that the employee must be compensated for the time spent, even if the employer did not ask him to send the Tweet.

Discrimination/harassment

Social media use also provides the potential for discrimination and harassment — it is yet another location where discrimination and harassment may occur. As such, it is important that an employer’s anti-discrimination and harassment policies explicitly state that they apply to employee use of social media, regardless of whether such use takes place during or after work hours.

Employers also run the risk of violating Title VII of the Civil Rights Act of 1964 as amended, 42 U.S.C. §2000e, if they use social media in their recruitment of candidates, and then make employment decisions based on protected class information learned from the website(s). Does this mean that employers should refrain from using social media sites for pre-hiring screens? Not necessarily. Rather, employers should carefully weigh the benefits of engaging in pre-hiring screening using social media websites against the risks associated therewith. Social media sites often provide more information concerning an applicant than an employer wants to know, such as his ability to spell or write coherently. An employer may also learn an applicant’s age when they stumble his high school graduation date. Or the employer may learn the applicant’s religious beliefs based on online posts about attending a particular church or temple. The protected class information that the employer inadvertently learns, which the employer does not want to know, cannot be “unlearned.” Although knowledge of this information does not, by itself, defeat all defenses to a claim of discrimination and harassment, it will bar the employer’s first-line defense of “We didn’t know he was a member of [insert protected class here].”

Employers may also face discrimination and harassment lawsuits from current employees. Consider a supervisor who befriends certain subordinates on Facebook, but who does not befriend other subordinates who are members of a protected class. Although this action likely would not constitute an adverse employment action sufficient to support a claim of discrimination by itself, these types of claims are not uncommon in the workplace, and this type of evidence could provide the employee with ammunition for a discrimination claim when the employee is ultimately demoted or terminated.

Concerns may also arise under the Americans with Disabilities Act, 42 U.S.C. §12101 *et seq.* Consider an employ-

er who scans an employee's social media page and notices the employee complaining about a condition that could be claimed as a disability, such as back pain or diabetes. Does the employer now have knowledge of the disability such that he must interact process the employee to determine whether an accommodation at work is necessary?

Finally, employers may face liability for applying policies regarding social media use in a discriminatory fashion. By way of example, a flight attendant, who was fired for posting "revealing" pictures of herself while wearing her airline uniform on her blog, sued her employer alleging that male employees who had posted pictures of themselves engaging in similar "unsuitable conduct" while in uniform had not been disciplined. Employers should consider these risks and determine a consistent position on social media use before employing and enforcing social media use haphazardly.

NLRA

Employers must be careful not to violate the National Labor Rights Act (NLRA) when enforcing and policing social media use. For example, Section 7 of the NLRA, 29 U.S.C. §517, provides that, "[e]mployees shall have the right to self-organization, [and] to form, join, or assist labor organizations, to bargain collectively through representatives of their own choosing, and **to engage in other concerted activities** for the purpose of collective bargaining **or other mutual aid or protection.** ..."

Additionally, Section 8 of the NLRA, 29 U.S.C. §518, states that it shall be an unfair labor practice for an employer to "interfere with, restrain, or coerce employees in the exercise of the rights guaranteed in section [7] of this title. ..."

These rules have broad applicability, which extend beyond the union context. For example, many workplaces discourage employees from mutually discussing topics such as wages and working conditions. Section 7 of the NLRA, however, protects an employee's right to discuss wages and working conditions with other employees. Thus, an employee who writes about his pay or working conditions with other employees on social media may have protection for such statements under the NLRA if access to the site is limited to other employees.

An employer may also face liability under the NLRA, even in situations where a potentially unfair labor practice is never enforced. Where an employer's work rules are "likely to have a chilling effect on [an employee's statutory] rights, the National Labor Relations Board may conclude that their maintenance is an unfair labor practice, even absent evidence of enforcement."⁸ Additionally, even if an employer's policy or rule doesn't explicitly restrict protected activity, the rule or policy may still violate the NLRA if employees would reasonably construe the language to prohibit the protected activity.

Privacy

Employers must also be aware of, and address, employee privacy rights when using social media, particularly from work computers. Employees may have privacy rights on their office computers — particularly where the office is a private one and kept locked, and the computer is password protected with the password known only to the employee user.⁹ These common law rights to privacy may exist even where the employer has a policy attempting to negate any expectation of privacy, but where the company has failed to enforce this policy.

Additionally, an employee may have privacy rights under the Stored Communications Act (SCA), 18 USC §2701 et seq., a part of the Electronics Communications Privacy Act. The SCA provides for a civil cause of action against any person or entity who, "with a knowing or intentional state of mind...(1) intentionally accesses with-

An employer may also face liability under the NLRA even in situations where a potentially unfair labor practice is never enforced.

out authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system. ..."

Recently, a court upheld a cause of action under the SCA where the employer intentionally, and without authorization, accessed the employee's personal, password-protected America Online email account.¹⁰ Similarly, a jury found a violation of the SCA after an employer fired two employees for their role in creating a password-protected MySpace chat group where employees were invited to complain about their job. It was found that management had coerced an employee into giving the employer the password, and thus, the employer had accessed the chat group without authorization.¹¹

The SCA was also recently applied by the Central District Court of California in the *Crispin v. Audigier* case, to prohibit the disclosure by social media sites, including Facebook and MySpace, of private messages sent by users

without such user's authorization, even pursuant to a lawful subpoena.

As a result, employers should be cautious of employee privacy rights by minimizing any employee expectation of privacy through a computer-technology use/privacy policy, which explicitly states that the employer has the right to monitor all activity. The policy should make clear that the employee has no expectation of privacy for anything entered into the company's computers or other information technology system. Employers should monitor and enforce their policies regularly, consistently and without discrimi-

Recently, a court upheld a cause of action under the SCA where the employer intentionally, and without authorization, accessed the employee's personal, password-protected America Online email account.

nation. Employers, however, should be wary of monitoring all social media use, particularly password-protected personal sites and accounts, without risk of encroaching upon employee privacy rights.

Defamation/libel

Generally, defamation is a false, negative statement communicated to another, and libel occurs when the false, negative statement is published. Because the potential for damage is significant in the social media context, given the rapid pace at which information may be disseminated to large numbers of people, employers must take care in ensuring that employees are not using social media to make defamatory statements. An employer may be liable, for example, for knowingly allowing an employee to defame a competitor to gain a competitive advantage in the industry.

Wrongful termination

In most states, employment is "at-will," meaning that employees may be terminated for any reason or no reason, as long as it is not an illegal reason (e.g., termination based upon membership in a protected class). In these states, terminating an employee for social media use, even if done outside of work hours, will likely be upheld. For

example, an employer may terminate an employee who blogs negatively about the employer in an at-will state. Employers must be careful, however, before terminating employees in states that have enacted so called "lifestyle discrimination" statutes, which seek to protect legal, off-duty conduct such as blogging.

Non-at-will employment states may prohibit termination unless done with cause. Furthermore, even in at-will employment states, employers with personnel policies or handbooks that state an employee will not be fired except for good cause, or after a specific process is followed, may inadvertently create a cause of action for wrongful termination. In these instances, an employer must take care to follow its termination policies and procedures to ensure that it is not terminating employees in violation of statutory or policy rights.

FTC guidelines

Recently, the Federal Trade Commission (FTC) issued revisions to its federal guidelines to protect consumers from false and deceptive online advertising. These revisions, found at 16 C.F.R. Part 255, address the use of endorsements and testimonials in online advertising. Specifically, the new guidelines provide employer liability for false or unsubstantiated statements about the employer's products or services — even if the comments are not authorized or known by the employer.

By way of example, a company requests that a blogger try its new lotion and write a review of the lotion on the blog. Although the company does not make any specific claims about the lotion's attributes and the blogger does not ask the employer whether there is substantiation for the claim, in the review, the blogger writes that the product cures eczema, and recommends the product to blog readers who suffer from this condition. The employer may be subject to liability for the misleading or unsubstantiated representations made through the blogger's endorsement or testimonial. Of course, the blogger may also be subject to liability for misleading or unsubstantiated representations made in the course of the endorsement, and for failing to disclose, clearly and conspicuously, that she is being paid for her services. In order to limit potential liability, the company should provide guidance and training to bloggers concerning the need to ensure that their statements are truthful and substantiated. The company should also monitor bloggers who are being paid to promote its products, and take steps necessary to halt publication of deceptive representations when discovered.

Similarly, employers may be liable for employees who blog about services or products without first disclosing their "material relationship" with the employer as a result of their employment. The FTC provides the following ex-

Top 10 Employment Law Considerations for Social Media

10. The nature of information posted on social media/networking sites often blurs the line between an individual's professional and private life. If you post, use caution in posting and limit access to data where possible. Once data is posted, it remains accessible even if later deleted.
9. Unless your system blocks access to social media/networking sites, assume your employees are accessing these sites at work. A recent workplace study by Deloitte found that 55 percent of employees admitted visiting a social networking site a minimum of once weekly, and 21 percent admitted doing so during work hours.
8. Social media is here to stay, so embrace it. Savvy marketing and business development departments have latched onto the reach these sites offer. According to the same Deloitte study, 34 percent of individuals believe companies should have a presence in the social media milieu.
7. Consider how and whether social media should be used in your recruiting efforts. Remember that once information is learned, a presumption exists that it is always known. For instance, knowledge learned from a social networking site about an applicant's race, age, marital status, religious practice or disability may be used as the basis of a later discrimination in hiring allegation.
6. Become versed in "lifestyle" discrimination statutes in the states in which you practice or operate. Generally, these statutes prohibit discrimination based upon lawful, off-duty conduct, such as limiting available discipline for the employee who, in his off-duty time, criticizes your company or client. To dissuade "bad behavior," consider broadening policies to include on-duty and off-duty postings or public exchanges that mention or relate to your company/client. Explain that all such postings must adhere to the guidelines and policies stated in your handbook. Or, consider adding a disparagement clause to your conflict of interest policy.
5. If an hourly, non-exempt employee's job duties require, or if you ask, that she update company blogs or other social media sites, ensure that the employee is paid for all time worked in compliance with state and federal law, including after hours and overtime work.
4. Confidential or proprietary data and trade secrets can swiftly and effortlessly be disseminated through social media. To protect your company's most valuable confidential and intellectual property, regularly police social media sites to ensure that this information is not inappropriately disclosed.
3. Do not assume the inapplicability of any laws to your workforce. For instance, an overly broad confidentiality provision in your policies may be found to unlawfully restrict an employee's lawful discussion of wages and other terms and conditions of employment under the NLRA even if your workforce is not unionized.
2. Employees may have common law or statutory privacy rights to information sent, accessed or stored within their company-issued computers based on state law. Ensure that your company's policies clearly remove any reasonable expectation of privacy and are compliant with state law nuances.
1. When in doubt, contact your employment/labor law specialist and implement a comprehensive social media policy to address social networking use by employees. Remember, even once implemented, a policy is only as good as its enforcement.

ample: An online message board designated for discussions of new music download technology is frequented by MP3 player enthusiasts. They exchange information about new products, utilities and the functionality of various playback devices. Unbeknownst to the message board community, an employee of a leading playback device manufacturer has been posting messages on the discussion board, promoting the manufacturer's product. Knowledge of this poster's employment likely would affect the weight or credibility of her endorsement. Therefore, the poster should clearly and conspicuously disclose her relationship with the manufac-

turer to members and readers of the message board.

Employees who fail to disclose the employment relationship may subject the employer to liability for false or misleading statements, even where the employee's statements are posted on a site that is not maintained by the employer and without the employer's request. For these reasons, it is essential for employers to take appropriate steps to address social media use, including who may speak on the company's behalf, to ensure that material relationships are adequately disclosed and that disclaimers are used where appropriate.

ACC Extras on... Social Networking in the Office

ACC Docket

- *Tracking Employees Using Technology (July 2009)*. Need to know what your staff is doing when they're on company time, but away from the office? This article explains how employers can implement GPS tracking without infringing on individual privacy rights. www.acc.com/trackempls_tech_jul09
- *The Millennial Generation's Wireless Work Styles: Cutting Edge or Slippery Slope? (April 2009)*. The revolution has not only been televised — it's been beamed, emailed and scanned. Find out the risks of touch-button technology and strategies for in-house counsel to protect sensitive company information? www.acc.com/docket/mil_wireless_apr09

Webcast

- *The Millennial Generation in the Digital Workplace: Emerging Data Security, Privacy, Harassment and Liability Issues (Nov. 2008)*. This webcast transcript examines digital issues in the workplace in light of the "Millennial" generation of employees. www.acc.com/web/mil_digwkpl_nov08

Program Material

- *Can We Control Blogging, IM & Other Employee Communication Inside the Workplace and Beyond (Dec. 2007)*. What your employees are saying may be putting your organization at legal risk. This panel discusses employee rights and workplace laws implicated in controlling these

communications, and effective corporate policies and practices. www.acc.com/empl-wkplcomm_dec07

InfoPAKSSM

- *Technology Primer (April 2008)*. Designed for use by law departments with between one and five lawyers, this material is intended to provide information on technology issues within the in-house legal department. www.acc.com/infopaks/techprim_apr08
- *Email and Internet Policies (Feb. 2007)*. Explore the relationship between employee access to the internet and email; employer regulation and monitoring of internet use addresses; and new issues presented by the increased use of electronic means of communication and their effect on the process of discovery. www.acc.com/infopaks/email_inter_feb07

Article

Rules of Engagement for Online Networking (Nov. 2008).

Read this article from ACC Alliance Partner, Robert Half Legal, and find key points on using online networking in a professional setting. www.acc.com/rules_online_ntwrk_nov08

ACC has more material on this subject on our website. Visit www.acc.com, where you can browse our resources by practice area or use our search to find documents by keyword.

Other risks

There are other significant risks inherent to social media use, such as concerns over intellectual property. For example, employers should have policies that address the use and disclosure of their confidential, proprietary and/or trade secret information, as well as the use of their company trademarks and other intellectual property. While employers will often address these concerns in other policies, a comprehensive social media policy should reaffirm these commitments and remind employees of their duties in this regard.

Some employers believe that only an outright ban on social media use in the workplace can remedy confidentiality and intellectual property concerns. However, this approach is nearly impossible to enforce in a non-discriminatory way, and could leave the employer subject to liability for lawsuits, as described in more detail herein. Moreover, this type of ban would not prohibit employees from discussing their employer or their workplace on

social media sites during each employee's own "personal" time. Instead, a comprehensive social media policy should be used to address social media use with regards to the employee's regular work duties, and personal, off-the-clock time.

Lawyers face additional unique risks when it comes to social media use. Lawyers who post and answer fact-specific legal questions on LinkedIn, for example, may inadvertently create an unintended attorney-client relationship. Lawyers who blog about their work may unintentionally violate ethics rules relating to confidentiality, including ABA Model Rule 1.6, which prohibits revealing "information relating to the representation of a client." Similarly, a lawyer who provides specific legal advice via a social media site to a participant in another state, where that lawyer is not licensed to practice, may unwittingly engage in the unauthorized practice of law in violation of ABA Model Rule 5.5.


Policy considerations

According to Deloitte's 2009 workplace study, despite the rapidly growing use of social media in the workplace, only 15 percent of executives have considered social media risks at the board level and only 17 percent have a risk mitigation policy and program in place.¹² The best way to maximize the benefits of social media with regard to advertising, marketing, recruiting and employee retention, while minimizing the legal risks, is to implement a comprehensive social media policy.

Importantly, employees should be required to use disclaimers when discussing anything related to their employment, regardless of whether such use is done during work hours.

There is no one policy that will work for every employer, and there is no "fool proof" way to craft away all risk in drafting a policy, because each employer will use social media in a different way, depending on that employer's business model and product/services. However, employers should begin by educating employees regarding social media. They should define social media use and determine what activities are subject to the social media policy. The social media policy should outline when social media use is permitted, if at all. Requiring employees to attend training and receive prior approval before posting on behalf of the company is essential. Where posting or blogging on behalf of or about the company, employees should use their real name and work title. They should be advised to tell the truth and not disparage, and they should not identify customers, partners, vendors or clients without prior consent from both your company and the involved third party. Importantly, employees should be required to use disclaimers when discussing anything related to their employment, regardless of whether such use is done during work hours.

The social media policy should also reference all other relevant policies, including but not limited to the following: anti-discrimination and harassment policy; computer-technology use policy (which should reiterate that employees have no expectation of privacy when engaging in social media use using company computers and information

technology); public relations policy; hours of work policy; conflict of interests policy; code of conduct policy; and any other related or relevant policy. A detailed social media policy will go a long way toward protecting a company from the inherent dangers of social media use, while at the same time allowing the company to take advantage of the opportunities provided. 

Have a comment on this article? Email editorinchief@acc.com.

NOTES

- 1 Kaplan, Andreas M., Haenlein, Michael, *Users of the world, unite! The challenges and opportunities of Social Media*, Business Horizons, Vol. 53, Issue 1, p. 59-68 (2010) (provides a definition for Social Media, Web 2.0 and user generated content, and distinguishing between the three terms/concepts).
- 2 www.socialnomics.com.
- 3 www.leadernetworks.com/documents/networks_for_counsel_2009.pdf.
- 4 Social Networking and Reputational Risk in the Workplace, Deloitte LLP, 2009 Ethics & Workplace Survey Results, www.deloitte.com/assets/dcom-unitedstates/local%20assets/documents/us_2009_ethics_workplace_survey_220509.pdf.
- 5 *Id.*; see also, The Collaborative Internet: Usage Trends, End User Attitudes and IT Impact, FaceTime Communications, Inc., Fifth Annual Survey, March 2010, <http://info.facetime.com/survey10request.html>.
- 6 For ease of reference, this article will use the term "employee," but that term will typically (but not always, such as in the FLSA discussion herein) encompass contractors and agents as well.
- 7 29 C.F.R. § 785.15.
- 8 *Guardsmark, LLC v. NLRB*, 475 F. 3d 369 (D.C. Cir. 2007).
- 9 *USA v. Ziegler*, 474 F. 3d 1184, 1189-90 (9th Cir. 2007) [citing *Mancusi v. DeForte*, 392 US 364 (1968)].
- 10 *Van Alstyne v. Elec. Scriptorium Ltd.*, 560 F.3d 199 (4th Cir. 2009).
- 11 *Pietrylo v. Hillstone Rest. Group*, 2009 U.S. Dist. LEXIS 88702 (D.N.J. Sept. 24, 2009) (unpublished opinion).
- 12 Social Networking and Reputational Risk in the Workplace, Deloitte LLP, 2009 Ethics & Workplace Survey Results, www.deloitte.com/assets/dcom-unitedstates/local%20assets/documents/us_2009_ethics_workplace_survey_220509.pdf.