jackson|lewis
Preventive strategies.
Positive solutions.®

Social Media in the Workplace

October 2013

All We Do Is Work.
Workplace Law. In five time zones
and 55 major locations coast to coast.

www.jacksonlewis.com

jackson lewis
Preventive strategies.
Positive solutions.®

About Jackson Lewis

Founded in 1958, Jackson Lewis is dedicated to representing management exclusively in workplace law. With over 770 attorneys practicing in 55 locations throughout the U.S. and Puerto Rico, Jackson Lewis is included in the AmLaw 100 and Global 100 rankings of law firms. *U.S. News - Best Lawyers* "Best Law Firms" named Jackson Lewis the **2014 "Law Firm of the Year"** in the Litigation-Labor and Employment category. The firm was also named a Tier 1 National "Best Law Firm" in **Employment Law – Management**; **Labor Law – Management**; and **Litigation – Labor & Employment**. The firm's wide range of specialized areas of practice provides the resources to address every aspect of the employer/employee relationship. Jackson Lewis has one of the most active employment litigation practices in the United States, with a current caseload of over 6,500 litigations and approximately 550 class actions.

Jackson Lewis is a founding member of L&E Global Employers' Counsel Worldwide, an alliance of premier employment law boutique firms and practices in Europe, North America, and the Asia Pacific Region.

Additional information about Jackson Lewis can be found at www.jacksonlewis.com.

Privacy, eCommunication and Data Security

Accessing and exchanging business information in cyberspace fosters both unlimited possibilities and new risks and vulnerabilities for companies across the globe. Jackson Lewis' interdisciplinary Privacy, eCommunication and Data Security group stays on the edge of legal developments affecting our clients' business and workplace risks—and opportunities— in the digital age.

Our Privacy, eCommunication and Data Security group regularly advises companies in three primary areas:

- Achieving a balance between an entity's need to learn about, use or disclose personal or confidential information with an individual's or entity's interest in keeping that information private and secure;
- Harnessing the power of social media while avoiding legal pitfalls; and
- Developing strategies, policies and procedures for managing the storage, transmission and security of data, as well as for addressing breaches of data.

Because data is everywhere and part of every situation, we take a holistic approach to advising clients, regularly interacting with other Jackson Lewis attorneys to provide coordinated, common sense advice and preventive strategies that address the range of potential issues relating to privacy, social media and data management. The increasing mobility and technical savvy of the global population heightens the need for this approach.

Privacy. As the capacity for transmitting and storing data grows exponentially, so does the general concern for informational privacy in the United States and around the world. This concern applies to both personal information about individuals and the confidential and proprietary information of organizations. Achieving a balance between the need for information and individual/organizational privacy is critical, particularly for companies that provide services involving the regular handling of sensitive information and/or have a multi-jurisdictional presence. We provide products and services to clients in key areas to assist them with achieving this balance, including:

- Monitoring Activities and Communications
- HIPAA Privacy and Security
- Leave Management
- International/Cross Border Compliance
- Workplace Investigations
- Mergers and Acquisitions

eCommunication. Forward-thinking companies across the globe are embracing social media, networking sites and blogs for, among other things, branding, client development and service, research, recruiting, and to improve employee engagement and facilitate multi-office

workplaces. While the benefits could be significant, social media use is not without challenges for employers. We regularly advise our clients concerning (i) whether and how to monitor and regulate employees' social media use; (ii) the use of information obtained through social media in hiring, promotion, discipline and other decisions; and (iii) the challenges of social media in litigation. Examples include:

- Crafting policies/training to guide employees' acceptable use of social media, as well as internal protocols for management.
- Recognizing the limits on employers in controlling employee communications, such as under the National Labor Relations Act.
- Developing strategies for limiting cyber-smearing and non-disparagement in social media.
- Policies to avoid impermissible endorsement of company products and services.
- Working with our litigation and e-discovery attorneys to advise clients concerning the limits on mining social media for advantages in litigation.

Data Security. A company's most critical assets include information concerning its business and employees. Like other assets, such information needs to be appropriately safeguarded, accessible and preserved. We provide a range of products and services to help clients manage this important asset, including:

- Data Security
- Data Breach Avoidance, Response, Investigations and Litigation
- e-Application and Onboarding
- Training
- Vendor Management and Contracting
- Governmental Contractor Compliance
- Going Paperless

SOCIAL MEDIA IN THE WORKPLACE

Social media continues to be an ever-evolving frontier for companies seeking to attract new business and recruit top talent. At the same time, customers, employees and business partners increasingly utilize social media to research and purchase products and services, connect with fellow employees and network with contacts.[1] In this arena, many employers need to strike an often difficult balance between taking advantage of the power of social media and ensuring that employees do not trigger exposure in the process of branding, client development, employee recruiting and discipline, and other business purposes. Additionally, many employers continue to struggle with a minefield of legal risks flowing from areas such as privacy-related concerns, labor law obligations, and discrimination and harassment protections. This white paper is intended to provide an overview of the various laws and other issues that come into play with respect to social media use in today's workplace.

I. Overview of Social Media

A. What Is It?

Social media has been defined as "a group of Internet-based applications that... allow the creation and exchange of user-generated content."[2] It is the myriad of ways these applications can be used and the variety of outlets that has attracted billions, creating a wide range of challenges as well as opportunities for businesses. Some of the more popular social media outlets include the following:

Facebook is a social networking site that allows users to create profiles, connect with "friends," exchange messages, upload and share photos, "tag" "friends" in those photos, share news and other stories, identify current locations, and join groups. According to Facebook's own statistics, there are currently over 1.15 billion monthly active users—more than 819 million of whom access Facebook through a mobile device.[3]

LinkedIn is "the world's largest professional network on the internet" with over 238 million members and growing at more than two members per second. LinkedIn members create online profiles, which include information about their professional and academic background and experience, "connect" with other members, and "[share] insights and knowledge" with

[1] *See* Joanna Brenner & Aaron Smith, *72% of Online Adults are Social Networking Site Users,* Pew Internet (Aug. 5, 2013), http://pewinternet.org/reports/2013/social-networking-sites.aspx.
[2] Wikipedia, *Social Media*, http://en.wikipedia.org/wiki/Social_media#cite_note-0 (last visited Sept. 16, 2013) (*citing* Andreas M. Kaplan & Michael Haenlein, *Users of the world, unite! The challenges and opportunities of social media*, BUSINESS HORIZONS, Vol. 53, Issue 1, January-February 2010, at 59-68).
[3] Facebook Newsroom, http://newsroom.fb.com/Key-Facts (last visited Sept. 16, 2013).

other professionals."[4] Executives from all 2013 Fortune 500 companies have LinkedIn accounts, and 90 of the Fortune 100 companies use its corporate hiring solutions.[5]

Twitter is a "real-time information network that connects [users] to the latest stories, ideas, opinions and news….At the heart of Twitter are small bursts of information called Tweets. Each Tweet is a maximum of 140 characters long….You can see photos, videos and conversations directly in Tweets to get the whole story at a glance, and all in one place."[6] As of March 2013, Twitter reported over 400,000,000 Tweets per day and 200,000,000+ active users.[7]

YouTube allows individuals to post their own videos and watch videos created and posted by others. According to the statistics on YouTube's website, 100 hours of video are uploaded every minute. More than one billion unique users visit YouTube each month and over six billion hours of video are watched each month on YouTube—that's almost an hour for every person on Earth.[8]

Instagram allows individuals to post pictures and videos and share them on social media sites, including Facebook and Twitter. Launched in October 2010, as of September 2013, Instagram has 150 million active users. 55 million photos are shared daily, and over 16 billion photos have been posted in total.[9]

In addition to these social media sites, many individuals and organizations maintain their own online **blogs**, where the blogger posts entries about a particular subject and typically allows readers to post comments. According to Word Press, a blogging software developer, over 370 million people view more than 11.8 billion blog pages each month.[10]

B. How Is It Used?

Whether for business or personal use, individuals can access social media sites from their own device, another individual's device (whether the individual knows it or not) or a company-issued device, such as a computer, smartphone or tablet. People can use public networks, WiFi and other wireless networks and can interact with the social media community at any time. Thus, employees can engage in social media activity (professional or personal) while at work, on employer-issued devices or network or their own device(s), as well as on their own time using employer-issued or their own devices.[11] Regardless of when or how employees use or participate in social media, they use social media to communicate with their family, friends, co-workers, clients, customers and others, both on and off the job, to talk about their employer

[4] LinkedIn Press Center, http://press.linkedin.com/about (last visited July 25, 2013).
[5] LinkedIn Press Center, http://press.linkedin.com/about (last visited Sept. 16, 2013).
[6] About Twitter, http://twitter.com/about (last visited Sept. 16, 2013).
[7] Celebrating #Twitter7, https://blog.twitter.com/2013/celebrating-twitter7 (March 21, 2013).
[8] YouTube Press Room, http://www.youtube.com/yt/press/statistics.html (last visited Aug. 10, 2013).
[9] Instagram Statistics, http://nitrogr.am/instagram-statistics/ (last visited Sept. 16, 2013).
[10] Word Press, http://en.wordpress.com/stats/ (last visited Sept. 16, 2013).
[11] Of course, some employers can and do limit access to social media through company information systems, even at the risk of upsetting employees who increasingly demand this access.

(both in positive and negative ways), to discuss politics, to express themselves artistically or otherwise, and so on.

At the same time, solely from a business perspective, social media can be a great way to promote the company and help it grow.[12] Additionally, businesses increasingly rely on social media use by their human resources departments for recruiting. Individual employees may have Twitter, LinkedIn and Facebook profiles set up to promote themselves in their role at the company.

The line between professional and private usage is often unclear, particularly as the law struggles to catch up with technology. Likewise, it is not uncommon for there to be a gap between what an employer expects an employee's use to be of one of these accounts for job-related or other purposes and the employee's expectations and privacy interests. The ability of a business to successfully manage social media and harness its benefits will depend in significant part on understanding that these gaps exist and developing preventive strategies to address them.

II. Employment and Labor Law Considerations

A. Using Social Media in the Hiring, Discipline and Termination Process

1. Hiring Process Considerations

Employers are increasingly turning to social media for information about job applicants, yet these sources are replete with information, some of which is not accurate, that should not be considered in the hiring process. Jobvite's 2012 Social Recruiting Survey found, for example, that 92 percent of respondents plan to use social media for recruiting; the same survey found that LinkedIn, which may contain information that should not be considered when searching for or selecting candidates, is the most popular social networking site for recruiters.[13]

Generally speaking, so long as the employer does not violate state or federal discrimination laws, nothing currently prohibits an employment decision based on information an applicant places in the public domain. However, when using social media to vet job candidates, an employer may inadvertently become aware of certain information or characteristics of an applicant (including a current employee seeking a different position in the company) that can expose the employer to risk of a lawsuit if the employer makes a decision adverse to the individual based on that information or characteristic.

[12] According to one study, "more than 90 percent of brands surveyed for the Technorati Media Digital Influence Report stated they have a presence on Facebook. It's nearly as high for Twitter (85%) and YouTube (73%)." *2013 Digital Influence Report,* Technorati Media (2013), http://technoratimedia.com/report/2013-dir/.

[13] Jobvite Reports, http://recruiting.jobvite.com/resources/reports/ (last visited Oct. 4, 2012).

Here are some examples:

- ***Federal and state discrimination laws.*** Various federal and state laws prohibit employers from basing a hiring decision on an applicant's race, age, sexual orientation, marital status, disability and even genetic information, which are all protected under federal law.[14] In the case of genetic information, the law is relatively new and the proscription somewhat counter-intuitive. Under the Genetic Information Nondiscrimination Act ("GINA"), "genetic information" includes, among other things, the manifestation of disease in a "family member," a term that is defined to include an applicant or employee's spouse, despite no genetic connection.[15] The general rule under GINA is that genetic information cannot be collected by an employer or used for an employment purpose, unless an exception applies. Thus, for example, purposefully searching for more information on Facebook about the health of an applicant's spouse (perhaps because of concerns of significant cost to the company's medical plan or increased need for the employee to take leaves of absence) is prohibited under GINA.

  Some states also prohibit discrimination on account of sexual orientation, genetic information, disability status, political affiliation, receiving workers' compensation benefits, and lawful off-duty conduct. State laws prohibiting discrimination on the basis of lawful off-duty activity[16] can be particularly troublesome. Consider, for example, a hiring employer in a state with such a law finds photos on the applicant's website showing the applicant smoking marijuana and decides not to hire that individual. Certainly, the use of the marijuana can be illegal, but it may not be. The individual could be legally using it for medicinal purposes or using it in a state or country where marijuana is permissible. The material the individual is smoking may not even be marijuana or another illegal substance.

- ***Background and Credit History Information*.** Making a hiring decision based on an individual's arrest history, conviction[17] or credit history can be problematic under federal and/or state law. For example, the Federal Fair Credit Reporting

[14] Employers should be aware of the EEOC's current focus on eliminating systemic discrimination, such as discriminatory barriers in recruitment and hiring.
[15] 42 USC §2000 ff.
[16] *See, e.g.,* Colo. Rev. Stat. Ann. § 24-34-402.5(1); N.D. Cent. Code Ann. § 14-02.4-03, -8; and N.Y. Lab. Law § 201-d.
[17] The EEOC recently set new parameters on the use of criminal records in hiring and retention decisions. *See* EEOC Enforcement Guidance, Number 915.002 (April 25, 2012), http://www.EEOC.Gov/laws/guidance/arrest_conviction.cfm. In light of the EEOC's Guidance, before disqualifying an individual with a criminal record from employment, employers should engage in an individualized assessment involving a dialogue with that individual. While the Guidance states that employers would not violate federal anti-discrimination law if they disqualify an applicant based on separate federal restrictions on the employment of persons with criminal records, an employer may not defend a decision to qualify an individual solely on state restrictions on the hiring of persons with criminal records. The Guidance also discourages the use of criminal conduct inquiries on employment applications, recommending that such inquiries be addressed later in the employment consideration process. *See also New Jersey Lawmakers Introduce Their Version of "Ban the Box,"* Jackson Lewis (Feb. 22, 2013), http://www.jacksonlewis.com/resources.php?NewsID=4387.

Act ("FCRA") requires employers to obtain consent before conducting background checks through consumer reporting agencies. This means that employers that engage certain third parties to obtain background information on applicants, such as information concerning reputation, may be required under FCRA to obtain the applicant's written consent. If an employer decides not to hire an applicant based on information in a consumer report obtained from a social networking site through a third party, the employer may be required under the FCRA to notify the applicant that its decision was based on that information. Some state fair credit reporting laws are more stringent than the federal law.

Federal law also prohibits employers from discriminating against an applicant based on the employee's current or prior filing for bankruptcy. At the state level, likely in response to economic conditions, new laws in certain jurisdictions prohibit employers from discriminating against employees and applicants on the basis of credit-related information, such as payment history.[18]

- ***Inaccurate information***. The cliche - *Don't believe everything you read!* - applies not only to information you find in the newspaper. Information obtained online frequently is inaccurate, misleading or not provided in the proper context. Basing a decision on incorrect information not only poses the risk of a lawsuit from the applicant, but even if the applicant does not sue, the company can potentially lose its next star employee. The same can be true for an employee seeking a different position inside the company. In that case, the problems that tainted the hiring process would be likely to also adversely impact the individual's current employment.

- ***Impermissibly obtaining access to the information.*** Employers must also be cautious in how they go about accessing information available about a job applicant through social media. A number of states (Maryland, Illinois, California, Arkansas, Colorado, New Mexico, Oregon, Utah, Vermont, Washington, Michigan, Nevada, New Jersey)[19] have made it illegal to request and/or require employees or applicants to provide the username and passwords necessary to access their Facebook and other social media and online accounts, or created a commission to look at the issue. These laws vary

[18] *See Use of Credit Information In Employment*, National Conference of State Legislatures (last visited Sept. 9, 2013), http://www.ncsl.org/issues-research/banking/use-of-credit-info-in-employ-2013-legis.aspx (e.g., California, Illinois, Maryland, and Washington). *See also Colorado Becomes Latest State to Restrict Use of Credit Checks for Employment Purposes*, Jackson Lewis(Apr. 26, 2013), http://www.jacksonlewis.com/resources.php?NewsID=4460.

[19] Md. Labor & Employment Code Sec. 3-712; 820 Ill. Comp. Stat. 55/10 (2013); Cal. Lab. Code §980 (2013); (permits employers to request an employee to divulge personal social media activity reasonably believed to be relevant to an investigation of allegations of employee misconduct or employee violation of applicable laws and regulations; exception applies so long as the social media is used solely for purposes of that investigation or a related proceeding); AR H.B. 1901 (effective Aug. 16, 2013); Colo. Rev. Stat. §8-2-127 (2013); N.M. S.B. 371 (effective June 14, 2013); OR H.B. 2654 (effective Jan. 1, 2014); Utah Code Ann. §34-48-101 (2013); VT S. 7 (effective May 24, 2013) (creates a commission to study whether there should be a prohibition on employers); Wash. S.B. 5211 (effective July 28, 2013); Mich. Comp. Laws Serv. §37.271 (2013); Nev. A.B. 181 (effective Oct. 1, 2013); N.J. Rev. Stat. § 34:6B-5 (effective Dec. 1, 2013).

> in some respects, but generally limit an employer's ability to get past the employee's or applicant's privacy settings. By way of example, Colorado's law does not prohibit certain employers (those in certain industries (e.g., securities, finance) who have to comply with certain regulatory requirements) from conducting investigations concerning the use of personal websites, web-based accounts or similar accounts by an employee for business purposes. It also is imperative that employers avoid circumventing a potential employee's privacy settings by pretending to be someone else in order to gain access to a restricted network. [20]

A decision not to hire an individual based on some of the activities described above could result in the individual suing the employer, alleging that the decision was discriminatory or otherwise unlawful. This risk among other considerations has caused many employers to stop requiring applicants to submit certain information with their resume or application, as well as to cease searching social networking sites that may reveal sensitive information. Companies that take this approach need to be sure that directive has reached all of the managers and supervisors that are involved in the hiring process as many turn to social media as a matter of course in vetting candidates.

Acquiring the information also poses risks even if the company hires the individual. If the new employee is aware that the company has certain information, such as health-related information (e.g. cancer diagnosis) concerning the employee's spouse, and is later subject to an adverse employment decision, the employee may attribute that decision to the information the employer obtained in the hiring process, and not the poor performance the employer claims is the basis of the adverse action.

One potential solution for employers is to separate recruiters who screen applicants using social media and other resources from individuals who are making the hiring decision. This would require a recruiter to search applicants online, scrub prohibited or sensitive information, and deliver scrubbed profiles to a decision-maker. Of course, the process relies heavily upon a recruiter's knowledge of employment laws to scrub prohibited information. Companies also can utilize outside third parties to screen applicants through social media as long as they are aware of the pitfalls. For instance, a company would still be prohibited from causing an agent of the company to discriminate against an individual.[21] At the end of the day, employers must realize that ignoring this very real issue or simply outsourcing recruitment to a third party without careful consideration of the legal issues and the recruiter's qualifications is an untenable solution. Even this "solution" raises issues of whether the third party constitutes a consumer reporting agency, triggering FCRA notice and other requirements.

[20] *See, e.g., Brian Pietrylo v. Hillstone Rest. Group*, 2009 U.S. Dist. LEXIS 88702 (D.N.J. Sept. 25, 2009) (court refused to overturn jury verdict finding managers accessed a private, invitation-only chat group without authorization in violation of the federal SCA).
[21] *See* 29 CFR §1635.6.

2. 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 other social media sites having nothing to do with his or her job responsibilities. Other situations may include employees who criticize a supervisor or client, post distasteful photos or videos, or call in sick and then tweet about their being out and about. In the health care industry, employee social media activity can be particularly troubling, such as where employees may decide to post about patients' injuries (with photos) on Facebook.[22]

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, as well as practical considerations. Some of the legal constraints and practical considerations employers must consider include:

> ***Does the employer have a legal right to be viewing the employee's activity?*** Technologies exist that permit the tracking of keystrokes on a keyboard, enabling an employer/manager to discern an employee's username and password to online accounts. Less technologically savvy employers/managers might simply approach, pressure or otherwise obtain from an employee's co-worker(s) (who also are friends of connections of the target employee) access to the target employee's activity in the social media venue. In the first scenario, the employer runs the risk of violating the Stored Communications Act ("SCA"), which generally prohibits accessing the online account of another without that individual's consent.[23] The second scenario can also raise SCA issues, as well as potential violations of common law privacy torts (e.g., intrusion upon one's seclusion). And, of course, as noted above, simply asking employees for the passwords to access their social media or online account generally is impermissible in a number of states.[24] Additional concerns arise if the employer permits employees to utilize their own personal devices for work activity. Typically called "bring your own device" ("BYOD") programs, an employer's ability or "right" to access information on the mobile device may be diminished when the device is owned by the employee.
>
> ***Could the employee be protected under a whistleblower statute?*** Federal and state whistleblower laws may protect employees who complain about certain company activities or conditions affecting public health and safety or violating public policy standards, as well as employees who report potential securities fraud violations.

---

[22] *See, e.g.,* Molly Hennessy-Fiske, *When Facebook goes to the hospital, patients may suffer*, LA Times (Aug. 8, 2010), http://articles.latimes.com/2010/aug/08/local/la-me-facebook-20100809; *HIPAA Case Study: Temporary Employee Post Patient Records on Facebook, Hospital Faces Stiff Penalties*, Dexcomm (June 19, 2012), http://www.dexcomm.com/hipaa-case-study-temporary-employee-post-patient-records-facebook-hospital-faces-stiff-penalties/.

[23] *See, e.g., Rene v. G.F. Fishers, Inc.*, 817 F. Supp. 2d 1090 (S.D. Ind. 2011).

[24] *See supra* note 19.

For example, the Sarbanes-Oxley Act of 2002 ("SOX") prohibits employers from terminating employees for "provid[ing] information, caus[ing] information to be provided, or otherwise assist[ing] in an investigation regarding any conduct which the employee reasonably believes constitutes a violation of … any rule or regulation of the Securities and Exchange Commission, or any provision of Federal law relating to fraud against shareholders."[25] 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.

Note, however, that the privacy regulations under the Health Insurance Portability and Accountability Act also contain a whistleblower protection provision.[26] However, that provision protects the whistleblower only if he or she reports the violations to his or her attorney or the appropriate public health agency, not on social media.

Was the communication related to political activities or affiliations? Many states prohibit employers from regulating employee political activities and affiliations or influencing employees' political activities.[27] Taking action against an employee for objectionable political speech could violate these restrictions.

Was the employee engaging in illegal activity or "lawful off-duty activity" protected by state law? As discussed above, some states protect employees from adverse employment action on the basis of their engaging in lawful activities when not at work. Thus, in some states, an employer may be prohibited from terminating an employee who, for example, posts pictures of himself intoxicated at a party (assuming the employee is over 21 years old). In contrast, the employer may have more leeway where the conduct is illegal. However, even where conduct appears to be illegal, the employer may still need to take additional steps to investigate and consult with counsel before taking any action. For example, in California, employers are prohibited from excluding someone from employment based solely on an arrest, marijuana convictions more than two years old, or convictions that have been expunged or dismissed.[28] Additionally, "liking" something on Facebook can constitute speech covered by the First Amendment for public sector employees.[29] The law is far from clear in this area, and employers should consider each situation independently.

---

[25] 18 USCS § 1514A.
[26] *See* 45 CFR 164.502(j).
[27] *See, e.g.*, Cal. Lab. Code § 1102; Col. Rev. Stat. Ann. § 8-2-108; La. Rev. Stat. Ann § 23:961; Minn. Stat. Ann. § 10A.36; Mo. Ann. Stat. § 115.637(b); Neb. Rev. Stat. Ann. § 32-1537; Nev. Rev. Stat. Ann. § 613-040; S.C. Code Ann. §16-17-560; W.Va. Code Ann. § 3-8-11; Seattle, Wash. Mun. Code § 14.04.040.
[28] Cal. Lab. Code §§432.7 & 432.8.
[29] The U.S. Court of Appeals for the Fourth Circuit recently held that an employee's clicking of the Facebook "like" button was sufficient to merit constitutional protection under the First Amendment. *Bobby Bland v. B.J. Roberts*, No. 12-1671 (4th Cir. Sept. 18, 2013).

Does the employee have a potential discrimination claim? As noted above, employers are prohibited from unlawfully discriminating against employees as well as applicants on account of protected characteristics, including race, age, sexual orientation, marital status, disability and genetic information. An employee's manager may learn from an employee's Facebook status, for example, that the employee is pregnant. In this case, the employer cannot fire the employee on account of the pregnancy or otherwise take adverse action against the employee.

Wrongful termination claims. An employer may also face wrongful termination claims for an allegedly improper termination decision in connection with social media use. For example, employers (including non-union employers) need to be mindful of the recent interpretations of the National Labor Relations Act concerning protected concerted activity rights related to social media policies and employee disciplined pertaining to social media activity, which are discussed in detail below.

Does the employer make things worse by trying to make things better? Consider discovering social media activity that addresses your workplace, refers to high level persons in your company and makes troubling allegations, but you cannot determine who is responsible for the posts or immediately confirm whether the allegations are true. Should you start questioning employees potentially responsible or named in the posts, or conducting forensic investigations? Maybe. The decision will, of course, turn on the facts and circumstances, but one course of action that ought to be considered is doing nothing. Frequently, the person responsible for the social media activity is simply seeking attention, and if the person does not get it, he or she may just move on to another topic.

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

3. Labor Relations Considerations

The National Labor Relations Act ("NLRA") affords employees (even those who are not unionized) the right to engage in "concerted activity," including the right to discuss the terms and conditions of their employment—and even to criticize their employers—with co-workers and outsiders.[30] Not all concerted activities are protected by the NLRA; only those activities that are engaged in for the purpose of collective bargaining or other mutual aid or protection are covered.[31]

[30] *See* 29 U.S.C. §157.

[31] *See, e.g., Federal Security, Inc., and its alter egos or agents, James R. Skrzypek and Janice M. Skrzypek and Joseph Palm*, 359 NLRB No. 1 (Sept. 28, 2012).

a. *What is Concerted Activity?*

In general, concerted activity is activity "engaged in with or on the authority of other employees, and not solely by and on behalf of the employee himself." Concerted activity also includes "circumstances where individual employees seek to initiate or to induce or to prepare for group action" and where individual employees bring "truly group complaints" to management's attention. However, the Labor Board has held that individual employee gripes are not concerted activity.[32]

b. *When is Concerted Activity Protected?*

An employee's concerted activity will be protected under Section 7 of the NLRA where, for example, the employee's statements implicate the employee's working conditions, regardless of how those statements are communicated. Another example of protected activity under Section 7 occurs when the employee protests supervisory actions. However, these protections can be lost where the employee's outbursts about a supervisor are too "opprobrious" to maintain protection under Section 7. The use of curse words or expletives alone is unlikely to reach this level. Protection also could be lost where the communication is disloyal or has the tendency to damage an employer's business *and are made with reckless disregard of the truth or are maliciously untrue*. What exactly constitutes protected concerted activity requires further examination and analysis of the facts at issue on a case-by-case basis.

Recent decisions from the National Labor Relations Board ("NLRB"), the government agency charged with interpreting the NLRA, shed some light on what constitutes protected concerted activity in the social media context. In one decision, for example, the NLRB held that the employer acted unlawfully when it discharged two employees who made comments on Facebook about terms and conditions of employment, including the conduct of their supervisor, because such protests constituted protected concerted activity.[33] In another case, on the other hand, the NLRB ruled that an employee who communicates an "individual gripe rather than any shared concerns about working conditions" has not engaged in protected concerted activity.[34]

In addition to these cases, the NLRB Acting General Counsel Lafe Solomon issued a report in August 2011 summarizing his reasoning in pending cases involving social media.[35] As set forth

[32] *See JT's Porch Saloon & Eatery LTD*., NLRB Div. of Advice, No. 13-Ca-46689 (July 7, 2011); *Martin House*, NLRB Div. of Advice, No. 34-Ca-12950 (July 19, 2011).

[33] *Bettie Page Clothing*, 359 NLRB No. 96 (Apr. 19, 2013). *See also Three D LLC d/b/a Triple Play Sports*, NLRB ALJ, No. 34-CA-12915 (Jan. 3, 2012) (holding that an employee, whose involvement in an online employee discussion of payroll tax withholding was merely clicking the "Like" button on Facebook, was engaged in concerted activity because clicking the "Like" button expressed approval of employee complaints regarding the payroll tax mismanagement and made "a meaningful contribution to the discussion"); *Hispanics United of Buffalo Inc*., 359 NLRB No. 37 (Dec. 14, 2012) (affirmed an administrative law judge's finding that an employer violated the NLRA by firing five employees for posting Facebook comments in response to a co-worker's criticism of their job performance).

[34] *Tasker Healthcare Group, d/b/a Skinsmart Dermatology*, NLRB Div. of Advice, No. 04-CA-094222 (May 8, 2013).

[35] *Acting General Counsel releases report on social media cases,* National Labor Relations Board, (Aug. 18, 2011), http://www.nlrb.gov/news-outreach/news-releases/acting-general-counsel-releases-report-social-media-cases.

in that report, the following conduct constituted protected concerted activity even though it took place online:

- Conversations among co-workers regarding job performance and staffing levels that implicated working conditions;
- Discussing supervisory actions with co-workers;
- Posting photos and comments reflective of co-workers' concerns regarding terms and conditions of employment; and
- Shared concerns about terms and conditions of employment.

The Acting General Counsel subsequently issued two additional opinion memoranda regarding social media. In his latest report, the Acting General Counsel found certain policy language regarding employee social media use to be problematic, including the following[36]:

- Prohibiting posts discussing the employer's non-public information, confidential information, and legal matters (without further clarification of the meaning of these terms);
- Prohibiting employees from harming the image and integrity of the company, making statements that are detrimental, disparaging or defamatory to the employer, and prohibiting employees from discussing workplace dissatisfaction;
- Prohibiting posts that are inaccurate or misleading or that contain offensive, demeaning or inappropriate remarks, and instructing employees to use a friendly tone and not engage in inflammatory discussions;
- Requiring employees to secure permission prior to posting photos, music, videos, quotes and personal information of others;
- Prohibiting the non-commercial use of the employer's logos or trademarks;
- Discouraging employees from "friending" co-workers;
- Prohibiting online discussion with government agencies concerning the company;
- *Encouraging* employees to solve work problems in the workplace rather than posting about such problems online; and
- Threatening employees with discipline or criminal prosecution for failing to report violations of an unlawful social media policy.

On the other hand, the Acting General Counsel found a social media policy that prevented "inappropriate postings that may include discriminatory remarks, harassment and threats of violence or similar inappropriate or unlawful conduct" to be lawful "since it prohibit[ed] plainly egregious conduct, such as discrimination and threats of violence." Additionally, the Acting General Counsel determined that an employer's social media policy preventing the dissemination of trade secrets and confidential information was lawful where the policy provided numerous examples of what specifically should not be disseminated, such as system development information, processes and internal reports. By providing these examples, the

[36] *Acting General Counsel releases report on employer social media policies*, National Labor Relations Board (May 30, 2012), http://www.nlrb.gov/news-outreach/news-releases/acting-general-counsel-releases-report-employer-social-media-policies.

Acting General Counsel found that employees would "understand that it does not reach protected communications about working conditions." Employment decisions based on these types of social media activities, then, are likely to be deemed lawful.

B. Employer Liability for Employees' Misuse

Employees may intentionally or inadvertently use social media—whether on-the-job or at home—in a way that poses risks for their employers. When employees use social media to harass co-workers, reveal confidential information, endorse products or services without proper disclosure, or engage in criminal conduct, for example, employers face risks. Some of the legal risks employers face when employees misuse social media include:

***Hostile Work Environment and Discrimination Claims*.** Social networking sites and blogs provide employees with additional avenues for engaging in inappropriate conduct. Employees may vent workplace frustrations by posting discriminatory statements, racial slurs or sexual innuendos directed at co-workers, management, customers or vendors. If a supervisor has posted discriminatory statements regarding an employee's protected status on his or her Facebook page, for example, and the employee is later terminated or subjected to an adverse employment action, the supervisor's discriminatory statements could be used as evidence that the employment action was motivated by discriminatory animus in a subsequent lawsuit or administrative claim.[37]

Genetic Information Nondiscrimination Act (GINA). Title II of this law, which specifically applies to private employers, employment agencies, unions and certain government employers, and the EEOC implementing regulations[38] prohibit, among other things, the acquisition of genetic information (such as an employee's family medical history) except in limited circumstances. For example, a manager who is "friended" by one of her employees in social media would not violate GINA if she inadvertently learns the employee's mother has breast cancer (which would be genetic information with respect to the employee) because of information posted on the employee's page for all "friends" to see. This is the case because the manager had permission to access the employee's profile from the employee. Otherwise, the manager would have to show access is routinely granted to all who request it. However, intent is key: if it can be shown that the manager had been searching for medical information about the employee's family member(s) because of recent high-dollar claims under the company's health plan, that would likely violate GINA (and also raise HIPAA privacy issues). Similarly, if after inadvertently accessing genetic information online, which generally is

[37] *See, e.g.,* Lisa Rein, *Gay man sues Library of Congress, alleging discrimination*, Washington Post (Apr. 22, 2012), http://articles.washingtonpost.com/2012-08-22/politics/35493126_1_federal-lawsuit-gay-man-facebook-page. *See also Stewart v. CUS Nashville, LLC*, 2013 U.S. Dist. LEXIS 16035 (M.D. Tenn. Feb. 6, 2013) (federal district court allows claims alleging employer liability for retaliation based on its owners', directors', managers' and supervisors' personal social media statements (including Facebook); *Espinoza v. County of Orange*, 2012 Cal. App. Unpub. LEXIS 1022 (Ct. App. 4th Dist. 2012) (unpublished).

[38] Equal Employment Opportunity Commission, *Regulations Under the Genetic Information Nondiscrimination Act of 2008*, *available at* https://www.federalregister.gov/articles/2010/11/09/2010-28011/regulations-under-the-genetic-information-nondiscrimination-act-of-2008.

permissible under GINA, the manager decided to dig further concerning the employee's mother's health condition, that too would violate GINA.

***Defamation Claims*.** Employers may face liability for defamation based on electronic communications disseminated by employees. Employee bloggers, for example, can create unrest in the workplace by posting rumors, gossip and offensive false statements about co-workers and supervisors, as well as third parties. Negative comments made by management about a departing employee may also create liability. Consider the following example: An employee leaves Company A to take advantage of more promising opportunities with Company B. Prior to starting with Company B, her supervisor at Company A posts false and damaging comments regarding her abilities and work habits on a blog. An employee at Company B stumbles upon these comments, and Company B withdraws its employment offer based on the false information. As a result of the comments posted in the blog, the former employee may have a cause of action against Company A and the supervisor for defamation or interference with prospective economic relations.[39]

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 customer/client/patient information with the simple click of a button. For example, consider a corporate attorney working on a merger and acquisition who updates her Facebook status to read: "So glad the deal is done. I need some sleep!" Someone who knows that the attorney handles mergers and acquisitions and represents a particular client may piece together that something important is about to happen. If that person decides to buy a significant amount of stock in one of the companies, the attorney and his or her law firm may have to answer for that post. Employees may also act more deliberately, such as a disgruntled employee revealing a company's trade secrets and other proprietary information on a blog.[40]

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

[39] *See, e.g., River v. National R.R. Passenger Corp.*, 331 F.3d 1074 (9th Cir 2003) (employer may be held liable for the defamatory statements of employees under the doctrine of respondeat superior if the defamation occurred within the scope of employee's employment).

[40] *See, e.g., Coface Collections N. Am. v. Newton*, 430 Fed. Appx. 162 (3d Cir. 2011) (granting preliminary injunction and finding that employer was likely to succeed on the merits where employee breached non-solicitation and non-competition clause through the use of LinkedIn and Facebook to solicit business and potential employees); *Art of Living Found. v. Doe*, 2012 U.S. Dist. LEXIS 61582 (N.D. Cal. May 1, 2012) (denying defendant's motion to strike plaintiff's trade secret claim where defendant posted putative trade secrets belonging to plaintiff on his blog); *Dynamic Sports Nutrition, Inc. v. Roberts*, 2009 US. Dist. LEXIS 3322 (S.D. Tex. Jan. 16, 2009) (granting permanent injunction on plaintiff's claim for misappropriation of confidential information and trade secrets where defendant, a former employee of plaintiff, posted such information on his personal blog and other websites).

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.

III. Social Media and Business Risks

There are a number of business-related risks and considerations related to social media use. Some of these issues, such as compliance in highly-regulated industries, are unique to specific sectors of the economy, while others, such as intellectual property questions, are more general. Though by no means exhaustive, this section highlights some of the issues that businesses must consider and address with respect to social media use.

A. Intellectual Property and Account Ownership

Disputes between employers and departing employees over the ownership of social media accounts are on the docket of a number of federal district courts throughout the nation. Employers in these cases are asserting ownership over company Twitter and LinkedIn profiles claiming, among other things, that they contain "trade secrets." [41] 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. Such cases can entail prolonged discovery and extensive litigation that may be avoidable if the parties enter into clearly written agreements at or near the inception of the employment relationship.[42]

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. Virtually all states with trade secret protections require entities endeavoring to protect their secrets to put safeguards in place to preserve the confidentiality of these trade secrets. For example, most states have adopted versions of

[41] *See, e.g., PhoneDog v. Kravitz*, 2011 U.S. Dist. LEXIS 129229 (MEJ) (N.D. Cal. Nov. 8, 2011) (district court denied a motion to dismiss employer's claims, including misappropriation of trade secrets, conversion, and tortious interference with prospective advantage, asserted against former employee who changed the Twitter account handle and continued to use the account given to him for the employer's business during his employment; the parties did not have a written agreement as to ownership of the account). *See also Eagle v. Morgan*, 2011 U.S. Dist. LEXIS 147247 (RB) (E.D. Pa. Dec. 22, 2011) (district court denied employer's motion to dismiss suit brought by former company president to regain control of his LinkedIn account; parties did not have a written agreement as to ownership of the account).

[42] Such an agreement was upheld in *Ardis Health, LLC v. Nankivell*, 2011 U.S. Dist. LEXIS 120738 (S.D.N.Y. Oct. 19, 2011) (district court granted preliminary injunction requiring employee to give her employer access to social media sites pursuant to obligations under the parties' written Non-Disclosure and Rights to Work Product Agreement).

the Uniform Trade Secrets Act, which provides for specific confidential designation of materials deemed trade secrets or confidential information. Following such standards and establishing protocols and agreements for the use of social media should be one of a number of safeguards a company adopts to help better its position to defend ownership of social media accounts as trade secrets.

In addition to protecting trade secrets, maintaining ownership and editorial control of social media accounts protects the goodwill of the enterprise. If a single employee has the password to a Twitter account associated with a business and tweets an offensive or inappropriate remark, the company will have difficulty correcting or responding to negative publicity. And, in many cases, the account may have built up a valuable list of "followers" or "friends" that the company wants to keep for marketing purposes. If the employee departs and takes the account and the followers with him or her the business has to start all over.

B. Consumer Protection

The Federal Trade Commission's ("FTC" or the "Commission") revised *Guides Concerning the Use of Endorsements and Testimonials in Advertising* (the "Guides")[43] are important for businesses whose employees are likely to be commenting online about the company's products and services. The revised Guides took effect December 1, 2009 and address the application of Section 5 of the FTC Act[44] to the use of endorsements and testimonials in advertising.

The Guides provide the following example of an employee's blog posting concerning his employer's product, where the employment relationship is not previously disclosed, that could potentially result in employer liability:

> 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 numerous 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 to the manufacturer to members and readers of the message board.

[43] 16 CFR Part 255.
[44] 15 U.S.C §45.

In comments to the proposed revisions, the Commission agreed that the establishment of appropriate procedures governing "new media" would be a factor in its determination as to whether law enforcement action is appropriate. Tellingly, the Commission stated that it has brought enforcement actions against companies "whose failure to establish or maintain appropriate internal procedures" had resulted in consumer injury. However, the Commission refused to spell out the procedures companies should put in place to monitor compliance with the principles set forth in the Guides, leaving companies to determine for themselves the process that would best fulfill their responsibilities.

C. Some Specific Concerns in Highly-Regulated Industries

As each and every industry is uniquely impacted by social media, attempting to address social media use in a one-size-fits-all manner without taking appropriate considerations into account is not only impractical, but in some cases unlawful. The following discussion highlights some particular concerns for certain highly-regulated industries.

1. Health Care Industry and the Health Insurance Portability and Accountability Act

The use of social media in the health care setting presents a range of challenges under the Health Insurance Portability and Accountability Act ("HIPAA") and patient privacy generally. The basic rule under HIPAA is that "protected health information" ("PHI") may not be used or disclosed except as permitted under the HIPAA privacy rule.[45] These rules also impose substantial limitations on the use of patient data for marketing purposes and fundraising, which have been significantly tightened under provisions of the Health Information Technology for Economic and Clinical Health ("HITECH") Act.[46]

The risks could be substantial for a health care entity. Disclosures of the PHI of patients in social media can easily trigger breach notification requirements. Employees may think they have "de-identified" the information, but may be unaware of the highly technical de-identification requirements.[47] In addition, final HITECH regulations issued in January 2013, make the requirement of reporting a breach more likely by removing the "risk of harm" standard in exchange for a more objective standard for determining whether a "breach" has occurred.[48] Under the new rule, impermissible uses and disclosures of PHI are presumed to be breaches, unless an exception applies or the covered entity can rebut that presumption through a multi-factored risk assessment.[49] Breach notifications can, in turn, trigger complaints which can increase the likelihood of a compliance review by the Office for Civil Rights.

---

[45] 45 CFR §164.502.
[46] 45 CFR §§ 164.508 and 514.
[47] *See* U.S. Department of Health and Human Services, *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, available at* http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/guidance.html#preparation. De-identification can be accomplished by two methods: expert determination or safe harbor. *See* 45 CFR §164.514(b)(1) and §164.514(b)(2).
[48] The inquiry into whether there is a significant risk of harm to privacy and security is no longer appropriate.
[49] 45 CFR §164.402.

Additionally, patients may have the ability to sue under state law for the inappropriate safeguarding and wrongful disclosure of their medical information.[50] In the process, and perhaps most damaging, is the reputational harm a health care institution may suffer in its community.

Health care employers should note that the Federation of State Medical Boards ("FSMB") recently adopted model policy guidelines for the appropriate use of social media and social networking in a medical practice.[51] In its findings, the FSMB reports that 67 percent of 4,000 physicians surveyed use social media for professional purposes and that research indicates 35 percent of practicing physicians have received friend requests from a patient or member of their family, and 16 percent of practicing physicians have visited an online profile of a patient or patient's family member.[52] This growing online connection between doctors and patients requires doctors and their employers to enact policies to ensure compliance with professional, legal and ethical standards. The guidelines also point to model social media policies that have been published by the American Medical Association, the Cleveland Clinic[53] and the Mayo Clinic.[54]

2. Pharmaceutical Industry and the Food and Drug Agency

With heavy regulation by the Food and Drug Administration ("FDA"), the pharmaceutical industry faces a specific set of concerns when it comes to social media use. Draft Guidance on the use of social media by pharmaceutical companies issued in January 2012 specifically addressed how pharmaceutical companies should respond to unsolicited requests for off-label information about prescription drugs and medical devices.[55] While the guidance addressed the FDA's concerns regarding requests for off-label information received via social

[50] *See, e.g., Runyon v. Smith*,163 N.J. 439 (2000) (doctor's testimony violated the psychologist-patient privilege); *Randi A.J. v. Long Island Surgi-Center*; 46 A.D.3d 74 (2007) (damages awarded in connection with improper disclosure of patient treatment); *but see Acara v. Banks*, 470 F.3d 569 (5th Cir. 2006) (HIPAA does not provide individuals with a private right of action to sue covered entities for violations of HIPAA).

[51] Federation of State Medical Boards, *Model Policy Guidelines for the Appropriate Use of Social Media and Social Networking in Medical Practice, available at* http://www.fsmb.org/pdf/pub-social-media-guidelines.pdf.

[52] For examples of incidents involving hospital employees sharing information pertaining to a patient through social media, *see, e.g.,* Alice Park, *Are Med-Student Tweets Breaching Patient Privacy?*, Time (Sept. 23, 2009), http://content.time.com/time/health/article/0,8599,1925430,00.html; Jennifer Fink, *Five nurses fired for Facebook postings*, Scrubs (June 14, 2010), http://scrubsmag.com/five-nurses-fired-for-facebook-postings/; Julie Straw, *Woman out of a job after sending tweet to Governor Barbour*, MS News, http://www.msnewsnow.com/global/ story.asp?s=11713360.

[53] Cleveland Clinic, *Social Media Policy*, http://my.clevelandclinic.org/about-cleveland-clinic/about-this-website/social-media-policy.aspx (last visited Sept. 19, 2013).

[54] Mayo Clinic, *Sharing Mayo Clinic,* http://sharing.mayoclinic.org/guidelines/for-mayo-clinic-employees/ (last visited Sept. 19, 2013). The ECRI Institute also recently published an excellent summary of key issues for hospitals concerning social media (registration required), a valuable read for any hospital administrator, risk manager or human resources director. ECRI Institute, *Social Media in Healthcare,* https://www.ecri.org/EmailResources/HRC/ eSource/AdSup4.pdf.

[55] *Responding to Unsolicited Requests for Off-Label Information About Prescription Drugs and Medical Devices*, FDA Draft Guidance (Dec. 2011), *available at* http://www.fda.gov/downloads/drugs/guidancecompliance regulatoryinformation/guidances/ucm285145.pdf. Additionally, in December 2012, the FDA issued a Warning Letter to AMARC Enterprises, Inc. in part due to the company having "liked" a favorable consumer Facebook posting. *Warning Letter to AMARC Enterprises, Inc.*, FDA WL No. 11-13 (Dec. 11, 2012), *available at* http://www.fda.gov/ICECI/EnforcementActions/WarningLetters/2012/ucm340266.htm.

media, the guidance touched on requests made through traditional forms of communication as well. For example, the Administration recommends responding privately to public requests for off-label use made on a social media website. The Draft Guidance also discusses solicited requests for off-label use, which may constitute illegal promotion of a product if responded to. Although FDA guidance regarding the use of social media is currently incomplete and requires clarification, companies are encouraged to conform their online presence to existing FDA guidelines.

3. Financial Services Industry

Regulation of the financial services industry by both the Financial Industry Regulatory Authority ("FINRA") and the Securities and Exchange Commission ("SEC") likewise presents unique issues regarding the use of social media. In August 2011, FINRA issued Regulatory Notice 11-39 to provide guidance on how advisors should use social media sites to communicate with their clients.[56] This Notice clarified the guidance previously issued by FINRA in January 2010 through Regulatory Notice 10-06.[57] Notice 11-39 addresses concerns regarding recordkeeping responsibilities, supervision of persons associated with a financial entity, links to third-party websites, and management of data feeds into a firm's websites. For example, whether a firm is required to retain a social media communication made by an associated person depends on whether the content of the communications constitutes a business communication. Similarly, firms are required to adequately train and supervise associated persons intending to use social media websites for business purposes.

The SEC's recent guidance allows corporations to use social media websites to make business announcements without violating the Regulation Fair Disclosure rule. However, such disclosures should not be made on the personal website of a corporate officer. The SEC explained that "[p]ersonal social media sites of individuals employed by a public company would not ordinarily be assumed to be channels through which the company would disclose material corporate information." Accordingly, the Commission seeks to ensure that social media communications regarding material, nonpublic information do not unfairly influence investor behavior, while also recognizing that the widespread use of social media by corporations has transformed how business communications are made.[58]

4. Federal Contractors

Federal contractors are generally subject to the same data privacy and security standards as the government agencies with which they contract, including the Privacy Act of 1974 and the Federal Information Security Management Act of 2002. Government

[56] *Social Media Websites: Guidance on Blogs and Social Networking Web Sites*, FINRA Regulatory Notice 11-39 (Aug. 2011), *available at* http://www.finra.org/Industry/Regulation/Notices/2011/P124186.

[57] *Social Media Websites and the Use of Personal Devices for Business Communications: Guidance on Social Networking Websites and Business Communications*, FINRA Regulatory Notice 10-06 (Jan. 2010), *available at* http://www.finra.org/Industry/Regulation/Notices/2011/P120779.

[58] *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: Netflix, Inc. and Reed Hastings*, Release No. 69279 (Apr. 2, 2013), *available at* http://www.sec.gov/litigation/investreport/34-69279.pdf.

contractors, therefore, need to be aware of the data privacy and security mandates that can become applicable when they engage in social media-related activities.

5. Legal Services

One industry that has been particularly affected by social media use is legal services. While this could easily be the subject of its own white paper, the discussion below highlights some key considerations.

a. *Attorney Ethics*

The rules of professional conduct for attorneys, which differ depending upon state, apply with equal force in the realm of social media. These rules apply to most aspects of an attorney's practice, such as attorney advertising and investigating client matters. In the case of advertising, for example, there are rules pertaining to listing of "specialties" on LinkedIn if the attorney is not certified as a specialist, "testimonials" posted by clients through LinkedIn's recommendation feature, and other requirements for any attorney advertising, such as listing an office address, including appropriate disclaimers, and submitting advertisements for review.[59] Additionally, recent ethics rulings have addressed the directions or instructions attorneys may give clients with regard to their social media accounts. For example, in New York, attorneys are permitted to advise clients that certain social media content may be used against the client for impeachment or similar purposes, but the attorney may not suppress, conceal or knowingly fail to disclose evidence which the attorney is required by law to reveal.[60] Attorneys also should avoid asking other persons to reach out to a witness in social media in order to gain access to that witness' personal profile, as well as engaging in ex parte communications themselves.[61]

With respect to the rules governing attorney-client confidentiality, attorneys must be careful to avoid disclosing a client's legal issues through social media, and need to carefully consider whether information exchanged between an attorney and his or her client on a social networking site is considered confidential.[62] Attorneys should also remind clients that they risk waiving the attorney-client privilege by sharing information about their case on a social media site.

---

[59] *See, e.g.*, *Cal. State Bar Formal Opn. 2004-166* (Dec. 21, 2012) (Attorney cannot disseminate "communications" with testimonials or endorsements of the attorney unless the communication also contains an express disclaimer. Tweeting "Another great victory in court today" may be permissible by itself, but adding "Who wants to be next?" creates an ethical problem in California.); *NYSBA Ethics Op. 972* (June 26, 2013) (law firm may not list its services under heading of "Specialties" on a social media site, and lawyer may not do so unless certified as a specialist by an appropriate organization or governmental authority). *See also* Susan Cartier Liebel, *12 Social Media Ethics Issues for Lawyers* (March 11, 2010), http://solopracticeuniversity.com/2010/03/11/a-dozen-social-media-ethics-issues-for-lawyers/.

[60] *NYCLA Ethics opinion 745*, July 2, 2013.

[61] *See, e.g.*, *Philadelphia Bar Ass'n Professional Guidance Comm. Opn. 2009-02* (March 2009); *SDCBA Legal Ethics Opinion 2011-2* (May 24, 2011).

[62] *See Virginia State Bar ex rel. Third District Comm. v. Hunter*, Va Cir. Ct., No. CL12-335-7 (June 5, 2012) (an attorney violated the Rules of Professional Conduct when he discussed details of his cases on his blog without obtaining the consent of his clients).

b. *E-discovery and Litigation*

The availability of information through social media has no doubt influenced the way attorneys investigate and develop strategies for litigating cases. With information about the parties, witnesses and opposing counsel merely a click away, attorneys must carefully consider how to properly access and use such information, and how opposing counsel may use information similarly accessible.

Using search engines, such as Google, at the beginning of the informal phase of discovery can be an invaluable tool in determining potential sources of discoverable evidence, such as social networking sites. If the plaintiff's site is not password-protected and is open to the public, counsel generally may view, copy and print the content. Attorneys cannot, however, circumvent an individual's privacy settings or inappropriately access restricted information.[63]

With respect to formal discovery, generally, under the Federal Rules of Civil Procedure, a party may seek discovery of "any non-privileged matter that is relevant to any party's claim or defense." However, even relevant information may be excluded from discovery if the potential harm of the requested discovery outweighs the probative value of the evidence sought. Prior decisions indicate that courts will enforce properly tailored discovery requests for potentially relevant information from social networking sites. For example, in a 2010 sexual harassment case brought by the Equal Employment Opportunity Commission on behalf of the plaintiff and similarly situated employees, a federal court in Indiana allowed discovery of the plaintiff's social networking profile information and postings relating to general emotions and mental states.[64] The court said that while privacy concerns may be relevant to questions of discovery being burdensome or being sought for a proper purpose, a person's expectation that communications are private does not shield them from discovery. In a more recent case, however, a district court in California found similar requests to be "overbroad and vague."[65] Additionally, courts may be inclined to punish plaintiffs who take steps to prevent the discovery of relevant social media content. For example, a New Jersey district court recently sanctioned a personal injury plaintiff for spoliation following the deletion of his Facebook

[63] For example, the New Jersey Office of Attorney Ethics ("OAE") alleged that two attorneys impermissibly caused a paralegal to "friend" the plaintiff in a personal injury case so they could access information on the plaintiff's Facebook page that was not publicly available. The OAE alleged that the conduct violated Rules of Professional Conduct governing communications with represented parties, along with other rules. Both attorneys denied the charges and claimed that they only directed the paralegal to do general internet research, and that they did not tell her to add the plaintiff as a "friend" to gain access to otherwise private information. *See* Donald Scarinci, *Warning for Lawyers: Facebook Is Not Always Your Friend*, Martindale.com blog (Sept. 28, 2012), http://blog.martindale.com/warning-for-lawyers-facebook-is-not-always-your-friend. While no New Jersey ethics opinion to date addresses "friending" individuals in connection with litigation, the bars of New York, New York City, Philadelphia, and San Diego have deemed it unethical. *See, e.g., SDCBA Legal Eth. Op. 2011-12* (May 24, 2011); *New York State Bar Ass'n Comm. on Professional Ethics*, Opinion 843 (Sept. 10, 2010).

[64] *EEOC v. Simply Storage Mgmt., LLC*, No. 1:09 -cv-1 223 -WTL -DML, 2010 U.S. Dist. LEXIS 52766 (S.D. Ind. May 11, 2010).

[65] *Mailhoit v. Home Depot U.S.A., Inc*., 2012 U.S. Dist. LEXIS 131095 (C.D. Cal. Sept. 7, 2012). In another case, a Georgia district court held that opt-in plaintiffs were not required to produce all social media postings made "during … working hours," finding the request too speculative to justify the burden imposed on the class plaintiffs. *Jewell v. Aaron's, Inc*., No. 1:12–CV–0563–AT (N.D. Ga. July 19, 2013).

account which defendants were trying to access.[66]

Social media will continue to play a major role in how attorneys litigate cases (whether in private practice or as in-house counsel), including how juries are selected and what information the jurors themselves can access. The more information attorneys can harness about the major players in a given case, the greater their potential advantage—up and until they step over the line and inappropriately access such information.

6. Colleges and Universities

Some states are beginning to restrict the ways in which colleges and universities can access applicants' and students' social media activities, including prohibitions on public or nonpublic academic institutions from requesting or requiring current students or applicants to disclose account information.[67]

In collegiate sports, too, social media is increasingly being utilized by coaches to contact, recruit and gather information about players. For players, it's a way to get recruited, control the message and interact with fans and other recruits at unprecedented levels. And, like in the workplace, misuse of the media can have unfortunate consequences.[68] To keep up with social media, some schools are hiring individuals to monitor the social media of prospective student-athletes and to make sure that improper interaction is not occurring, as well as to ensure confidential information, such as under Family Educational Rights and Privacy Act, is not being disclosed.

Of course, schools also are employers; while universities and colleges need to institute effective policies and procedures to address their use of social media in recruiting, they also must address social media use in the employment context.

IV. Regulating Social Media Activity and Monitoring Compliance

After considering the significant potential liability and other risks employers face from employees' social media use as well as the necessity of social media in today's workplace, how far should employers go in monitoring these communications? And how far can they go? Although the Fourth Amendment to the U.S. Constitution prohibits unreasonable searches and seizures by the government, it generally does not apply to private sector employers. While

[66] *Gatto v United Airlines and Allied Aviation Serv.*, No. 10-cv-1090, 2013 U.S. Dist. LEXIS 41909 (D.N.J., Mar. 25, 2013).

[67] *See Employer Access to Social Media Usernames and Passwords 2013,* National Conference of State Legislatures, http://www.ncsl.org/issues-research/telecom/employer-access-to-social-media-passwords-2013.aspx (last visited Sept. 12, 2013).

[68] *See, e.g., Social Media For Universities and Colleges--Beyond Recruiting,* Jackson Lewis, (Feb. 1, 2012) http://www.workplaceprivacyreport.com/2012/02/articles/social-networking-1/social-media-for-universities-and-collegesbeyond-recruiting/ (a high school football player was expelled and received negative media attention in connection with comments posted on his Twitter account).

private sector employees may have a constitutional right to privacy in a limited number of states,[69] employer conduct generally is limited by federal and state privacy laws, and common law principles, including:

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.[70] The *Stored Communications Act ("SCA")*, part of the ECPA, covers stored electronic communications.

In one case, a New Jersey district court grappled with the question of whether a private Facebook page is protected by the SCA, finding that while non-public Facebook wall posts are covered, under the facts of that case, the "authorized user exception" of the SCA applied. The case involved an existing "friend" of the plaintiff—authorized to access the plaintiff's wall postings, who had taken screenshots of her Facebook postings and provided them unsolicited to the plaintiff's employer. Relying on the testimony that the "friend" had acted on his own initiative, and the employer had not solicited this action, the court found that the SCA exception applied.[71]

State Law. Various states protect a person's right to privacy through state constitutions, state statutes and common law. Some states, for example, prohibit electronic monitoring of employee communications without two-party consent. In addition, as mentioned above, it is illegal in a number of states for employers to ask employees or applicants for their Facebook and other social media passwords.

Common law privacy 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 social media use is "intrusion upon the plaintiff's seclusion or solitude."[72] Under this theory, an employee must generally 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

[69] *See, e.g.,* Cal. Const. art. I, § 1; Fla. Const. art. I, §§ 12, 23, and Wash. Const. art. I, § 7.
[70] 18 U.S.C. § 2511(2)(a)(1)(2006).
[71] *Ehling v. Monmouth-Ocean Hosp. Serv. Corp*., Civ. No. 2:11-cv-03305 (WJM) (D.C.N.J. August 20, 2013) ("The evidence does not show that Defendants obtained access to Plaintiff's Facebook page by, say, logging into her account, logging into another employee's account, or asking another employee to log into Facebook. Instead, the evidence shows that Defendants were the passive recipients of information that they did not seek out or ask for. Plaintiff voluntarily gave information to her Facebook friend, and her Facebook friend voluntarily gave that information to someone else.") *But see Brian Pietrylo v. Hillstone Rest. Group*, 2009 U.S. Dist. LEXIS 88702 (D.N.J. Sept. 25, 2009).
[72] RESTATEMENT (SECOND) OF TORTS § 652 (1965).

reasonable expectation of privacy in the electronic communications.[73] 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.

While different employers can reach different conclusions about whether to monitor employees' social media use, in all cases, employers should avoid efforts to gain unauthorized access to an employee's account information and should carefully consider any employment decisions it intends to implement on account of information obtained through social media.

V. Avoiding the Risks

A. Implement a Social Media Policy

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

The precise contours of an employer's social media use policy will depend on the organization, its culture and approach to social technologies, its business and that business' regulatory environment, and the nature of work performed. For instance, a social media use policy for health care workers may be very different from a policy aimed at employees who are encouraged to use social media for developing client relationships. Even for employers that do have social media policies, they often do not address key issues such as the company's presence online, regulatory requirements that apply in their industry, and how managers and supervisors should and should not be using the medium for employment purposes.

As a general matter, employers seeking to implement or revise a social media policy should consider, with the assistance of counsel, the following general provisions and implementation procedures:

- Language addressing postings that contain specific proprietary and confidential company information, as well as discriminatory statements or sexual innuendos regarding co-workers, management, customers or vendors will not be tolerated and will subject the individual to discipline.

[73] *See, e.g., Thygeson v. U.S. Bancorp*, 2004 U.S. Dist. LEXIS 18863 (D. Or. Sept. 15, 2004) (holding employee had no reasonable expectation of privacy in the internet websites he accessed while using his work computer where the company only gathered information available on its own network and had a policy regarding personal computer use and monitoring).

- Specification that the policy's prohibitions apply to postings and blogging occurring at any time, on any computer.
- Supplemental amendment to the company's handbook policies to provide a detailed explanation of what is considered "acceptable use."[74]
- Policy distribution to all employees in employee handbooks, policy manuals (as a stand-alone policy), paycheck reminders, and annual or more frequent e-mail reminders.
- Required employee acknowledgments for receipt of all of the above.
- Uniform policy enforcement, training and monitoring as appropriate.

As noted above, before implementing a social media policy, employers must take care not to unlawfully restrict protected concerted activity. According to the Acting General Counsel's third report, a policy is more likely to avoid infringing upon an employee's right to engage in protected concerted activity if it "provides sufficient examples of prohibited conduct so that, in context, employees would not reasonably read the rules to prohibit Section 7 activity." Consider the following examples contained in the Acting General Counsel's report:

- A social media policy that prevented "inappropriate postings that may include discriminatory remarks, harassment and threats of violence or similar inappropriate or unlawful conduct" found to be lawful "since it prohibit[ed] plainly egregious conduct, such as discrimination and threats of violence."

- The same policy, which commanded that employees be respectful and "fair and courteous" in connection with "posting of comments, complaints, photographs, or videos," could be construed as overly broad.

- Policy which contained additional guidance that individuals should not post items that "could be viewed as malicious, obscene, threatening or intimidating" or "contribute to a hostile work environment on the basis of…any…status protected by law or company policy" would not infringe upon an employee's right to engage in protected concerted activity.[75]

B. Consider Hiring a Social Media Specialist

As companies struggle to keep up with the rapidly evolving world of social media, some businesses have decided to hire social media managers. While in many instances this may be an effective technique, companies should be leery of the "jump first, look second" approach, and, instead,

[74] 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.

[75] The Acting General Counsel's report noted that a social media policy's "savings clause," stating the policy would "be administered in compliance with applicable laws and regulations (including Section 7 of the National Labor Relations Act)," was insufficient to cure ambiguities in the policy's overbroad rules.

should ask several key questions before hiring a new employee with responsibility for a company's social media existence and, therefore, its brand.

Qualifications:

- What qualifications are you looking for? Often companies seek a younger employee who is "tech-savy." Traditional employment issues notwithstanding (*i.e.*, age discrimination when an "older" employee is not hired/considered for a position), companies must also consider what their social media mission/focus will be. For example, to the extent a company utilizes social media as a marketing tool, will you want your social media manager to have a background in marketing? Similarly, to the extent you wish to utilize social media to handle client/customer complaints, will you want your social media manager to have a background in customer relations? Will you hire an external candidate who is perhaps unfamiliar with your company and its mission, or will you hire an internal candidate who understands your culture and client/customer base?

Responsibilities:

- What products/services will the social media manager be responsible for discussing/marketing?
- Will the social media manager have total freedom to explore and execute social media opportunities?
- What policies will the social media manager be responsible for implementing? Will the social media manager have responsibility for implementing the company's social media policy to employees and managers as well?
- What steps have been taken to ensure the social media manager will protect confidentiality of company and personal information?

Training/Protocols:

- What training will be provided to your social media manager? For example, will the social media manager be trained on what information he/she should or should not consider when examining posts by customers and/or employees?
- What policies will govern your social media manager's employment? Will the social media manager be permitted to "friend" employees/subordinates on social media or establish policies for employees to follow?
- What safety protocols will be in place? For example, if your company has a Facebook page, will you social media manager be responsible for maintaining the password and access to same? How will the company transition its social media presence if and when the social media manager separates from employment?

While the above list is by no means exhaustive, it demonstrates some of the additional considerations that must be examined when a company wishes to create or expand its social media presence. Companies are often unaware of the need to consider these questions prior to

implementing a social media policy or hiring a social media manager. However, examining these points will help ensure your company's social media experience flows more smoothly.

VI. Conclusion

Social media use presents a multitude of opportunities—and risks—for employers. As more and more companies turn to social media for business purposes, it is imperative for employers to provide employees with clear guidelines detailing what is and what is not acceptable use. Employers also will need to understand the limits of using social media for hiring, promotion and termination decisions. Organizations should, among other things, develop and shape their policies, training and discipline concerning social media with an eye toward their particular businesses, regulatory environments, and whether they are in the public or private sectors. This paper just scratches the surface of the multitude of issues that must be considered in the age of social media; new issues emerge almost as rapidly as new technology in this rapidly evolving area of the law.

For additional information, please contact:

Joseph J. Lazzarotti, CIPP
Shareholder
Morristown Office
(973) 538-6890
lazzaroj@jacksonlewis.com

Nicky Jatana
Shareholder
Los Angeles Office
(213) 689-0404
jatanan@jacksonlewis.com

Jason C. Gavejian, CIPP
Shareholder
Morristown Office
(973) 538-6890
gavejiaj@jacksonlewis.com