Social Media Policies for the New Digital Age:

New Issues for Employers

Douglas Dexter
Farella Braun + Martel LLP
San Francisco, CA
ddexter@fbm.com

Internet use is at an all-time high, with 82% of Americans spending, on average, more than 18 hours per week on-line.¹ Social media use is also on the rise: 32% of adult Internet users create content for video sharing and social networking sites like YouTube and Facebook,² 13% are on Twitter, and just under half of the U.S. population is on Facebook.³ As information sharing on social media sites reaches unprecedented levels, employers have taken notice. According to a 2009 survey by Jump Start Social Media, 75% of hiring managers acknowledged using LinkedIn to research job applicants and 48% have used Facebook for hiring purposes.⁴ There are good reasons for employers to be concerned. Digital interconnectedness means that social media has ever greater potential to generate buzz, sell products, expose confidential

² Id.
information, and make or break reputations.

The explosive growth of social media has sparked greater awareness of the privacy concerns that arise from sharing and over-sharing information on the Web. In particular, Internet consumers are becoming increasingly worried that businesses are checking their actions on the Internet. This public awareness has propelled the development of new services and technologies such as reputation scrubbers, social media expiration dates, and other means of empowering Internet users to manage their on-line reputations and digital footprints more effectively. Whether these technologies will be successful in changing the social networking landscape has yet to be seen. However, the popularity of these technologies highlights the tensions that emerge from, on the one hand, a human desire to share information with others, while on the other hand, maintaining one’s privacy. As society moves inexorably deeper into the digital age, employers will need to consider how best to address concerns that arise from employees’ social media use, new technologies that may obscure their digital footprints, and legal developments impacting an employer’s ability to monitor and regulate employee activities.

WHAT IS SOCIAL MEDIA AND WHY SHOULD EMPLOYERS CARE?

Social media is an important component of Web 2.0, a class of web-based applications that focus on user- and consumer-generated content, rather than top-down publishing. Conventionally, social networking sites and social media comprise services that “allow

---


individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system.”

In recent years, social media has become a screening mechanism and monitoring tool for employers. Companies researching employees and job applicants through social media sites may come across everything from inappropriate photographs and commentary to unique or distasteful hobbies. Employers may also find that social networking sites are useful for monitoring employees’ activities, such as tracking whether a worker is disparaging a company’s brand and verifying claims of illness, disability, harassment, and emotional distress. However, in the absence of a clear social media policy, these monitoring actions may backfire, leaving companies vulnerable to claims of discrimination, invasion of privacy, or violation of anti-monitoring or off-duty conduct laws. Yet doing nothing may also result in liability. An employer who turns a blind eye to its employee’s abuses of social media may find itself battling claims based of sexual harassment and hostile work environment, defamation, public disclosure

---

9 See Helen Popkin, Twitter gets you fired in 140 characters or less, MSNBC.COM, Mar. 23, 2009, http://www.msnbc.msn.com/id/29796962/ns/technology_and_science-tech_and_gadgets/t/twitter-gets-you-fired-characters-or-less (Cisco applicant publicly disseminated a dismissive tweet regarding summer internship offer, to which Cisco employee responded).
11 See, e.g., EEOC v. Simply Storage Management, LLC, 270 F.R.D. 430 (S.D. Ind. 2010) (holding that all information from plaintiffs’ social networking profiles relating to their general emotions, feelings, and mental states is discoverable); Romano v. Steelcase, Inc., 906 N.Y.S.2d 650 (N.Y Sup. Ct. 2010) (because plaintiff claimed she was injured and confined to her home, defendant was entitled to discovery of Facebook and Myspace photographs showing plaintiff smiling during vacation in other states).
of confidential information, false advertising, vicarious tort liability, or negligent hiring.12

Social media also represent tremendous potential for generating buzz – both positive and negative. Employers across the country have used social media platforms to expand professional networks, stay in touch with clients, and promote brands. Social media has also created the phenomenon of “viral” marketing. On-line campaigns can be hugely effective because the ease of posting information on the web and forwarding links to contacts enables content to reach thousands and even millions of recipients within a short period of time. For instance, in marketing its new Fiesta car, Ford Motor Company selected 100 individuals to share their experiences on their web logs (“blogs”), Twitter, Facebook, Flickr, and YouTube profiles. The information spread quickly within these individuals’ social networks to their contacts, the contacts of their contacts, and so forth. Within 18 months, the marketing movement had produced 11 million social networking impressions, 11,000 videos, 15,000 tweets, and 13,000 photos, resulting in a huge marketing boost for Ford.13

The viral nature of social media, however, can also create huge risk of reputational damage.14 For example, in April 2009, two Domino’s Pizza employees posted a YouTube video depicting a worker stuffing cheese up his nose, covering a sandwich with nasal mucus, and violating other health code standards while apparently preparing food for delivery.15 Within less than a day, the video had attracted more than a million views and become a public relations

---

14 For instance, in a 2009 study by Deloitte, 74% of surveyed individuals agreed that it is easy to damage a brand’s reputation via social media sites such as Facebook, Twitter, and YouTube. DELOITTE, LLP, ETHICS AND WORKPLACE SURVEY (2009), available at http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/us_2009_ethics_workplace_survey_220509.pdf.
disaster. The company responded quickly, firing the employees, posting an apology video on YouTube, and establishing a dedicated Twitter account to address comments. Nevertheless, a consumer survey conducted by YouGov showed that within just a few days, public perception of the company had gone from “positive” to “negative.”

POTENTIAL PITFALLS FOR EMPLOYERS

Employers who use social media to investigate or monitor existing employees and job applicants may risk potential liability under federal and state laws that prohibit unauthorized access of electronic communications and discriminatory practices, labor laws that protect “concerted” activities, and state off-duty conduct laws. This section provides a brief discussion of how federal laws may apply to an employer’s use of social media or monitoring and regulation of employee social media use.

THE ELECTRONIC COMMUNICATIONS PRIVACY ACT

The primary source of federal electronic privacy law is the Electronic Communications Privacy Act (ECPA), which prohibits unlawful monitoring of electronic communications. Title I of the ECPA modifies the Wiretap Act to regulate interception of electronic communications while in transit. Title II, also known as the Stored Communications Act (SCA), protects against unauthorized access to communications that are not in transit, including e-mails and other data located on network servers. The SCA assesses criminal penalties on anyone who “(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic

\[16\] Id.
\[18\] 18 U.S.C. §§ 2701 to 2712.
communication while it is in electronic storage in such system.”\(^\text{19}\)

Potential liability under the ECPA or SCA could arise in two common situations: (1) where an employer monitors an employee’s electronic activities in the workplace without providing any notice of surveillance, or (2) where an employer obtains, through unauthorized means, access to an employee’s electronic information outside the workplace.

In the first scenario, providing adequate notice and obtaining consent will help manage risk. The ECPA carves out exemptions for electronic interception if one party consents to the interception or if monitoring is done in the ordinary course of business.\(^\text{20}\) Employers contemplating electronic monitoring should implement an electronic monitoring policy that clearly instructs employees to use work resources only for legitimate business purposes, and informs them that their electronic activities may be subject to monitoring. Such a policy will clarify that employees have no expectation of privacy over their electronic activities, and thus, minimize risk of liability under the ECPA.\(^\text{21}\)

In the second scenario, employers should refrain from any attempts to gain unauthorized access to an employee’s private electronic communications outside the workplace, through false, deceptive or coercive means. For example, an employer who accesses a public profile available on a social networking site would be in the clear because the employee has made the information widely available to the public. On the other hand, an employer who secretly obtains access to an

\(^\text{19}\) Id. § 2701(a).
\(^\text{20}\) 18 U.S.C. § 2511(2)(a)(i); Id. § 2511(2)(d).
\(^\text{21}\) Additionally, two states, Delaware and Connecticut, have enacted statutes requiring employers to provide notice to employees prior to monitoring e-mail and Internet access. DEL. CODE ANN. tit. 19 § 705 (2007); CONN. GEN. STAT. § 31-48d (2007). Similar legislation is pending in Massachusetts, New York, and Pennsylvania. See Corey Ciochetti, The Eavesdropping Employer: A Twenty-First Century Framework for Employee Monitoring, AM. BUS. L. J. (2011) (citing proposed legislation).
employee’s private website may be liable for a violation of the SCA.\textsuperscript{22} Employers seeking to minimize risk under the SCA should take steps to ensure that their managers and workers do not use threats, fake profiles, or other deceptive or coercive\textsuperscript{23} practices to gain access to any private, non-public information.

**DISCRIMINATION CLAIMS**

Employers who investigate employees or job applicants on social media sites may also be setting themselves up for a possible discrimination claim under federal or state antidiscrimination statutes.\textsuperscript{24} At the federal level, Title VII of the Civil Rights Act, the Americans with Disabilities Act (ADA), the Genetic Information Nondiscrimination Act (GINA), and the Age Discrimination in Employment Act (ADEA) create protected classes that include age, sex, religion, disability, genetic information, race, color, national origin, and pregnancy.\textsuperscript{25} Employers who fail to hire or take adverse employment action against an individual because of that person’s protected class membership may be liable and subject to a claim of discrimination.

Social networking sites contain a wealth of information about job candidates and employees, including protected class information that would not otherwise be apparent from the individual’s cover letter and resume. Even if the employer did not rely on that protected status in

\textsuperscript{22} See Konop v. Hawaiian Airlines, 302 F.3d 868 (9th Cir. 2002) (potential violation of Stored Communications Act where company executive created unauthorized user account to gain access to employee’s private website); Pietrylo v. Hillstone Rest. Group, Case No. 2:06-cv-05754 (D.N.J. 2008) (upholding jury verdict finding that employer violated Stored Communications Act by improperly pressuring employee to provide user name and password to private MySpace group).

\textsuperscript{23} An issue may also arise where an employer uses key-logging software to track an employee’s user name and password to an e-mail account or social media profile. At least one court has allowed a claim that keystroke-logging surveillance may constitute “interception” under the Electronic Communications Privacy Act. See Brahmana v. Lembo, No. C-09-00106, 2009 WL 1424438 (N.D. Cal. May 20, 2009).


\textsuperscript{25} Many states also have antidiscrimination statutes that protect against discriminatory hiring or employment decisions. For instance, in California, the Fair Employment and Housing Act (FEHA), Gov. Code §§ 12900 -12996, includes protections for all the federally protected classes and also prohibits discrimination on the basis of several additional categories, including sexual orientation and marital status.
making a hiring or interview decision, a snubbed candidate might still bring suit alleging that the employer took into account the impermissible factors in making its decision.

If a company’s enforcement of its policies is inconsistent, it may also be subject to a claim of discrimination. For instance, in Simonetti v. Delta Airlines, a flight attendant was terminated after she posted “inappropriate” photographs of herself while wearing her company uniform.26 She filed suit for gender discrimination, alleging that the company had failed to discipline male workers who maintained similar blogs containing photographs of them wearing uniforms. Although the case was administratively terminated when Delta filed for bankruptcy, it serves as an example of the potential risks that employers may face if their policies are not consistently applied to all employees.

FEDERAL LABOR LAW

Even clear, consistently implemented social media policies may still run afoul of federal law. Section 7 of the National Labor Relations Act (NLRA)27 protects the right of employees to engage in “concerted” activities, including discourse about pay, hours, workload, or workplace safety, and other group activities. Under Section 8(a)(1), employers may not interfere with, restrain or coerce employees in their exercise of their rights under Section 7.28

Social media is especially conducive to concerted speech because it provides individuals with easy access to communication outlets that can quickly reach large audiences. Blogs that enable comments, Facebook wall posts, and on-line discussion forums allow—and often encourage—visitors to chime in with their opinions and support or debate with the original

28 Id. § 158.
poster. Those features, however, can create a formidable reputational challenge for employers. Employees who post their grievances on social networking sites and blogs are not just discussing issues with their coworkers; they are also laying their grievances for public consideration.

A social media policy is not per se impermissible under the NLRA. An employer may prohibit employees from engaging in non-protected activities, such as disloyal speech or insubordination. However, a policy may violate Section 8(a)(1) if: “(1) employees would reasonable construe the language to prohibit Section 7 activity; (2) the rule was promulgated in response to union activity, or (3) the rule has been applied to restrict the exercise of Section 7 rights.” As a rash of recent cases indicates, the NLRB has not hesitated to go after companies that regulate or take action against employee social media use.

In In re American Medical Response, the NLRB brought a complaint alleging, in relevant part, that a company’s Internet policy violated Section 7 because it prohibited employees from making any “disparaging, discriminatory or defamatory comments when discussing the Company or the employee’s superiors, co-workers and/or competitors.” American Medical Response (AMR) had terminated an employee pursuant to the policy when she posted comments on Facebook calling her boss a “scumbag” after she was refused union representation at a meeting. The complaint settled, with AMR agreeing to revise its “overly-broad rules to ensure that they do not improperly restrict employees from discussing their wages, hours and working

29 See Sears Holding (Roebucks) Advice Memorandum, N.L.R.B. General Counsel Advice Memorandum, 2009 WL 5593880, Dec. 4, 2009, available at http://www.nlrb.gov/case/18-CA-019081 (); Lee Enterprises, Inc. d/b/a Arizona Daily Star Advice Memorandum, N.L.R.B. General Counsel Advisory Memorandum, Case 28-CA-23267 (recommending dismissal of Section 7 charge where, in absence of social media policy, employee was “terminated for writing inappropriate and offensive Twitter postings that did not involve protected concerted activity.”).
30 In re Lutheran Heritage Village, 343 NLRB 646, 647 (N.L.R.B. 2004).
31 Complaint at 2, In re American Medical Response, No. 34-CA-12576 (N.L.R.B. 2010).
conditions with co-workers and others while not at work[.]”

In perhaps a more surprising case, the NLRB recently filed a complaint against a BMW car dealership in Chicago after the company fired an employee who posted photographs and critical comments regarding the quality of food and beverages at a customer appreciation event. The worker’s posting sparked an online discussion with his co-workers, complaining that the strategies could cut into their sales commissions. The NLRB alleged that the company’s decision to fire the worker violated Section 7 because it discouraged him and other workers from engaging in protected, concerted speech regarding the terms of their employment.

At the time of this writing, none of these NLRB cases have reached a decision. However, these cases and other circumstances suggest that the NLRB is taking a much broader view of what constitutes protected, concerted activity. The NLRB’s Acting General Counsel, Lafe Solomon, has added social media to the list of subjects in which he is taking particular interest, and has acknowledged that there are social media cases pending in all of the NLRB’s regional offices. And in a recent presentation to the Connecticut Bar Association, an NLRB Regional Director remarked that, with regards to social media, “It doesn’t take much to establish the concerted nature of the discussion, so long as it involve[s] or touche[s] upon a term or condition

---

34 Id.
35 National Labor Relations Board, Office of the General Counsel, Memorandum from Lafe E. Solomon Re: Mandatory Submissions to Advice 1-2 (Apr. 12, 2011), available at http://privacyblog.littler.com/uploads/file/NLRBMemorandumGC11-11.pdf (list of “[c]ases requiring a decision by the General Counsel because of the absence of precedent or because they involve identified policy priorities” includes “[c]ases involving employer rules prohibiting, or discipline of employees for engaging in, protected concerted activity using social media, such as Facebook or Twitter.”).
of employment” and “anything short of physically threatening activity will likely be protected.”37

Employers wishing to reduce the risk of litigation will need to be careful in their regulation of employees’ social media use, both in the form of social media policies and any adverse actions against employees who use social networking sites to discuss their work conditions, pay, or terms of employment. Employers must also be mindful that the NLRA’s reach may extend beyond adverse employment actions. Even giving an employee an oral admonition not to air employment grievances in a public forum may invite enforcement by the NLRB if such a warning is found to have “chilled” an employee’s right to concerted activities.38 And because Section 7 also prohibits employers from monitoring concerted activities, an employer who knowingly accesses a social media profile or posts comments on an employee’s blog may be in violation of the statute. Even making comments to an employee that gives the impression of surveillance may suffice to create liability.39 With the growing popularity of site trackers, employees are finding themselves with the means to monitor the IP addresses of visitors to their blogs and other websites. Thus, managers who conduct regular, unannounced checks of employee blogs or other websites could create an impression of surveillance that could be deemed as chilling or restraining employees’ rights to concerted activities.

37 Posting of Philip Gordon to Littler Mendelson Privacy Blog, supra note 35.
39 Konop v. Hawaiian Airlines, 302 F.3d 868, 884 (9th Cir. 2002) (“[S]urveillance tends to create fear among employees of future reprisal and thus, chills an employee’s freedom to exercise his rights under federal labor law.”) (internal citations omitted); Flexsteel Indus., Inc., 311 N.L.R.B. 257, 257 (N.L.R.B. 1993) (“[T]he test for determining whether an employer has created an impression of surveillance is whether the employee would reasonably assume from the [employer’s] statement that [the employee’s] union activities had been placed under surveillance.”).
OFF-DUTY CONDUCT LAWS

Employers in certain states must also be aware of laws that, to varying degrees, prohibit employers from taking adverse employment actions against employees who engage in lawful off-duty activities. Currently, six states offer limited protections for off-duty conduct: California, Colorado, Illinois, Massachusetts, New York, and North Dakota. For instance, New York prohibits employers from discriminating against employees who engage in off-site, off-duty “legal recreational activities” unless those activities “constitute habitually poor performance, incompetence, or misconduct” or create a “material conflict of interest related to the employer’s trade secrets, proprietary information or other proprietary or business interest.” 40 California’s Labor Code section 96(k) allows employee claims for wrongful termination, demotion, or discipline based on “lawful conduct occurring during nonworking hours away from the employer’s premises.” 41

Off-duty conduct laws, however, do not grant employees completely free rein. The laws in New York, North Dakota and Colorado allow employers to ban legal activities if they relate to a bona fide occupational requirement or are rationally related to employment activities. 42 Connecticut only protects an employee’s First Amendment speech rights, as long as off-duty speech does not interfere with the employee’s job performance or work relationships. 43 And in New York and California, the off-duty conduct laws have been given narrow application. New York’s statute, which only protects “recreational” activities, extends to games, hobbies, exercise, exercise, exercise, exercise.

40 N.Y. LABOR LAW § 201.
41 CAL. LAB. CODE § 96(k).
42 COLO. REV. STAT. ANN. § 24-34-402.5(1) (2010); N.D. CENT. CODE § 14-0.4-08 (2009). Under Colorado law, there may also be an implied duty of loyalty for an employee’s off-duty activities. See Marsh v. Delta Air Lines, 952 F.Supp. 1458 (D. Colo. 1997) (finding no violation of Colorado off-duty conduct law where employer fired worker for writing a letter to local newspaper criticizing employer’s hiring policies).
43 CONN GEN. STAT. ANN. § 31-51q (West 2003).
and reading, but does not apply to dating.\textsuperscript{44} California courts have ruled that section 96(k) does not provide substantive protections for employees but rather, a procedural remedy for asserting one’s constitutional rights.\textsuperscript{45} Because the First Amendment’s free speech protection only extends to public employers,\textsuperscript{46} private-sector employees are limited to making constitutional claims for privacy or claims under the Labor Code if their activities are otherwise protected, e.g., political activities, discussions of wages or terms of employment, and religious expression.

In the context of social media use, employers that are subject to off-duty conduct laws will need to carefully consider whether the conduct in question bears a relationship with the employee’s work performance or the employer’s interests, or if the conduct is otherwise protected. For instance, an employee who posts photographs depicting off-hours drinking may be protected from termination in New York, but may not be protected in California. In contrast, an individual who maintains a blog discussing politics may be shielded from termination in California, but may not have the same protections in New York unless the activity was considered a “recreational activity.” On the other hand, employees who disparage their employers in social media are almost certainly fair game for termination based on a violation of an implied duty of loyalty to their employers.

**FAIR CREDIT REPORTING ACT**

The Fair Credit Reporting Act (FCRA)\textsuperscript{47} imposes procedural requirements on employers who wish to use a third-party consumer reporting agency to conduct background checks or obtain credit reports of employees and job applicants. Employers must provide written notice.

\textsuperscript{47} 15 U.S.C. § 1681, et seq.
and receive consent before requesting a consumer report, and must also provide notices prior to and after taking any adverse action based on information contained in a consumer report.\footnote{FEDERAL TRADE COMMISSION, USING CONSUMER REPORTS: WHAT EMPLOYERS NEED TO KNOW (1999), \url{http://business.ftc.gov/documents/bus08-using-consumer-reports-what-employers-need-know}.}

The FCRA defines “consumer reporting agency” to include “any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports.”\footnote{15 U.S.C. § 1681a(f).} Although this definition does not appear to extend to employers who take it upon themselves to run a Google search on an employee or access a job applicant’s Facebook profile, the definition may be broad enough to reach social aggregator sites or data mining services that compile information about users through social media.

Notably, the Federal Trade Commission recently announced that social media information is considered “consumer information” for the purposes of the FCRA. After a year-long investigation, the Commission determined that Social Intelligence, a service that conducts background checks via social media, is a consumer reporting agency within the regulatory scope of the FCRA.\footnote{Social Intelligence, Corp., Fed. Trade Comm’n Letter (May 9, 2011), \url{http://www.ftc.gov/os/closings/110509socialintelligenceletter.pdf}.} In addition, several complaints have been filed in federal court and with the Federal Trade Commission against Spokeo, a company that allows its users to prepare a report of anyone identified by name, e-mail address, or phone number, by running simultaneous searches.
across more than 50 social networking sites. Those complaints allege that the company violated the FCRA by offering inaccurate data about consumers without allowing them to correct their reports. Spokeo has taken the position that it is not a consumer reporting agency and thus, is not subject to the FCRA. At the time of this writing, none of the cases has reached a decision, although at least one FCRA claim brought against Spokeo has survived a motion to dismiss on the issue of whether the company is a consumer reporting agency.

CONSTITUTIONAL PROTECTIONS

Public-sector employers should be mindful of constitutional limitations on how much they can regulate employee social media use. Although public sector employees do not have an absolute right to free speech in their employment, they do enjoy some limited First Amendment protections. Courts employ a balancing test that weighs the interests of the employee, as a citizen, in commenting upon matters of public concern and the interest of the government, as an employer, in promoting the efficiency of the public services it performs. The Supreme Court has held that a “matter of public concern” includes speech “relating to any matter of political, social, or other concern to the community” but not statements about office policies, office morale, or employment characterizations. Thus, for instance, public-sector employers may be limited in their ability to terminate employees who maintain blogs or participate in on-line discussions regarding government policies, politics, social issues in the community, and other matters of public concerns. However, employers may still take action against employees who air

internal office grievances that have no relevance or concern to the community or post inappropriate photographs on social networking sites.

The Fourth Amendment’s prohibition of unreasonable searches and seizures may also apply to employer electronic surveillance, although such cases in the social media context are likely to be rare. The core inquiry driving the Fourth Amendment’s privacy protections is whether the employee had a reasonable expectation of privacy. Because much of what appears on social networking sites has been purposely shared with the public, an employee would be hard-pressed to argue that he or she had a reasonable expectation in privacy – absent, of course, an employer’s unauthorized access into secret, non-public information. To minimize risk, employers would be well advised to avoid such unauthorized access, which could also incur liability under the ECPA and SCA, as well as any applicable state laws. Employers who engage in workplace monitoring of employee social media use may further reduce liability by being transparent about monitoring activities, thus cutting off any expectation of privacy.

NEW TECHNOLOGIES

One of the key concerns involving social media is the Internet’s long, unforgiving memory. Once posted on the web, information does not disappear easily. Facebook photographs may be tagged, downloaded, and forwarded – and even when “deleted,” they may

---

55 Id.
58 See Katz v. United States, 389 U.S. 347, 351 (1967) (“What a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection.”).
59 See, e.g., Biby v. Bd. Of Regents of Univ. of Nebraska, 419 F.3d 845 (8th Cir. 2005) (finding no reasonable expectation of privacy where employer’s computer policy stated that employee computer files were subject to search in connection with litigation discovery requests).
still remain accessible through backup copies that linger on Facebook’s servers indefinitely.\textsuperscript{60} An impulsive or drunken tweet is not only sent out to a user’s Twitter subscriber list but also memorialized in the Library of Congress’s archives.\textsuperscript{61} Profiles that have long since been deleted may have already yielded information to data mining services that purchase consumer information or crawl the web in search of publicly-available information.\textsuperscript{62} Websites that have been taken down may continue to survive in Internet infamy. The Wayback Machine has archived more than 85 billion webpages comprising approximately 2 million gigabytes of data, and their archives expand at a rate of 20 terabytes per month.\textsuperscript{63} The Google cache and other web search engine caches often retain snapshots of webpages that persist for weeks and even months even after they have been modified or removed.\textsuperscript{64}

As society struggles to deal with the explosive growth of social media and the Internet’s irrepressibly long memory, many new technologies propose to help Internet users manage their digital footprints.\textsuperscript{65} Reputation scrubbing services, such as Reputation.com, will, for a fee, search the web to identify and remove negative information about their clients, while using search-optimization strategies to push positive or neutral information to the top of search results.\textsuperscript{66} Social media expiration dates enable users to set expiration dates after which

\begin{footnotesize}
\begin{itemize}
  \item[66] Id.
\end{itemize}
\end{footnotesize}
information self-destructs. Site trackers allow bloggers to track the IP addresses and locations of visitors to their webpages, enabling users to sniff out those who may be snooping on them. New websites and software enable users to see what services are tracking their information and modify their privacy settings accordingly. Combined with enhanced privacy and security settings, these technologies may make it more difficult for employers, and others, to track the social media activities of their workers.

For employers, these new technologies can have both positive and negative implications. Reputation scrubbers, enhanced privacy settings, encryption software, and expiration dates may mitigate a poor on-line reputation, or reduce a user’s digital footprint, which could be useful to an employer seeking to ensure that their workers present positive or neutral web profiles or minimize fallout from negative publicity on the Internet. However, these technologies may also make it harder for employers to monitor their workers or screen new hires. Employees tracking social media may find themselves coming up with only limited information within public view. Employees may take advantage of reputation promoting services to present a rosier picture than the truth may warrant.

In addition, these new technologies are not infallible. Much information is almost impossible to erase, as e-mails get forwarded, photographs and videos are downloaded onto local hard drives, and stories are republished in new media outlets. Additionally, data mining services and other information aggregators may crawl the web, using public records, digital archives, and

---

67 Id.
data purchased from social media platforms to compile profiles of Internet users.70 Because data mining services may access and record information as soon as it is posted, data may continue to survive on their servers long after the original content has been removed. However, these “workaround” solutions may pose their own challenges. The mining process makes innumerable assumptions about consumer behavior and may compound errors and assumptions through successive iterations, much like a digital version of the “Telephone Game.” For instance, these services may yield misleading or erroneous information when individuals purchase gifts for friends, use other people’s computers, share the same name as others, live at the same address as others, or visit sites by accident.71 Employers who resort to such services may end up with results that are incomplete, outdated, or plain incorrect.

DEVELOPING A SOCIAL MEDIA POLICY

According to a 2010 survey conducted by the Pew Research Center, only 27% of employed Internet users work for an employer who has a social media policy in place.72 Companies need to understand that implementing a social media policy is an important first step in managing risk and promoting business goals. A clear social media policy should provide employees with notice of a company’s monitoring practices and educating both managers and workers about the need for informed and responsible usage of the social media platforms.

THE SCOPE OF A SOCIAL MEDIA POLICY

A fundamental challenge in developing a social media policy is defining the scope of

70 Joel Stein, Data Mining: How Companies Now Know Everything About You, TIME, Mar. 10, 2011, available at http://www.time.com/time/business/article/0,8599,2058114,00.html (recounting personal experiences with various data mining services and noting that a significant amount of the information was inaccurate).
71 Id.
covered activities. Social networking sites such as Facebook, MySpace, and LinkedIn only form part of the Web 2.0 universe. As people spend more time on the web and Internet companies become increasingly interconnected, “social media” now embraces a much broader range of activities. For instance, Facebook Connect strives to create coherent on-line identities by enabling users to take their Facebook profile information, friends, and privacy preferences to other participating sites.73 Users who visit other sites may find their activities are tracked back to their Facebook status and news feeds. Online retailers like Amazon.com encourage consumers to publicize their reading lists, post recommendations, and share opinions regarding a broad range of products and services.74 Feedback and rating systems on sites like Netflix and eBay.com can reveal information about individuals’ consumption habits, even when the sites attempt to anonymize the data.75

Employers and employees should understand that as social media use continues to grow, managing one’s on-line reputation will necessarily extend beyond the information that an individual creates or shares on a social networking site. Even a person who is careful about what information she posts and assiduously manages her privacy settings may still need take additional steps to search out and address information that may have been posted or collected by other individuals and sites.

75 For instance, when Netflix released 100 million “anonymous” movie ratings submitted by 500,000 users during the 1999 to 2005 period, researchers were quickly able to identify people in the database by name, based on public data posted on other movie ratings websites. See ARVIND NARAYANAN AND VITALY SHMATIKOV, ROBUST DE-ANONYMIZATION OF LARGE SPARSE DATASETS (2008), available at http://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf.
PROMOTING AWARENESS

Even as social media users, as a whole, become more cognizant of privacy concerns, a large percentage of Internet users are unaware of or uninterested in the ramifications of their online activities. A 2009 Deloitte study, for instance, showed that 27% of surveyed employees do not consider the ethical consequences of posting comments, photographs, or videos online. Most individuals do little or nothing to monitor their digital footprints. Another 2009 study conducted by Pew shows that only 2% of those surveyed regularly look up information about themselves on the web, and 19% do so “every once in a while.” Moreover, low rates of self-searching correlate with high percentages of individuals who are not aware of the information posted about them on the Internet or state that they are not concerned about what information is available about them.

A social media policy that encourages employees to conduct themselves in a mature, responsible, and self-aware manner may help push workers to think about managing their digital presence. Although many, if not most, users create content with the clear purpose of sharing their message with the world, others may not know that their actions and behaviors could potentially end up immortalized in a public forum. The dissemination of Representative Anthony Weiner’s explicit text messages and private photographs is only one recent example of how social media use can inadvertently end up under public scrutiny. Throughout the years, employees have been terminated or forced out of their jobs for emails, photographs, and videos

76 DELOITTE, LLP, ETHICS AND WORKPLACE SURVEY, supra note 14.
77 MADDEN & SMITH, HOW PEOPLE MONITOR THEIR IDENTITY AND SEARCH FOR OTHERS ONLINE, supra note 72.
they never thought would see the light of day.\footnote{See, e.g., \textit{TV Anchor Resigns Over Wet T-Shirt Video}, ABC \textsc{Good Morning America}, Jan. 20, 2005, http://abcnews.go.com/GMA/story?id=128067&page=1; Dan Abramson, \textit{The Funniest Facebook Snaus of All Time (Pictures)}, \textsc{Huffington Post}, Jul. 26, 2010, http://www.huffingtonpost.com/2009/12/08/the-funniest-facebook-sna_n_383847.html#s55536&title=A_New_Problem.} And with facial recognition technologies reaching new levels of sophistication, even individuals who diligently remove photographs of themselves from their social networking profiles may still end up tagged for activities that they may not want disseminated to the on-line public.\footnote{Facebook Photo Tagging: Cool or Creepy?, Posting to Reuters Wealth Blog, http://blogs.reuters.com/reuters-wealth/2011/06/14/facebook-photo-tagging-cool-or-creepy (June 14, 2011).} Employees who understand that their employer has a social media policy in place may think twice before posting unsavory pictures or comments that gratuitously disparage their employers or coworkers, and may take more proactive steps to manage their online reputations.

To reduce risk exposure, employers should also be aware that any attempts at secret surveillance may fail. Social networking sites may provide their users with information about all visitors who have accessed their profiles or visited their blogs. Even sites that do not provide end users with visitor tracking information may retain internal records which could be produced during litigation discovery. A policy of surreptitious monitoring may end up backfiring, especially if employers seek to take action against employees for activities that have been secretly monitored.

**AVOIDING ILLEGAL PRACTICES**

An effective social media policy must also advise management and workers alike not to engage in unlawful uses of social media. For some employers, it may be extremely important to rein in the monitoring activities of overzealous supervisors or human resources staff. Companies should also tread carefully when researching job candidates through social media. Although employers may use social networking sites to glean information about unprofessionalism,
inappropriate behavior or character, they may also discover information about an applicant’s membership in a protected class. Employers should consider separating the tasks of researching a candidate and making the hiring decision among two or more individuals, or relying on a third party to prepare a report that only contains relevant information for a job position, while filtering out unnecessary personal information. Employers should be advised, however, that using a third party agency will likely require employers to comply with the notice and consent requirements of the Fair Credit Reporting Act. Notwithstanding the current lack of precedent, employers seeking to minimize exposure to litigation should observe the requirements of FCRA if they use data mining services or a social aggregator site.81

GETTING THE OTHER SIDE OF THE STORY

Employers should also recognize that they cannot trust all or even much of the information on the Internet.82 Data mining services may rely on incorrect data or baseless assumptions, similar names may yield false positives, and even facial recognition software is not infallible. Especially during pre-hiring screening, employers may come across information that is inaccurate or incomplete. Acting on this information without allowing the individual to address the issue or failing to treat the matter with the appropriate confidentiality, could create liability under defamation or invasion of privacy law.83

81 Although no cases have yet addressed this argument, screening a candidate via a professional networking site such as LinkedIn may also help companies avoid litigation risk. Because those sites serve a primarily professional, rather than social, purpose, employers may be able to argue that the available information is fair game for consideration in employment decisions, much like one’s résumé and cover letter.

82 For instance, 51% of Internet users say that only a small portion or none of the information on social networking sites is reliable and accurate. See 2010 DIGITAL FUTURE REPORT, supra note 5.

83 Allow applicants to answer negative background-check results, BUSINESS MANAGEMENT DAILY, Aug. 1, 2003, available at http://www.businessmanagementdaily.com/articles/2649/1/Allow-applicants-to-answer-negative-background-check-results/Page1.html# (job applicant successfully stated claims for defamation and false light invasion of privacy after hotel acted on erroneous background check results by denying him employment and telling others that he was an ex-convict).
An employer should also consider giving a warning before taking adverse employment actions. Depending on the seriousness of an employee’s social media indiscretion, an employer may find it more expedient to ask the individual to remove the offending information rather than to take steps that might generate negative publicity or invite expensive litigation.

IDENTIFYING BUSINESS GOALS

Employers looking to harness the power of social media can encourage employees to get more involved in social networking efforts that increase appreciation and awareness of the productive uses of social media. Employers can establish a Facebook or MySpace presence, ask that employees maintain a professional LinkedIn profile, or maintain a company blog where employees take turns writing posts. Some companies, for example, have encouraged employees to maintain blogs to publicize new product releases, solicit input from customers, or share and gather other information with the Internet public.84

Even an employer who may have limited use for viral marketing or social media branding may find it helpful to offer social media assistance to its employees. Allowing employees to consult with management may help clarify gray areas and promote responsible social media use. For instance, a company may offer guidance to employees who have questions about setting up a professional networking profile or whether it is permissible to post certain information on a personal blog. Employers may also wish to educate employees on how to manage their on-line reputations. Employees who are more diligent in managing their profiles will have greater impetus to closely monitor their privacy settings, de-tag or remove inappropriate photographs, refrain from making disparaging or disrespectful on-line comments, and engage in other self-

---

policing efforts that will benefit both employers and employees.

SEPARATING BUSINESS USE FROM PERSONAL USE

Much social media use will fall outside the scope of employment. Employers considering the myriad risks that arise from social media use may contemplate an outright ban, but that approach would almost certainly violate the NLRA and, for some employers, statutory or constitutional protections of free expression or legal, off-duty conduct.85

Instead, employers should encourage responsible social media use that is separate and distinct from the employee’s professional identity. An employer should require employees with social networking profiles to register using their personal e-mail addresses, and bar employees from using company logos or trademarks without permission. Employees who maintain blogs should be required to include disclaimers stating that their statements do not reflect the company’s views or opinions. And even if they are blogging or using social networking sites for their own social purposes, employees should be instructed to conduct themselves in a respectful, dignified manner and avoid illegal, disloyal, or insubordinate behavior.

A social media policy may not make blanket prohibitions that could be construed as chilling concerted activities. A good policy, however, can and should identify and prohibit speech that is not protected under federal labor law, such as disparaging an employer, coworkers, or competitors without relation to pay, work conditions, or terms of employment, publication of a company’s trade secrets, public disclosures in violation of federal securities law, and malicious, 85 From a business perspective, outright prohibitions on employees’ social media activities may also encourage the growth of anonymous blogs, breed resentment, or adversely impact employee morale. See Aaron Kirkland, Note, “You Got Fired? On Your Day Off?!: Challenging Termination of Employees for Personal Blogging Practices, 75 UMKC L. Rev. 545, 564 (2006).
defamatory remarks. To further reduce an employer’s risk exposure, a social media policy may also include a disclaimer clarifying that it does not apply to protected activities, such as discussions of one’s pay, work conditions, or terms of employment.

ENCOURAGING ALTERNATE CHANNELS OF COMMUNICATION

Employers may also wish to encourage employees to use alternative means to communicate with their coworkers about work conditions, such as websites with restricted access, e-mail lists, or private on-line discussion groups. Although an employer cannot require employers to use these “private” channels of communication, enabling or encouraging their use may limit the amount of “negative” information that appears in full public view on the Internet. If employees resort to these alternatives, employers should not attempt to monitor or unlawfully access those communications lest they face liability under federal and state privacy laws.

IMPLEMENTING A POLICY

Even the best-laid plans will fail if not properly implemented. A social media policy that appears in a company handbook may go unread and unheeded if a company does nothing to promote the policy. Companies should provide management and human resources staff with periodic training sessions to ensure that they understand their company policies and limitations

87 See, e.g., Posting of Philip Gordon to Littler Mendelson Privacy Blog, supra note 35. (“The [NLRB] Hartford Region will consider a disclaimer when evaluating whether an employer’s social media policy violates the NLRA . . . . [T]he disclaimer should become more specific as the policy becomes broader and more general. For policies that are narrow and easily understood, a disclaimer that the policy is not intended to violate the NLRA may suffice. For broader policies . . . the Region will require a disclaimer which states either that the rule does not apply to discussions or activities involving your terms and conditions of employer or that the policy does not apply to discussions and activities involving your wages, hours and working conditions.”) (internal quotations omitted).
88 According to a 2009 study, 23% of surveyed employees stated that their employer had no social media policy, 11% stated that their employer had a policy but the respondent did not know what the policy was; and 24% did not even know whether their employer had a social media policy at all. DELOITTE, ETHICS AND WORKPLACE SURVEY, supra note 14.
on monitoring and regulating employee social media use. Employees should, at the very least, be required to review and sign their employer’s social media policy acknowledging that they have reviewed and understand it. Going one step further, employers can offer an orientation or periodic training sessions for workers and encourage them to seek assistance from management or human resources if they need help setting up professional web profiles, have concerns about their on-line reputations, would like to develop a blog, or use company logos or work-related information in a blog or posting.

Moreover, enforcement of a social media policy must be consistent. In practice, this may be difficult for many employers, who may have no reason to monitor social media until an incident arises. Employers who don’t have a uniform policy may find themselves taking action when they receive complaints from customers or a supervisor accidentally stumbles upon an inappropriate photograph, disparaging comments, or other unsavory information. Nevertheless, employers must be aware that making exceptions for certain employees or having enforcement that is inconsistent across the company may set the stage for a discrimination complaint.

Employers should also be mindful that a social media policy that exists only in name may also lead to potential liability. Under common law tort theories, employers have a duty to supervise their employees to curtail harm to third-parties. If an employer has an express policy of monitoring employee’s social media usage or investigating candidates through social networking sites but then fails to do so, that employer may be liable to third parties for negligent hiring or failure to investigate claims.\(^89\)

\(^89\) C.f. Doe v. XYZ Corp., 887 A.2d 1156 (N.J. Super. Ct. App. Div. 2005) (allowing a complaint that alleged that employer failed to take steps action to investigate an employee’s pornographic Internet activity, which would have revealed employee’s sexual exploitation of his stepdaughter).
CONCLUSION

As the law struggles to keep up with the explosive growth of new social media technologies, the ever changing legal and technological landscape will continue to create new issues for employers. Information sharing on the web has reshaped our expectations of privacy. Privacy advocates are pushing for stronger electronic privacy protections and expanded off-duty conduct laws.\footnote{See, e.g., Bianca Bloster, Law to Make Social Networks Private By Default Worries Facebook, THE HUFFINGTON POST, May 16, 2011, http://www.huffingtonpost.com/2011/05/16/sb242-privacy-law-california_n_862381.html.} The NLRB is taking a broad view of concerted activities that encompasses social networking sites. And new technologies may make it easier for employees to manage, modify, and even erase their digital footprints.

Employers cannot afford to sit at the sidelines in the face of all of these changes. Developing a social media policy is a critical component of successfully navigating the challenges posed by social media. By promoting awareness and taking steps to educate employees on responsible social media use, employers can harness the benefits of social media while managing and reducing risk.