SOCIAL media may be the antithesis of privacy. After all, it’s called “social” media because its users intend for their postings to be viewed by people in their social screen world. While social media arguably diminishes the user’s expectation of privacy, some ancient and persistent vestiges of privacy concepts linger over social media postings.

For the workplace, social media has become a window for employers to see inside their employees’ personal, and not so personal, lives. Employers who want to track employees’ (or potential employees’) use of social media, and act on what they see, are challenging whether the traditional legal concepts for protecting privacy should attach to users of social media.

Technology continues to outpace the law that governs it. As a result, case law in the United States is sparse as to the rights and limitations of an employer who seeks to monitor its employees’ social media activities. Generally, employers may monitor an employee’s social media use and make employment decisions based upon the content of the employee’s online website or profile. But employers must be cautious with social media monitoring, especially in two main areas: (1) that the employer obtained the social media information properly and (2) that the employer does not use the obtained information in an unlawfully discriminatory, retaliatory, or other prohibited manner.

I. What is Social Media?

A. Current Tools and Technologies

“Social media” has been defined as “an umbrella term for social interaction using technology (such as the Internet or cell phones) with any combination of words, pictures, video, or audio.” In the beginning, the Internet, or Web 1.0, was “read only.” Now, Web 2.0 sites are “interactive and visitors can communicate, collaborate, and socialize with the web host and each other. Users
can share pictures, video, music, articles, or other user-generated content.”

Social media is appealing to big and small businesses alike. Indeed, credible companies are increasingly turning to social media both to develop a customer base and to build or maintain brand reputation. Many statistics now available allow companies to track social media usage and effectiveness worldwide. Here are some recent examples:

- **11%** of all time spent online in the U.S. is spent on social networking sites.
- Up from **13.8%** in 2008, over **25%** of U.S. Internet page views occurred at one of the top social networking sites in December 2009.
- In the U.S., **234 million** people age 13 and older used mobile devices in December 2009 alone.
- LinkedIn has over **75 million** users. Twitter now has more than **190 million** users, processes approximately **65 million Tweets** per day, and registers over **330,000 new users per day**.
- As of April 2010, an estimated **41.6%** of the U.S. population had a Facebook account.
- With a population of over **550 million** users, roughly one twelfth of the world’s population, Facebook would rank as the world’s third largest country, behind only China and India.

Given these statistics, more and more companies are compelled to take notice of the significant impact social media can have on the marketplace.

## B. Most Commonly Used Social Media Sites

As social media continues to grow and evolve, the ability to reach more consumers globally continues to increase. Twitter, for example, now reaches Japan, Indonesia, and Mexico, among other markets. This helps companies advertise in multiple languages and reach a broader range of consumers.

One of the ways social media is able to grow and evolve is through its variety. Social media takes on a myriad of forms, including these, which every international company, their CEOs and consumers are using, or are about to use:

1. **Blogs** (e.g., Blogger, LiveJournal, Open Diary, WordPress, TypePad, Vox, Xanga): Blogs are regularly updated websites (i.e., the entries are in reverse chronological order with the newest entry at the top) that typically combine text, graphics or video, and links to other sites. Blogs are often informal, taking on the tone of a diary or journal entry. There are blogs of all sorts, ranging from very personal to providing mainstream news updates. Blogs also encourage interactive dialogue with followers by allowing readers to leave comments.

2. **Microblogging / Presence applications** (e.g., Twitter, Yammer, Jaiku, Plurk, Tumblr,
Posterous): Microblogs are comprised of extremely short written blog posts, similar to text messages. Twitter is an example of a microblog service that lets users broadcast short messages, up to 140 characters long (“Tweets”), using computers or mobile phones.\textsuperscript{13}

3. Podcasts (e.g., audio sharing): Podcasts (from a blend of “iPod” and “broadcast”) are audio or video files that users can listen to or watch on their computers or portable media devices. Podcasts are usually short and often free, and users can subscribe via their computers or portable media devices to receive new podcasts automatically.\textsuperscript{14}

4. Social networks and online communities (e.g., Facebook, MySpace, LinkedIn, Friendster, Sermo, Ning, Orkut, Skyrock, Ozone, Xing, Bebo): Social networks are online communities that allow users to connect and exchange information with clients, colleagues, family and friends who share common interests.\textsuperscript{15} In many social networks, users create profiles and then invite people to join as “friends.” There are many different types of social networks and online communities, many of which are free. The sites typically range from general use to those targeted for a specific demographic or area of interest.\textsuperscript{16}

5. Online video share (e.g., YouTube, Blip.tv, Vimeo, Viddler, sevenload, Zideo): Video sharing allows individuals to upload video clips to an Internet website. The website’s video host will then store the video on its server and show the individual different types of codes to allow other users on the site to view or comment on the posted video.\textsuperscript{17}

6. Widgets: Allegedly short for “window gadget,” a widget is a graphic control on a website that allows the user to interact with it in some way. Widgets can be easily posted on multiple websites, often have the added benefit of hosting “live” content, and typically take the form of on-screen tools (e.g., daily weather updates, clocks, event countdowns, stock market tickers, flight arrival and departure information, etc.).\textsuperscript{18}

7. Wikis (e.g., Wikipedia, Medpedia, Wetpaint, PBworks): Wikis, derived from the Hawaiian word for “fast,” feature technology that creates access to webpages where users are encouraged to contribute to and modify the existing content.\textsuperscript{19} A wiki site can be either open or closed, depending on the preferences of its community of users. An open wiki site allows all site users to make changes and view content, while a closed wiki only allows community members to edit and view content.\textsuperscript{20}
C. Current Trends in Corporate Use of Social Media Sites

Just a few years ago, commentators pondered if corporations would adopt and use social media tools. Today, the only question is how much do they use them. According to Fulbright & Jaworski L.L.P.’s 2010 Litigation Trends Survey, approximately one fourth of surveyed companies reported using LinkedIn in pursuit of a business purpose. Others reported use of Twitter and/or Facebook. Another recent survey found that 91% of “Inc. 500” companies are reporting use, both internally and for business purposes, of at least one social media site. Surveyed companies overwhelmingly responded that social media has been successful for their businesses. For example, every social media tool studied enjoys at least an 82% success level with business users. Measuring success was determined as improving their communications approach, building internal knowledge, improving marketing and sales, and guaranteeing long-term sustainability and growth.

In August 2009, a research study found that 81% of senior management, marketing, and human resources executives of companies view social media as a valuable tool to build their company’s brand and to enhance relationships with customers. However, the study also found that an equal number, 81%, view social media as a corporate security risk. For that reason many organizations do not allow applications like Facebook, Twitter, LinkedIn, etc., to be used by employees via their corporate networks. These technologies, however, are difficult to control and can be easily accessed outside of corporate networks. Consequently, companies and executives face difficult issues regarding how to handle the use of social media, both in and outside of company time.

IV. The Use of Surveillance Software by U.S. Employers

A. Increased Use Due to Increased Awareness of Social Responsibility, Corporate Governance, and Compliance Guidelines

There is a burgeoning “cottage” industry of surveillance software providers. The technology, while originally primitive and limited in availability, has advanced in its sophistication dramatically in the past five years. Moreover, the multiple uses for the collected data have inspired the development of software with more precise findings. This in turn has brought the price-point for such software into the reach of many more companies.

Social media monitoring software is perhaps the fastest growing category of surveillance tools. Many companies embrace the technology to gain, competitive business intelligence and attempt reputation management. Vendors of social media surveillance software represent, for example, that the software can identify online postings to determine such things as where conversations about their products occur most often, or how much their products are being discussed versus those of a competitor. Many of
these monitoring tools are available as Software as a Service (SaaS) over the internet, making it easy for companies to access and deploy them.

Some corporations are now turning their surveillance software to monitoring internal company activity. Companies are seeking employee monitoring software applications designed to prevent employee theft and data leakage, and to eliminate inappropriate online activities. Many software surveillance companies pitch their surveillance software to corporations offering “the ability to monitor the social networking communications of their employees” on all major social networks such as Facebook and Twitter. Customers are told, for example, the software “provides granular and real-time tracking to eliminate significant corporate risks” related to: compliance issues, leakage of sensitive information, HR issues, legal exposure, brand damage and financial impact.

B. Available Tools are More Sophisticated than Last Year’s tools and the Innovation of New Tools is Increasing Exponentially

Like everything in the computer world, today’s technology will be outdated by the time you finish reading this article. Surveillance software is no exception. Basic and inexpensive techniques have always been available. Automating the process via sophisticated software that is installed at the network level will make monitoring more commonplace, say commentators. Some surveillance software purveyors offer applications “deployed discretely on PCs in an organization” with monitoring managed from a centralized location. The difference is where the employer has “access” to the employees’ activities – at the network level or at the end point – and the ability to control their communications, computer applications and online activities (not just the information that flows over the network). Some of the surveillance software purveyors represent they can monitor employees’ social media activities even from devices like mobile phones, not necessarily provided by the company to the employee.

C. Basic and Inexpensive Methods

Employers can monitor social media use by employees at little or no cost, except for the personnel and work time necessary to operate the on-line search tools. Here are some examples:

- Google Alerts – a content monitoring service, offered by the search engine company Google, that automatically notifies users when new content from news, web, blogs, video and/or discussion groups matches a set of search terms selected by the user. Alerts can be created for each employee’s name.
- Facebook Search – Facebook’s own search features allows searches by specific names. Searches can be limited to only publicly posted status updates.
The same application can search Twitter conversations.

- TweetDeck – an Adobe AIR desktop application for Twitter, Facebook, LinkedIn, Google Buzz, Foursquare and MySpace. It allows real-time keyword searches, and users can send and receive tweets and view profiles.
- Yahoo Pipes – a web application from Yahoo! that provides a graphical user interface for building data mashups (combinations of data from more than one Web data source into a single integrated Web application) that aggregates web feeds, web pages, and other services. The application works by enabling users to “pipe” information from different sources and then set up rules for how that content should be modified (by an employee’s name, for example).
- Desk Tube – a desktop application that allows users to browse and search YouTube videos, and to access Twitter and Facebook accounts all from the same location.
- Spokeo.com – a search engine and self-described “online USA phone book” that aggregates people-related information from purportedly public sources, including phone directories, social networks, marketing surveys, mailing lists, government censuses, real estate listings, and business websites.

D. Mechanistic Methods

Many vendors offer corporations the ability to monitor various aspects of their businesses via surveillance software. These companies offer software which can monitor a company’s business and competitive intelligence via network and server monitoring, website monitoring, and spy software.  

Many vendors also offer corporations the ability to monitor the social networking communications of their employees. Some vendors promise desktop-level visibility into employees’ activities, and most currently available software can: capture all keystrokes typed, take screenshots of any computer activity, monitor and read all employee communications such as email and instant message conversations, monitor and block software application use on a scheduled basis, monitor and filter Internet use on and off the company network, monitor PCs that never connect to a network, screen all email attachments for sensitive data, track documents to follow all file use (deletions, renaming, moving, etc.), monitor removable media, destroy data remotely, and locate and recover stolen computers.
V. Legal Considerations for Monitoring Employee’s Social Media Activities

A. General Privacy Law Considerations When Monitoring Social Media Use

No United States statutes or regulations specifically govern the monitoring of employees’ social media use. The Electronic Communications Privacy Act of 1986 (“ECPA”), which is intended to provide individuals with some privacy protection in their electronic communications, has several exceptions that limit its ability to provide protection in the workplace. Consequently, courts seeking to address electronic monitoring of employees must look to the awkwardly fitting laws that more generally govern privacy rights and employment.

Although U.S. courts have long recognized the right to privacy, the protections afforded by the U.S. Constitution address only government action, and so apply only to governmental employees. Many states, however, have extended certain privacy protections to non-governmental employees through state constitutions and statutes. Moreover, a common law right of privacy is recognized in the majority of the American jurisdictions. In fact, the tort action for invasion of the right of privacy, in one form or another, is currently recognized in thirty-six states. Thus, while a legal analysis of the privacy rights of public and private employees differs, the basic principles are very similar.

In sum, the right of privacy protects against “interference with the interest of the individual in leading, to some reasonable extent, a secluded and private life, free from the prying eyes, ears and publications of others.” This broad right can give rise to four, separate claims: (1) unreasonable intrusion upon the seclusion of another; (2) appropriation of the other’s name or likeness; (3) unreasonable publicity given to the other’s private life; or (4) publicity that unreasonably places the other in a false light before the public.

Electronic monitoring could most conceivably give rise to the first of those, a claim of unreasonable intrusion upon seclusion. Such a claim could result in liability if the defendant “intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns” and such intrusion would be “highly offensive to a reasonable person.” For sure, “there is no liability for the examination of a public record concerning the plaintiff. . . . Nor is there liability for observing him or even taking his photograph while he is walking on the public highway, since he is not then in seclusion, and his appearance is public and open to the public eye.” In other words, the defendant must have intruded into a private place. The same principle appears to apply to one’s online activities.

Intrusion into a private place is the focus of the Stored Communications Act (“SCA”) which has, perhaps, become the primary federal law used to regulate social media monitoring. The SCA is designed to protect private, electronic communications. Specifically, the SCA makes it an offense to “intentionally access[ ] without authorization a facility through which an electronic communication service is provided . . .
and thereby obtain[ ] . . . access to a wire or electronic communication while it is in electronic storage in such system.” 47 Exceptions to SCA prohibitions include “conduct authorized . . . by a user of that service with respect to a communication of or intended for that user.” 48 But the SCA was written before the advent of the Internet and, as a result, “the existing statutory framework is ill-suited to address modern forms of communication” like social media. 49

Applying the applicable laws, a critical issue is whether an employee has a reasonable expectation of privacy, and that is determined on a case-by-case basis. When evaluating a particular case, some primary considerations may include: whether the employee’s social media profile or website is public or private in nature, the employer’s social media policy, and the terms and conditions of the social medium itself.

B. Privacy Expectations Will to Some Extent Depend on the Whether the Employee’s Profile or Website is Public or Private

When an individual maintains a social media website that is accessible to the general public, he or she cannot have a reasonable expectation of privacy with respect to the content of that site. In Moreno v. Hanford Sentinel, Inc., 50 a California district court rejected an invasion of privacy claim based on information posted on a MySpace page. The named plaintiff, Cynthia Moreno, had posted her opinion about her hometown in an “Ode to Coalinga.” The ode began by saying “the older I get, the more I realize how much I despise Coalinga,” and then made several negative comments about the town and its inhabitants. Someone forwarded the ode to the editor of the local newspaper who, in turn, published it in the newspaper’s letters section. The community reacted violently to the ode, including death threats and a shot at the home of Moreno’s family. As a result, Moreno and her family filed suit against the newspaper, claiming public disclosure of private facts.

Affirming the district court’s decision, the court of appeals held that the plaintiffs could not state a cause of action for invasion of privacy because the ode was not private. 51 The court found Moreno’s publication of the ode on MySpace was an “affirmative act that made her article available to any person with a computer” and “no reasonable person would have had an expectation of privacy regarding the published material.” 52 Moreno thus shows that a person who openly shares information on a public social media site will likely have little ground to complain when the information is re-published.

In contrast, when an employee maintains a private social media website, he or she will likely receive some protection. To that end, when an online website or profile is truly private, an employer who uses improper means to gain access to such information may be held liable.

A New Jersey jury, for example, awarded two plaintiffs lost wages and punitive damages against an employer found to have accessed a MySpace chat group without authorization. 53 The plaintiffs, employees of a restaurant, had
set up an invitation-only MySpace chat group. In the initial posting, one of the plaintiffs stated that the purpose of the group would be to “vent about any BS we deal with at work] without any outside eyes spying in on us. This group is entirely private, and can only be joined by invitation.” After being shown the website by another employee, a manager requested the employee’s password to log onto the site. Based on the content viewed, the manager fired the employees who created the site. They responded by bringing an action against the employer, asserting claims of wrongful termination, invasion of privacy, and violations of wiretapping statutes.

Following the verdict, the court denied the employer’s motion for judgment as a matter of law and motion for a new trial. The employer argued that there was no evidence an invited member of the chat group did not authorize the manager to use her password. The court rejected the argument, ruling the jury could reasonably have inferred that the employee’s purported authorization was “coerced or provided under pressure.”

Similarly, in Konop v. Hawaiian Airlines, Inc., an airline pilot, who created and maintained a website where he posted bulletins criticizing his employer, was able to survive a motion for summary judgment. Alleging that Hawaiian Airlines, Inc. had viewed his website without authorization, the pilot asserted state tort claims, as well as violations of the federal Wiretap Act, the Stored Communications Act, and the Railway Labor Act. The court found the pilot’s website to be private. The pilot controlled access to his website by requiring visitors to log in with a user name and password. He created a list of fellow employees who were eligible to access the website. And he programmed the website to allow access only when a person clicked the “SUBMIT” button on the screen, indicating acceptance of the terms and conditions that prohibited any member of management from viewing the website and prohibited users from disclosing the website’s contents.

Despite the pilot’s precautions, a Hawaiian Airlines vice president was able to view the website. He did so by obtaining permission from two employees to use their names to gain access to the site. One or both of the employees had never logged onto the website to create an account.

The court of appeals’ analysis of the pilot’s SCA claim is significant. Hawaiian argued that it was exempt from liability under the SCA because Section 2701(c)(2) of the act allows a person to authorize a third party’s access to an electronic communication if the person is (1) a “user” of the “service” and (2) the communication is “of or intended for that user.” The district court granted summary judgment for Hawaiian, but the court of appeals reversed, finding that the plain language of Section 2701(c)(2) indicates that only a “user” of the service can authorize a third party’s access to the communication. The statute defines “user” as one who (1) uses the electronic communications service and (2) is duly authorized by the provider of such service to engage in such use. Finding no evidence that the consenting employees actually used the website, as opposed to
merely being eligible to use it, the court held that the Section 2701(c)(2) exception did not apply. This decision shows not only that a court may recognize one’s privacy when the person takes great steps to protect it, but also that employers cannot use unauthorized means to monitor their employees.

C. Privacy Expectations May Depend on an Employer’s Policies and Practices.

The employer’s written policies and practices may also become important in determining an employee’s privacy rights. Courts are focusing on any evidence that employers affirmatively took steps to inform employees of policies or regulations that govern their social media use. Although courts are just starting to grapple with the impact of employer policies on social media use, courts firmly embrace using employer policies to determine the privacy expectations for employee emails. To measure privacy expectations for employee emails, the court in In re Asia Global formed, and other courts have adopted, the following test: (1) is there a corporate policy; (2) does the company monitor employee email use; (3) do third parties have a right of access; and (4) did the company notify the employee or did the employee know about the use and monitoring policies?

While it can be anticipated courts reviewing privacy expectations related to social media will make similar analyses, the full value of any guidance by the above factors is uncertain. A potentially persuasive argument can be made that social media is simply the next generation of electronic mail, and that courts should extend their analysis of employee privacy expectations for emails to employee privacy expectations for social media. Conversely, the argument can be made that there are inherent differences between social media and email, and that those differences substantially diminish any privacy expectations for social media. It can be argued, for example, that social media (unlike email) is specifically designed to reach a large number of people. Posting information on a social media site is not just like sending an email. It is like sending a mass email.

In addition, it appears only two states—Delaware and Connecticut—require employers who engage in electronic monitoring to give written notice to their employees. The Connecticut statute sets forth noteworthy exceptions; it allows an employer to monitor without prior notice when “an employer has reasonable grounds to believe that employees are engaged in conduct which (i) violates the law, (ii) violates the legal rights of the employer or the employer’s employees, or (iii) creates a hostile workplace environment, and (B) electronic monitoring may produce evidence of this misconduct.” Employers in the remaining 48 states can argue that the absence of a statutory duty to provide notice of electronic monitoring suggests an absence of privacy rights.

In any event, the analyses for determining an employee’s privacy rights will likely be fact specific, thus an employer’s policy and practice regarding social media will likely be analyzed to evaluate whether an employee’s expectation to privacy is reasonable.

Consequently, prudent companies have come to adopt written social media
policies to regulate their employees’ social media activity. The following points, where appropriate, should be considered for inclusion in social media policies:

- A clear statement that misuse of social media can be grounds for discipline, up to and including termination;
- A prohibition on disclosure of the employer’s confidential, trade secret or proprietary information;
- A request that employees keep company logos or trademarks off their blogs and profiles and not mention the company in commentary;
- An instruction that employees not blog or post during business hours, unless for business purposes;
- A request that employees bring work-related complaints to human resources before blogging or posting about such complaints;
- A prohibition on using company e-mail addresses to register for social media sites;
- A prohibition on posting false information about the company or its employees;
- A general instruction that employees use good judgment and take personal and professional responsibility for what they publish online;
- A demand that all employees with personal blogs that identify the employer include a disclaimer that the views expressed on the blog are those of the individual and not the employer; and
- A prohibition on “Friending” members of management by non-management personnel, and vice versa.

D. Privacy Expectations May Depend on the Terms and Conditions of the Social Medium.

Social media sites do not “guarantee complete privacy,” so a court may conclude that the employee or applicant cannot have a reasonable expectation of privacy. In fact, Facebook’s privacy policy expressly states:

Risks inherent in sharing information. Although we allow you to set privacy options that limit access to your information, please be aware that no security measures are perfect or impenetrable. We cannot control the actions of other users with whom you share your information. We cannot guarantee that only authorized persons will view your information. We cannot ensure that information you share on Facebook will not become publicly available. We are not responsible for third party circumvention of any privacy settings or security measures on Facebook . . . .

A New York Supreme Court recently relied upon the terms and conditions of Facebook and MySpace to reject a personal injury plaintiff’s objection to production of material on those sites. The defendant moved for an order
granting it access to the plaintiff’s current and historical Facebook and MySpace pages on the grounds that the plaintiff had placed information on the sites that was inconsistent with her claims concerning the extent and nature of her injuries, especially her claims for loss of enjoyment of life.73

Ordering the plaintiff to grant the defendant access to her Facebook and MySpace pages, the court relied, in part, upon the policies of those sites. The court noted that Facebook policy states “Facebook is about sharing information with others” and that MySpace “is self-described as an ‘online community’ and as a ‘global lifestyle portal that reaches millions of people around the world.”74 As the court also pointed out, “MySpace warns users not to forget that their profiles and MySpace forums are public spaces and Facebook’s privacy policy set[s] forth, inter alia, that: ‘You post User Content . . . on the Site at your own risk . . . .’”75 Because neither Facebook nor MySpace guarantees “complete privacy,” and because the plaintiff when creating her accounts consented to the sharing of her personal information, the court held that the plaintiff had no legitimate reasonable expectation to privacy. Finally, the court concluded that “given the millions of users, . . . privacy is no longer grounded in reasonable expectations, but rather in . . . wishful thinking.”76

VI. Adverse Employment Actions Based on Social Media Activities

As a general rule, an employer is allowed to consider information on an applicant’s or current employee’s social media profile or website when making employment decisions. This general rule, however, is rife with limitations based in general employment laws.

A. Hiring

Employers certainly use social media sites to vet job candidates. Perhaps the most notable example of such vetting occurred in March 2009 when an applicant offered a job by Cisco tweeted, “Cisco just offered me a job! Now I have to weigh the utility of a fatty paycheck against the daily commute to San Jose and hating the work.”77 Soon thereafter, a Cisco employee posted this reply: “Who is the hiring manager. I’m sure they would love to know that you will hate the work. We here at Cisco are versed in the web.”78

But use of social media information during the hiring process may create liability risks for employers. For instance, an employer is still obligated to adhere to civil rights laws. Title VII of the Civil Rights Act of 1964 (Title VII), as amended, prohibits employment discrimination based on race, color, religion, gender and national origin.79 In addition, the Americans with Disabilities Act of 1990, as amended, prohibits discrimination on the basis of disability.80 Social media profiles often reflect personal attributes that qualify a person as part of a protected group under these statutes. A profile may reveal an applicant’s gender, race, national origin, religious beliefs, age, health problems, political affiliations, sexual orientation and even whether the person plans to have children. Because an adverse employment action based on a person’s
protected status is strictly prohibited whatever the source of the information, an employer monitoring social media should target only information relevant to the applicant’s abilities and qualifications for the particular job position.

In addition to civil rights laws, social media inquiries may be subject to limitations by the Fair Credit Reporting Act (“FCRA”). The FCRA is designed to protect the privacy of consumers’ credit report information and to guarantee that the information supplied by credit reporting agencies is as accurate as possible. Sections 604, 606, and 615 of the FCRA help ensure that applicants or current employees are not denied employment opportunities due to inaccurate or incomplete consumer credit reports. Those sections thus set forth certain responsibilities of employers when using consumer credit reports to hire new employees or evaluate current employees for promotion, reassignment, or retention.

Under the FCRA, if an employer uses a third party service to conduct certain types of background checks, the employer must give prior notice of the check to the individual being investigated. Some states have enacted more restrictive “FCRA plus” laws, which require prior notice and consent from the applicant even if the employer does not use a third party to do the search. Because prior notice affords an applicant time to remove offensive material before the search begins, it potentially defeats the purpose of a social media inquiry.

It is still unclear whether social media profiles are covered under the FCRA. The FCRA provides the following definitions:

- “The term ‘consumer report’ means any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer’s credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer’s eligibility for . . . employment purposes;” and
- “The term ‘investigative consumer report’ means a consumer report or portion thereof in which information on a consumer’s character, general reputation, personal characteristics, or mode of living is obtained through personal interviews with neighbors, friends, or associates of the consumer reported on or with others with whom he is acquainted or who may have knowledge concerning any such items of information.”

So while the legislature and courts have not definitively found that social media monitoring triggers FCRA protections, the above definitions certainly appear broad enough to include reports of a consumer’s social media use.
**B. Discipline and Discharge**

As with hiring, many employers have disciplined or even discharged employees for inappropriate messages on social media.\(^86\) Just recently, a math and science teacher was asked to resign after she complained on Facebook about her job, describing students as “germ bags” and school parents as “snobby” and “arrogant.”\(^87\) Notably, the teacher claimed that she had arranged her privacy settings to limit her profile to selected friends, but Facebook later defaulted her settings to allow viewing by the wider Facebook community.\(^88\)

While many employers have similarly disciplined or discharged employees for comments or other postings on social media sites, such employment actions could run afoul of employment laws. For sure, the same civil rights laws and FCRA considerations described above regarding the hiring process also apply to current employees.

In addition to those considerations, several states prohibit employers from taking adverse action against a current employee for engaging in lawful, conduct while the employee is not at work. Such statutes vary in scope. On one end of the spectrum, several states protect a single, specific activity—such as lawful tobacco use.\(^89\) On the other end, a few states—such as California, New York, and Colorado—protect all “lawful conduct occurring during nonworking hours away from the employer’s premises.”\(^90\) In particular, New York restricts employers from taking *any* adverse employment action against employees engaged in “recreational activities,” meaning “any lawful, leisure-time activity, for which the employee receives no compensation and which is generally engaged in for recreational purposes, including but not limited to sports, games, hobbies, exercise, reading and the viewing of television, movies and similar material.”\(^91\) Exceptions to these statutes may apply, such as when the employer’s restrictions are related to a bona fide occupational qualification, or are necessary to avoid a conflict of interest with the employees’ responsibilities.\(^92\)

These “off-duty activity” statutes may be implicated by social media in numerous ways. For example, the statutes may certainly limit an employer’s ability to terminate an employee who posts photographs of himself smoking tobacco. The broader statutes generally protecting “lawful conduct” or “recreational activities” could also limit an employer’s ability to hire, terminate, or make other employment decisions based on information gleaned from an employee’s social media page. Indeed, in states embracing broad off-duty activity statutes, one could argue that participating in social media sites, such as posting photographs on Facebook, blogging, or even “tweeting” rants about a supervisor, is a “recreational activity” itself and that adverse employment actions based on such participation is unlawfully discriminatory. But, if such participation creates a conflict of interest with the employees’ responsibilities (e.g., negatively impacts an employer’s business interest, customer relations, product image, or coworkers’ rights), an adverse action may be justified.

Also, the National Labor Relations Act (“NLRA”) makes it an unfair labor
practice “to interfere with, restrain, or coerce employees in the exercise of the rights guaranteed in [Section 7 of the NLRA].” Section 7 sets forth several rights, including the right “to engage in . . . concerted activities for the purpose of collective bargaining or other mutual aid or protection.” The National Labor Relations Board (“NLRB”) has held that an employer’s actions violate Section 7 if those actions would “reasonably tend to chill employees” in the exercise of their rights under the NLRA.

Recently, the NLRB announced its plans to prosecute a complaint under Section 7 against American Medical Response of Connecticut, regarding the termination of an employee who posted negative remarks about her supervisor on her Facebook page. The matter began when an employee was asked to prepare a report related to a customer’s complaint about the employee’s work. The employee asked for union representation regarding the complaint, and the company denied her request. The employee then posted a negative comment about her supervisor on her Facebook page, which elicited responses from coworkers and led to further negative comments by the employee. As a result, the company fired the employee, citing violations of the company’s internet policies, which prohibited employees from making disparaging remarks about their employer or supervisors. The NLRB determined that the Facebook postings constituted “protected concerted activity” under Section 7 of the NLRA and that the company’s internet policy was overly broad. While the outcome of this matter is pending, previous guidance has made clear that employees do not have unlimited discretion to publicly criticize their employers under the protections of the NLRA.

For example, in Endicott Interconnect Technologies, Inc. v. NLRB, the court found that an employee’s online communications were not protected under Section 7 as they were disloyal to his employer. As background, after Endicott Interconnect Technologies (“EIT”) permanently laid off 200 employees, an employee (who kept his job) was cited in a newspaper article, commenting on his disagreement with the layoff. In response, an EIT owner reprimanded the employee for his comments. Thereafter, the employee posted on a public website a message that included: “This business is being tanked by a group of people that have no good ability to manage it. They will put it into the dirt just like the companies of the past. . . .” As a result, EIT discharged the employee.

The Endicott court found that the employee’s communications were not protected by Section 7 of the NLRA. The court explained that an employee’s communication to a third party is deemed protected under Section 7 only if: (1) “it is related to an ongoing labor dispute” and (2) “it is ‘not so disloyal, reckless or maliciously untrue as to lose the Act’s protection.’” The court found the employee’s communications were “unquestionably detrimentally disloyal.” Thus, the court concluded that EIT did not violate the Act when it discharged the employee.

Similarly, in Sears Holdings, the NLRB’s Office of General Counsel issued an opinion memorandum concluding an employer’s social media
The employer had issued a social-media policy regarding its employees’ use of blogs, social networks, and other social media. The policy listed several subjects that employees were not permitted to discuss online. The union filed an unfair-labor-practice charge, alleging that the policy violated the NLRA.

In short, the Office of General Counsel concluded that the employer’s policy did not violate the NLRA because it could not reasonably be interpreted in a way that would chill activity under Section 7 of the NLRA. The memorandum explained that a review of a complained-of social media policy requires an evaluation of the policy as a whole, as “a rule’s context provides the key to ‘reasonableness’ of a particular construction.” The general counsel concluded that Sears’ policy against “[d]isparagement of company’s . . . executive leadership, employees, [or] strategy . . . “provided sufficient context to preclude a reasonable employee from construing the rule as a limit on Section 7 conduct.”

Given the decisions in Endicott and Sears Holdings, an employee cannot use Section 7 of the NLRA as a complete shield from discipline or discharge. These decisions also highlight the value of a clear social media policy.

C. Unintended Consequences of Social Media Monitoring

An employer who chooses to monitor its employees’ social media activity may be subject to some unintended consequences. While these consequences are beyond the scope of this article, employers should be mindful of them. In short, social media monitoring can provide an employer too much information. A few issues social media monitoring may raise include: employee records retention; unlawful collection of health records; discrimination and retaliation claims based on the failure to apply employment policies fairly; and expensive litigation discovery.

One of the main drawbacks to social media monitoring is that an employer may become more susceptible to claims where liability is based on the employer’s knowledge of an employee’s inappropriate conduct. For example, if an employee posts a discriminatory remark about a co-worker on the employee’s Facebook page, an employer monitoring that page may be unable to successfully claim lack of knowledge of the posting. Similarly, an employer can be held vicariously liable for its employee’s defamatory statements. Again, if an employer acquires knowledge of the defamatory remark (by way of monitoring or otherwise), it may be easier to impose liability on the employer. To be clear, employers have no affirmative duty to scrupulously police employees’ social media activities. If, however, the employer in fact becomes aware of inappropriate social media activity that impacts the workplace, the employer must take appropriate action. Otherwise, the employer may be perceived as condoning the inappropriate activity.

VII. Conclusion

As employee use of social media continues to increase, employers have a lot of windows through which to see their
employees. The technical ability to monitor social media is rapidly improving. Not only are monitoring tools more sophisticated and accurate now than they were a year ago, the innovation of new tools continues to increase exponentially.

Employers must, however, take care to avoid the legal pitfalls in monitoring employee social media activities. Thus, employers should consider all the circumstances of its social media monitoring, including whether the means of obtaining information are proper and authorized, whether the information is public or private in nature, the type of information they choose to monitor and whether the information is related to a protected status under civil rights laws, and how the employee uses such information to make employment decisions.

2 Id.; see also Alan J. Bojorquez & Damien Shores, Article: Open Government and the Net: Bringing Social Media Into the Light, 11 TEX. TECH. ADMIN. L.J. 45, 47 (2009) (explaining that social media is “the democratization of information, transforming people from content readers into content publishers.”) (citation omitted).
3 See Anthony L. Hall & Deanna C. Brinkerhoff, “Implementing an effective social media policy,” NEVADA EMPLOYMENT LAW LETTER Vol. 15, Issue 6, Mar. 2010 (noting that social media is “becoming an increasingly common method of communication for companies and their employees”).
of-us-internet-users-on-facebook-27-on-myspace/ (last visited Apr. 12, 2010).
5 Id.
6 Id.
12 Id.
14 HHS Center for New Media, supra note 11.
15 Id.
16 Id.
17 Id.
18 Id.
19 Id.


Id.

See e.g., Joshua Brustein, Keeping a Closer Eye on Employees’ Social Networking, N.Y. TIMES (Mar. 26, 2010).

See id.


For example, the act does not prevent access to electronic communications by system providers, which could include employers who provide the necessary electronic equipment or network to their employees. See, e.g., U.S. v. McLaren, 957 F. Supp. 215 (M.D. Fla. 1997).

See e.g., City of Ontario, Cal. v. Quon, 130 S.Ct. 2619, 2627-28 (2010) (“The Fourth Amendment applies as well when the Government acts in its capacity as an employer.”) (internal citation omitted); 15 Causes of Action 2d 139 §§ 1-2 (Sept. 2010) (“A § 1983 claim may also lie for violation of the public employee’s implied constitutional rights to privacy which have been interpreted by the United States Supreme Court as falling within the ‘penumbra’ of several constitutional amendments (and as applied to the states through the Fourteenth Amendment). A Section 1983 claim for violation of the employee’s constitutional rights to privacy will not lie as against a private employer.”)

E.g., CAL. CONST., ART. I, §1; ARIZ. CONST. ART. II, §8, MONT. CONST. ART. II, §10, WASH. CONST. ART. I, §7.

82 Am. Jur. 2d Wrongful Discharge § 165 (July 2010); Restatement (Second) of Torts § 652A, cmt. a (1977).

Id. at cmt. b.

Restatement (Second) of Torts § 652A.

Restatement (Second) of Torts § 652B.

Id. at cmt. c.


Id.

See S. Rep. No. 99-541, at 35-36, 1986 U.S.C.C.A.N. at 3599 (“This provision [the SCA] addresses the growing problem of unauthorized persons deliberately gaining access to ... electronic or wire communications that are not intended to be available to the public.”).


91 Cal. Rptr.3d 858 (Cal. Ct. App. 2009).
Renee M. Jackson, Social Media Permeate the Employment Life Cycle, NAT’L L. J. (Jan. 11, 2010).


Romano, 907 N.Y.S.2d at 656-54.

Id. at 651.


Id. at 651 & n. 9 (quoting Dana L. Flemming and Joseph M. Herlihy, Department: Heads Up: What Happens When the College Rumor Mill Goes Online? Privacy, Defamation and Online Social Networking Sites, 53 B.B.J. 16 (Jan./Feb. 2009)).

Samantha Rose Hunt, How to use technology wrong, TG DAILY (Mar. 18, 2009), http://www.tgdaily.com/trendwatch-opinion/41777-how-to-use-technology-wrong.

Id.


15 U.S.C. §§ 1681 (“There is a need to insure that consumer reporting agencies exercise their grave responsibilities with fairness, impartiality, and a respect for the consumer’s right to privacy.”

E.g., CAL. CIV. CODE § 1785.20.5.


Id.

E.g., ARIZ. REV. STAT. ANN. § 36-601.01(f) (2011); CONN. GEN. STAT. ANN. § 31-40s (West 2011); LA REV. STAT. ANN. § 23:966 (2011); MO. ANN. REV. STAT. § 290.145 (West 2011); NJ STAT. ANN. § 34:6B-1 (West 2011); TENN. CODE ANN. § 50-1-304 (West 2011).

E.g., CAL. LAB. CODE §§ 96(k), 98.6 (West 2011); Accord N.Y. LAB. LAW § 201-d (McKinney 2011); COLO. REV. STAT. § 24-34-402.5 (2007).


See N.Y. LAB. LAW § 201-d (McKinney 2011).


453 F.3d. 532, 537-38 (D.C. Cir. 2006).

Id. at 533-34.

Id. at 534-35.
100 Id. at 535.
101 Id. at 536-37 (citing NLRB v. Electrical Workers Local 1229, 346 U.S. 464 (1953) (other citations omitted).
102 Id. at 537.
104 Id.
105 Id. at *3.
106 Id. at *3-4.
107 See Blakey v. Cont’l Airlines, Inc., 751 A.2d 538, 542-43 (N.J. 2000) (The plaintiff sued her employer, alleging workplace discrimination in violation of Title VII of the 1964 Civil Rights Act, 42 U.S.C.A. § 2000e et seq. Several male employees, in response to the lawsuit, published messages about the plaintiff on an on-line electronic bulletin board used by employees. The plaintiff considered the messages as harassing, false and defamatory. The court held that the electronic bulletin board could be so closely related to workplace environment and beneficial to the employer that continuation of harassment on the bulletin board should be regarded as part of the workplace. The court also held that if the employer had notice that the co-employees were engaged in a pattern of retaliatory harassment towards plaintiff, the employer would have a duty to remedy that harassment).
108 See id.