Labor & Employment: Social Media in Focus

Issues With Self-Destructing Messages In the Workplace

BY PETER ISAJIW AND JOHN VAZQUEZ

Inside many businesses, emails and electronic communications are the primary—and sometimes only—way people communicate. As one federal judge noted, email has not only replaced paper memos and letters, but "many informal messages that were previously relayed by telephone or at the water cooler are now sent via email."[1]

But the convenience of electronic communication comes with some costs: Email's persistence and ease of duplication mean that once a message has been sent, the author loses all control over it. Emails can be easily distributed well beyond their intended audience, and often reemerge to the detriment of the sender in litigation or other disputes. Snapchat, an app that allows users to send picture and video messages that "self-destruct" after viewing, has achieved a $2 billion valuation by offering at least a partial solution to these problems. Encouraged by Snapchat's success, several recently launched apps aim to bring "self-destructing" messages to a more business-minded user demographic.

For example, an app called TigerText markets itself as an enterprise solution for complying with health care confidentiality and other privacy regulations, while promoters of the app Confide describe it as the "Snapchat of the C-suite." The need for confidential communication regarding sensitive business issues is common among busy executives and professionals, but trying to coordinate schedules for phone calls or other real-time meetings can be challenging, and in today's globalized marketplace this difficulty is often compounded by differences of time zone and geography. At the same time, the ubiquity of mobile devices and our "always-on" culture cause people to be less tolerant of communication delays. But despite the inconvenience and lost productivity involved in arranging real-time talks, it is wise to be cautious about discussing sensitive topics by email because of the risk such communications might find their way into the possession of a litigation adversary, competitor, or other hostile party. The ability to send secure messages that cannot be saved, stored, or forwarded could foster productivity by encouraging frank and timely communications, freeing people from both the need to coordinate real-time conversations and the fear that messages will fall into unwanted hands. As the draw of self-destructing messaging apps for busy professionals is likely to be strong, firms and their legal advisors need to be proactive in contemplating how such apps might be used in the workplace.

> The convenience of electronic communication comes with some costs: Email's persistence and ease of duplication mean that **once a message has been sent, the author loses all control over it.**

These apps raise a number of potential compliance and legal concerns. The fundamental problem with these self-destructing message systems is that users may view communications sent through them as unrecorded, similar to a phone call or face-to-face talk, but this perception is not correct. A communication that is quickly or automatically deleted is not the same as one that was never recorded. Sending communications through a system that makes deletion automatic (and perhaps irreversible) is not likely to excuse noncompliance with any legal or ethical obligation to preserve documents. Lawyers and compliance professionals will need to be vigilant to ensure that corporate personnel are not inadvertently violating document retention obligations by using these services, thereby exposing themselves or their employers to sanctions.

One potential concern is the use of these apps by companies in regulated industries, such as financial services firms, companies subject to Sarbanes-Oxley, or health care organizations, where their use may violate regulatory record retention obligations. For example, regulated financial entities are required to retain broad categories of internal and external communications, including electronic communications, and regulators have been aggressive in enforcing these requirements. In December 2013, the Financial Industry Regulatory Authority (FINRA) fined one member bank $3.75 million for failing to maintain emails, » Page 12

PETER ISAJIW *is a partner, and* JOHN VAZQUEZ *is an associate, at Cadwalader, Wickersham & Taft.*

BIGSTOCK

Achieving a Work Environment Free Of Cyber Bullying

BY MARA B. LEVIN

Last year's alleged bullying, via voicemails and text messages, of Miami Dolphins player Jonathan Martin by his teammate Richie Incognito, which caused Martin to leave the team, sparked a controversial debate over the fact that workplace bullying is not illegal under federal or state law.

A 2011 Monster Global Poll asked workers, "Have you ever been bullied at work?" Sixty-four percent of the 16,517 respondents answered that they had been bullied, physically hurt, driven to tears, or had their work performance affected, and 16 percent had witnessed a co-worker being bullied. In another 2011 study by the Society for Human Resource Management, incidents of workplace bullying occurred in more than 50 percent of companies, yet only 43 percent of companies reported having an "anti-bullying" policy in their employee manual.

Since 2003, 25 states have considered legislation and, at last count, 11 states have active bills promoting a healthy workplace environment. Yet, no state has passed legislation creating a private cause of action against an employer by an employee who is subjected to workplace bullying. The Incognito episode may prove to be the tipping point where enough public support is garnered to reverse the trend.

Bullying behavior can present in a number of ways, from face-to-face or telephone confrontation, to more passive email and text messaging bullying, to more aggressive cyber bullying conducted via Facebook posts, Twitter tweets, and blogs. In order to understand the colloquial terms "bullying" and "cyber bullying," which afford *no* statutory protections to those victimized in the workplace, one must understand the type of harassment that *is* legally prohibited in the workplace.

Currently, under federal law, employees are protected if subjected to a "hostile working environment" that is motivated by their perceived or actual race, color, religion, sex, national origin, disability, genetic information or age.[1] Various state and city laws may also protect employees against hostility aimed at, among other things, marital status, political affiliation, sexual preference, sexual orientation or gender identity.

Generally, in order to prevail on a hostile working environment claim, an employee needs to establish that the harassing conduct, regardless of the way it was communicated, was unwelcome, aimed at the victim's protected status, subjectively abusive to the employee, and "sufficiently severe or pervasive to alter the conditions of the [victim's] employment."[2] Whether the harassing conduct is considered severe or pervasive so as to be actionable is determined on a case-by-case basis, with consideration often paid to the following factors, none of which alone is dispositive:

> **No state** has passed legislation creating a **private cause of action** against an employer by an employee who is subjected to workplace bullying.

- the frequency and severity of the unwelcome conduct;
- whether the conduct was physically threatening or humiliating, or a mere offensive utterance;
- whether the conduct unreasonably interfered with work performance;
- the effect on the employee's psychological well-being; and
- whether the alleged harasser was a superior within the organization.[3]

In evaluating whether conduct that does not result in a tangible job detriment (i.e., failing to hire, termination, failing to promote, reassignment with significantly different responsibilities, or a significant change in benefits or compensation) is nevertheless actionable, the U.S. Supreme Court has specifically noted that "simple teasing, offhand comments, and isolated incidents (unless extremely serious)" are insufficient to constitute severe and pervasive. Statutes protecting employees from hostile working environments are not meant to be "a general civility code" and, when applied as intended, should not elevate a complaint involving "the ordinary tribulations of the workplace, such as the sporadic use of abusive language … and occasional teasing" to unlawful harassment.[4] » Page 12

MARA B. LEVIN *is a partner at Herrick, Feinstein, where she is co-chair of the employment practices group.*

Developing Social Media Policies That Survive NLRB Scrutiny

BY ERIC RAPHAN, JONATHAN STOLER AND SEAN J. KIRBY

Over the past few years, the National Labor Relations Board (NLRB or the Board) has taken an active role in attempting to shape (i) employer social media policies and (ii) employer use of social media in making employment related decisions.

This trend is likely to continue. In fact, in a January 2014 interview with Law360, the Chairman of the NLRB, Mark Pearce, and Board Member, Philip A. Miscimarra, explained that the NLRB intends to continue focusing on social media cases, and even noted that the Board's social media caseload has increased its public profile.[1] Given the NLRB's general stance on these issues, recent NLRB decisions, and the NLRB's stated intention to continue focusing on such cases, employers must take steps to ensure that their social media policies will pass NLRB scrutiny, while still protecting themselves in situations where an employee has posted unfavorable comments about the employer on social media.

Social Media Policies

Over the past few years, the NLRB has issued three separate reports in which it provided guidance to employers regarding social media policies. In the most recent report, the Board examined the social media policies of a number of different employers.[2] In a number of these cases, the Board's General Counsel's office found that certain provisions of the social media policies at issue were unlawful under §8(a)(1) of the National Labor Relations Act (NLRA) because they interfered with an employee's right to engage in protected, concerted activity under §7 of the NLRA.[3] In reaching these decisions, the NLRB applied a two-part analysis to determine if a social media policy violated the NLRA. First, the Board reviewed the social media policy to determine if it explicitly restricted §7 protected activities. If the policy contained such explicit restrictions, it was unlawful on its face. If the social media policy did not explicitly restrict §7 protected activities, the Board then analyzed whether (i) employees would reasonably construe the language in the policy to prohibit §7 activity; (ii) the policy was enacted in response to union activity; or (iii) the policy was applied to restrict the exercise of §7 rights.[4] If the answer to any of these questions was yes, then the policy was unlawful under the NLRA. In addition to setting forth the foregoing analysis, the Board also issued a sample social media policy for employer reference.[5]

Applying the » Page 13

ERIC RAPHAN *and* JONATHAN STOLER *are partners, and* SEAN J. KIRBY *is an associate, at Sheppard, Mullin, Richter & Hampton in New York.*

Inside

Beware the **Risks** of Using Social Media During **Recruitment**

BIGSTOCK

BY MARIANNE MONROY

With a few strokes of the keyboard or taps on the iPad, employers seemingly have a wealth of free and easily accessible information up for grabs to scout for new talent and recruits, and weed out less desirable applicants from the stack of resumes on their desks.

Employers may also seemingly have justification in firing an employee whose social media content impugns the reputation of the business, demeans or threatens staff, or divulges confidential business information. However, what may seem to be an appropriate use of publicly available information is not without legal implications and risks.

Employee Recruitment

Although there are no laws that prohibit the use of social media to screen or recruit applicants, conducting pre-hire social medial background checks may expose employers to potential "failure to hire" discrimination claims.

While the employer may be innocently looking at social media content to ascertain the candidate's prior work experience, education and skills, the employer may also obtain personal information about the candidate that legally cannot, and should not, be factored into the hiring process. For example, by accessing a job candidate's LinkedIn profile, an employer may obtain a photo identifying the candidate's race or ethnicity, and a similar search of the candidate's Facebook account may identify the candidate's religion, sexual orientation or perhaps a disability.

> While the employer may be **innocently looking** at social media content to ascertain the candidate's prior work experience, education and skills, the employer may also obtain personal information about the candidate that **legally cannot, and should not**, be factored into the hiring process.

Yet, it is unrealistic to entirely ignore the value of social media with regard to recruitment efforts. Just as job seekers use social media to look for positions and market themselves, employers should be able to use social media in a legally responsible manner. However, to harness the value of social media in recruitment efforts, while at the same time minimize the risk of discrimination or privacy claims, employers would be well served by taking the initial steps of: (i) adopting appropriate social media policies with regard to recruitment; (ii) preparing written detailed job descriptions; (iii) designating and training personnel to conduct social media background checks consistent with policy and law; and (iv) uniformly applying the policy.

Review and Expand Social Media Policies to Cover Recruitment Efforts. It has become fairly commonplace for employers to have social media policies governing usage by existing employees. Historically, employers were generally free to implement broad policies restricting employees from using social media sites such as Facebook, MySpace, Twitter and the like to disparage the company, product or services, demean staff, or even disclose what was traditionally considered "confidential" salary information. However, since 2011, the National Labor Relations Act (NLRA), which protects union and non-union employees' right to engage in "concerted activity" (including the right to discuss the terms and conditions of their employment), has been interpreted to prohibit employers from imposing such broad restrictions on an employee's usage of social media, which may discourage employees from organizing or negotiating terms of employment. See 29 U.S.C. §157; NLRB and Social Media, National Labor Relations Board Fact Sheet, available at http://www.nlrb.gov/news-outreach/fact-sheets/nlrb-and-social-media.

While employers can no longer impose sweeping restrictions, narrowly tailored social media policies remain a critical management tool. Among other things, social media policies remain an effective tool to minimize, and defend against, employee privacy and First Amendment claims, when such a policy clearly places employees on notice that their Internet, email and computer usage on company issued equipment may be accessed, read and monitored. Policies that restrict employees from using social media to unlawfully harass, intimidate or threaten staff, vendors and clients also remain critical to protecting the work environment and promoting an employer's zero-tolerance policy against acts of discrimination and workplace violence.

Employers who use social media to recruit or screen job applicants should make clear that their social media policy covers the pre-employment hiring process, and that it is not limited to setting forth the dos and don'ts of social media usage by existing employees. With regard to provisions of the policy that cover recruitment, ideally employers should consider implementing a process that involves conducting a social media background check after a conditional offer of employment has been extended and consent obtained from the applicant. This is similar to the approach taken by employers who extend a conditional offer of employment, subject to a criminal background check. By first extending the conditional offer, should the employer later uncover information in the criminal or social media background check that appropriately warrants revocation of the offer, it diminishes the applicant's ability to establish that they were denied employment due to race or other protected characteristics, which would have been known by the employer when he or she initially made the job offer.

Further, just as employees are given an opportunity to refute false information that may come up in a criminal background check or explain why any such record has no bearing on their ability to perform the job, applicants should arguably have a similar opportunity to confront and explain social media content that has been relied upon by the hiring decision-maker, which may be false or otherwise unreliable.

Employers should be wary about implementing policies and procedures demanding applicants to provide them access to "blocked" or password-restricted information. Job seekers are now more cognizant that employers may be trolling the Internet for information that they do not necessarily want a prospective employer to see, and they may limit access to select viewers (e.g., a person with a Facebook account may allow access to those individuals he or she formally accepts or acknowledges as a "friend") and block information to the general public. Several states, such as Arkansas, California, Colorado, New Jersey, Nevada, New Mexico, Oregon, Utah, Vermont, and Washington, specifically restrict employers from demanding an applicant or employee to provide password or login information to gain access to their social media accounts. See Society for Human Resources Management, Social Media Privacy, November 2013, available at http://www.shrm.org/legalissues/stateandlocalresources/stateandlocalregulations/documents/socialmediaprivacy.pdf. Although New York does not have such a law currently, similar legislation has been previously introduced in the state senate. See S. 1701, 2103 Leg., 236th Sess. (N.Y. 2013) Employers should also refrain from bypassing security settings and surreptitiously gaining access with a fake identity or other end-run means (e.g., an employer asking someone who may have access to the applicant's non-public social media content to feed them the blocked information). The Federal Stored Communications Act, 18 U.S.C. §2701, makes it an offense to intentionally access stored communications without authorization or in excess of authorization.

Drafting Written Job Descriptions. To supplement policies relating to recruiting and equal employment opportunities, it is important for employers to have detailed and standardized job descriptions, which specify the requirements and essential functions for all job positions. Thus, if a background check of an applicant's education, credentials, or social media profile reveals that the applicant does not meet the express criteria of the job description, the applicant will be hard-pressed to claim that he or she was not hired because of race, age, disability or other discriminatory reasons.

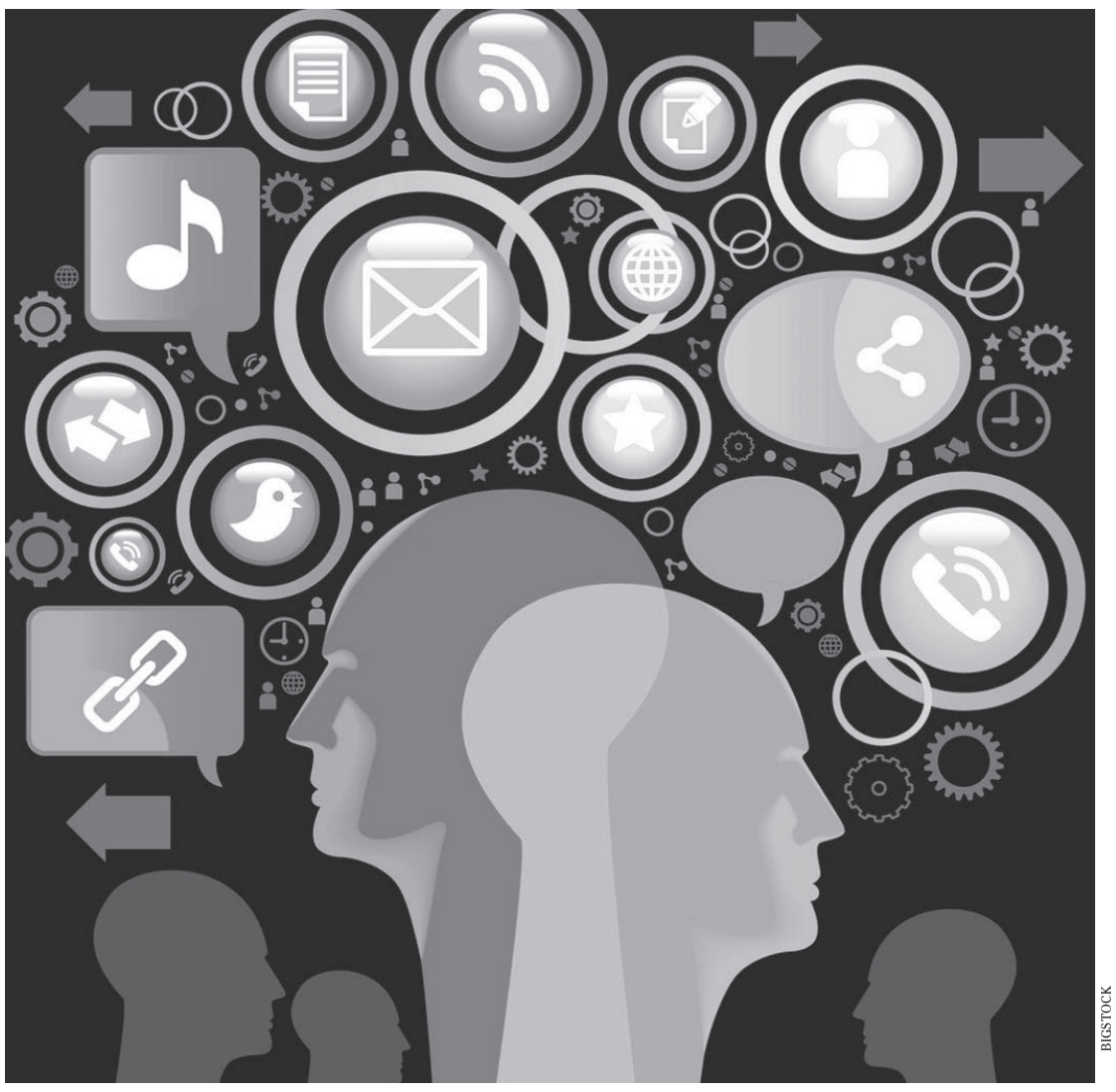
Designating Appropriate Personnel to Implement Policy. An employer may also be wise to designate a specific person—who is not involved with interviewing or making hiring decisions—to conduct the social media background check and report to the decision maker only information relevant to the position being sought. In other words, have a designated employee scrub from the social media background check any information that may not lawfully be considered by the decision maker, including the applicant's race, religion, disability, age, etc. Of course, this method assumes an honor system and that such impermissible information will not be leaked to the decision maker. Alternatively, employers may engage a third-party vendor to conduct the social media background search and scrub the information before reporting it to the employer, which is commonly done for purposes of running criminal or credit history background checks on applicants. As criminal and credit history reports conducted by third parties are viewed as consumer reports, a report of an applicant's social media history prepared by a vendor may be also be deemed a consumer report. And, as a consumer report, an employer would need to first obtain an applicant's consent to have the vendor conduct the social media background check to avoid running afoul of the

» Page 13

MARIANNE MONROY *is a partner at Garfunkel Wild and is co-chair of the firm's employment law practice group.*

Social Media: **Changing** the Face of **Employment Law**

BY LOIS CARTER SCHLISSEL



BIGSTOCK

Before social media changed the world, employers hired employees based on a one-page resume, some perfunctory references and an interview. After the employee was hired, most of the scuttlebutt around the office was shared in chatter at the water cooler, usually out of the earshot of a supervisor and thus, no harm no foul.

With the advent of social media, every aspect of a person's life in and out of the workplace is fair game for employers and anyone else who cares to look. Management can find out what employees think about the company, as can everyone else, including the customers the employer hopes to service. The power of communication through the use of social media is unmistakable and unstoppable. But with great power comes great responsibility—for employees and their employers.

Legal issues involving the use (and misuse) of social media are now coming before the courts for resolution. Management as well as employees need to know what they can and cannot do to avoid finding themselves embroiled in litigation or terminated from their jobs with little recourse. These issues include whether an employer can use information found on a job applicant's social media sites in considering whether to hire that candidate; whether an employer can force an employee or job applicant to provide passwords to access his/her Facebook page; whether an employee or prospective employee has any privacy rights in connection with information he/she posts on the web; whether an employee is protected when he/she posts something on social media that an employer finds unacceptable; and whether the employer can be liable for its employees' postings.

Pre-Hiring

Questions about religion, political affiliation and marital status are known to be off limits during the interview of a candidate for employment. Employers do not even want to receive a picture of a candidate for employment as it could lead to claims that the candidate's age or race played a role in the employment decision. Yet, with a world of information at the employer's fingertips at the touch of a key, some employers feel it would almost be an abdication of responsibility not to study a candidate's online presence before making the hiring decision.

Recognizing that users' postings—public and private—provide potentially useful information in assessing applicants for employment, a new name has been given to the practice: "cyber screening." According to Career Builders, 65 percent of employers surveyed said they research candidates to see if the job seeker presents themselves professionally. Fifty-one percent want to know if the candidate is a good fit for the company culture, and another 45 percent want to learn more about his/her qualifications. A third (34 percent) of employers who scan social media profiles said they have found content that has caused them not to hire the candidate and about half of those employers said they did not offer a job candidate the position because of provocative or inappropriate photos and information posted on his/her profile.[1]

Two issues are raised by "cyber screening." The first is will employers subject themselves to liability by simply gathering information such as a person's race or marital status from the candidate's public profile? The simple answer is: Possibly. If the employer actually has a written policy that it will engage in cyber screening, the risk increases that a candidate will assert a claim that he/she did not get the job because the employer took into account that candidate's race, marital status, et al. As such, an employer might be better off not instituting a formal policy.

Taking it to another level, another issue has become a topic of great debate. Specifically, some employers are not satisfied with merely viewing the public portion of a candidate's online profile. There are many instances where employers have demanded that a candidate produce passwords so it can access the private portion of the candidate's social media site. The ACLU and privacy advocates lobbied hard for legislative protections that would limit the use of private social media in hiring and prohibit employers from requiring applicants and employees to provide usernames and passwords to their social media sites. Bills were introduced in many state legislative bodies, and, on Oct. 1, 2012, Maryland's "User Name and Password Privacy and Exclusions Act" became law, making Maryland the first state to enact such legislation. The Maryland statute prohibits all employers doing business in the state from requesting or requiring that an employee or job applicant disclose any username, password or other means of accessing an electronic communications personal account or service, including a social media account. In the ensuing 16 months, Arkansas, California, Colorado, Illinois, Michigan, Nevada, New Jersey, New Mexico, Oregon, Utah and Washington passed legislation prohibiting employers from requiring prospective and current employees to disclose a username or password to a social media account. Several more, including New York state, introduced such legislation in 2013, and many are expected to be signed into law in 2014.[2]

> Recognizing that users' postings—public and private—provide **potentially useful information** in assessing applicants for employment, a new name has been given to the practice: **"cyber screening."**

The legislation introduced in the New York State Legislature would prohibit an employer or educational institution from requesting or requiring an employee, applicant or student to disclose any username, password or other means for accessing a personal account through specified electronic communications devices.

Recently, New Jersey became the twelfth state to enact social media password protection legislation, which became effective Dec. 1, 2013.[3] The law prohibits an employer from retaliating or discriminating against any job applicant or current employee for any of the following conduct: (1) refusing to comply with an employer's request for login information for a personal media account; (2) reporting a violation of the law to New Jersey's Commissioner of Labor and Work Force Development; (3) testifying, assisting, or participating in an investigation concerning a violation of the law; (4) otherwise opposing a violation of the law.

The recently enacted and pending state laws have distinct commonality with respect to the prohibitions against requesting disclosure of usernames and passwords, but they vary materially in other respects. Some, for example, exempt law enforcement agencies that screen applicants for law enforcement positions. New Mexico's law protects only job applicants, not current employees. Some provide a private right of action in the event of violation, some do not. And, enforcement procedures and penalties for non-compliance vary widely. As new state laws are added to the already complex fabric of state legislation, national and multi-state employers must adopt hiring policies that comply with dozens of divergent statutes and adjust them as pending bills are voted upon and become law. This rather daunting challenge, together with the risks inherent in basing employment decisions on information gleaned from the Internet, may well cause employers to rethink their reliance on social media searches as a hiring tool—at least until the passage of federal legislation that may bring a level of consistency and symmetry to the law. Currently, the Social Networking Online Protection Act, introduced by Congressman Eliot Engel, is pending in the House of Representatives. It would prohibit employers from (1) requiring or requesting that an employee or applicant for employment provide a username, password, or any other means for accessing a private email account or personal account on a social networking website; and (2) discharging, disciplining, discriminating against, denying employment or promotion to, or threatening to take any such action against any employee or applicant who refuses to provide such information, files a complaint or institutes a proceeding under the Act, or testifies in any such proceeding. The act would provide for civil penalties and injunctive relief in the event of violation.[4]

Post-Employment Dangers Lurk

The difficulties inherent in navigating the world of social media do not end after the candidate becomes an employee. Post-hiring questions abound such as: Can an employer punish an employee for online postings? Can an employee disparage the company on social media? One of the growing bodies of law as it pertains to an employee's online postings, whether on Facebook, Twitter or blogs, deals with the question of whether the on-line speech is "protected concerted activity" under the National Labor Relations Act (NLRA).[5] In 2011, the NLRB issued the first decision after a full hearing regarding employee social media use and NLRA rights. In *Hispanics United of Buffalo*,[6] the Board ordered reinstatement of five employees who were found to have been unlawfully discharged for their use of social media to discuss the terms and conditions of their employment.

In 2012, the NLRB's Acting General Counsel released two memos detailing the results of investigations in dozens of social media cases. The memos underscored two main points: (1) employer policies should not be so sweeping that they prohibit the kinds of activity protected by federal labor law, such as the discussion of wages or working conditions among employees;[7] and (2) an employee's comments on social media are generally not protected if they are mere gripes not made in relation to group activity among employees. Demonstrating that the use of social media will only expand in the workplace, on May 7, 2013 the Office of the General Counsel of the NLRB issued an "Advice Memorandum" in connection with a pending matter in which it concluded that the employee who, together with nine other current and former employees of the employer, engaged in a Facebook group message to organize a social event.[8] At some point during the group's e-conversation, the employee expressed her disdain toward a supervisor who had tried to speak to her. She said that she told this supervisor to "back the freak off" and had other choice words for her employer. The General Counsel concluded that the employee was not engaged in concerted activity when she posted her comments on Facebook. However, it also concluded that the employer violated §8(a)(1) of the NLRA by forbidding the employee to access Facebook at work or post similar online commentary at any time during the workday. Furthermore, the General Counsel recommended that the Regional Office use the above case "as a vehicle to argue that [the decision] in *The Guard Publishing Company d/b/a The Register-Guard*, should be overturned.[9] In *Guard Publishing*, the NLRB held that employees have no statutory right to use the employer's email system for §7 purposes. That decision has been extended to the use of employer's electronic equipment in general. According to the General Counsel, the reversal of *Guard*

» Page 13

LOIS CARTER SCHLISSEL *is the managing attorney of Meyer, Suozzi, English & Klein, chair of the management committee and head of the employment law practice.* PAUL MILLUS *is of counsel to the firm.*

Messages

« Continued from page 9

instant messages, and other electronic documents in a format that would prevent their deletion or alteration.[2] The extensive recordkeeping obligations imposed by financial regulators make it nearly impossible for such organizations to permit the use of any communication systems that cannot be archived, so these firms may need to augment their policies, and perhaps even implement technological restrictions, to prevent the use of self-destructing messaging systems by their employees.

Companies subject to Securities and Exchange Commission (SEC) rules promulgated under Sarbanes-Oxley may also be somewhat restricted in the use of these messaging apps. These rules generally require companies to retain records relevant to an audit or review for seven years after its completion. This recordkeeping requirement applies broadly to include any documents that form the basis of the audit or review, including all "memoranda, correspondence, communications, other documents, and records" that are "created, sent or received in connection with the audit or review" and "contain conclusions, opinions, analyses, or financial data related to the audit or review."[3] Sarbanes-Oxley also created severe criminal penalties for the destruction of, or failure to preserve, certain documents. The act provides for up to 10 years' imprisonment for knowingly violating its audit record retention requirements, and up to 20 years for anyone who should "corruptly alter, destroy, mutilate, or conceal documents with the intent to impair their integrity or availability in an official proceeding" or "knowingly destroy, alter, or falsify documents and other records in federal investigations and bankruptcy."[4] Accordingly, companies and their auditors need to consider policies or technological restrictions that limit the ability to use self-deleting messaging systems in these circumstances.

In contrast to the regulatory trend toward greater transparency in financial markets, health care industry regulations emphasize patient privacy and data security. Laws such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Clinical and Economic Health Act (HITECH), as well as professional ethical rules, require health care organizations to safeguard the confidentiality of patient information, and threaten severe penalties for noncompliance.[5] For example, in August 2013, a managed care organization in New York paid the Department of Health and Human Service (HHS) more than $1.2 million dollars to settle allegations that it violated its HIPAA obligations to safeguard data when it returned several photocopiers to a leasing agent without erasing the data contained on the copiers' hard drives.[6] The strict privacy requirements imposed on the health care facilities and providers may make self-deleting messages a potentially attractive industry tool. Timely communication among medical providers quite literally can be a matter of life and death, but even in the most urgent of circumstances, patient information must be kept from unauthorized or accidental disclosure. TigerText has attracted considerable attention from media and investors for its success in marketing its messaging service to hospitals and medical practices, and some industry watchers have predicted that TigerText and other apps like it are poised to become valuable tools to the $3 trillion U.S. health care industry.[7]

As it would be impossible to list every regulatory requirement that might be implicated by the use of self-deleting messengers, companies will need to conduct their own individual analyses and risk assessments. Such assessments should also look beyond regulatory obligations, and determine how using these apps fits into those companies' document retention policies.

Document retention policies generally dictate how long records must be retained, setting a point at which, absent exceptional circumstances, records should be destroyed so as to avoid the cost and litigation risk of storing records that no longer serve a clear legal or business purpose. When documents are unavailable as a result of a comprehensive and consistently-enforced retention policy, courts generally accept this as a defense to claims of spoliation. As the U.S. Court of Appeals for the Fifth Circuit noted,

> [T]here is nothing improper about following a document retention policy when there is no threat of an official investigation, even though one purpose of such a policy may be to withhold documents from unknown, future litigation.[8]

This same motivation to keep documents that might be damaging or prone to misinterpretation out of the hands of litigation adversaries is a strong enticement to use self-deleting messaging apps. However, while courts universally recognize the business need to destroy documents as a matter of course, "[o]nce a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put in place a 'litigation hold' to ensure the preservation of relevant documents."[9] This standard, articulated in *Zublake v. UBS Warburg*, has been widely adopted by state and federal courts, and it largely mirrors the guidelines of the Sedona Conference, which states that the obligation to preserve documents arises "at the point in time when litigation is reasonably anticipated whether the organization is the initiator or the target of the litigation."[10] Failure to preserve evidence as required can result in sanctions, ranging from monetary fines to adverse inference jury instructions or even termination of the litigation.[11]

The obligation to issue a litigation hold and to preserve potential evidence conflicts with the very self-deleting nature that makes the use of such apps appealing, as such messages cannot generally be retained or retransmitted. Unfortunately, there is little guidance as to how courts will treat the use of self-deleting messaging apps in the litigation hold context. On one hand, the obligation to prevent electronic records from being deleted pending litigation is not absolute. Federal Rule of Civil Procedure 37(e) provides that courts generally should not sanction parties for "failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system." Similarly, the Sedona Principles urge that the obligation to preserve relevant evidence "must be balanced against the right of a party to continue to manage its electronic information in the best interest of the enterprise, even though some electronic information is necessarily overwritten on a routine basis by various computer systems," and recommend that "if such overwriting is incidental to the operation of the systems as opposed to a deliberate attempt to destroy evidence in anticipation of or in connection with an investigation or litigation it should be permitted to continue after the commencement of litigation."[12]

The obligation to issue a litigation hold and to preserve potential evidence **conflicts with the very self-deleting nature** that makes the use of such apps appealing, as such messages cannot generally be retained or retransmitted.

On the other hand, despite the balancing approach advocated by Rule 37(e), courts are hostile toward litigants who are perceived as skirting their discovery obligations or destroying evidence by cleverly engineering information systems, even if those systems superficially comply with case law and consensus guidelines. In a 2009 case, the Supreme Court Commercial Division imposed adverse inferences on a defendant corporation for spoliation because it structured its email system to limit each user to only 200 megabytes of storage.[13] Once reached, this limit prevented users from receiving additional email until they manually deleted messages. The court reasoned that, while employees were deleting emails "in the ordinary course of business," it nonetheless constituted gross negligence for the company to fail to ensure that employees would not delete relevant evidence during the pendency of litigation. The use of self-deleting messenger apps for communications relevant to pending or anticipated litigation may raise similar concerns.

The tolerance a court may demonstrate for a party's inability to preserve or produce communications sent using a self-deleting messaging service may vary based on the jurisdiction, the foreseeability of litigation, and the court's assessment of the party's intent in failing to preserve the potential evidence. Proposed revisions to Rule 37(e), if adopted, would require federal courts to consider the reasonableness of efforts to preserve records, the proportionality of any preservation efforts to the litigation, the extent to which parties were on notice of likely litigation, and the reasonableness and clarity of requests by adversaries that such records be preserved.[14] While this amendment may add uniformity in the federal courts' analysis of document retention obligations, it does not clarify how reasonable a court may find the use of self-deleting messages in any given scenario. Accordingly, the most conservative practice would be to suspend the use of such services for communications subject to a litigation hold.

These self-deleting messenger apps, and the legal issues they present, are an example of how technology often outpaces the law. The use of instant, private, and secure electronic communications in the health care industry would be generally consistent with the regulatory goals, as well as potentially life-saving—and this is just one example of the business and social advantages these apps may offer. However, the rules relating to the preservation and production of evidence are founded upon decades of experience with paper-based records, making predictions about a court's potential view of these applications in regulatory or litigation contexts difficult. Judicial rules conferences, and professional groups like the Sedona Conference, have labored with much success to adapt traditional evidentiary principles to a digital era, but, as is demonstrated with the case of self-deleting messages, the technology nearly always moves more quickly. Self-deleting message services may present an opportunity to reconsider the sustainability of continued application of rules and principles held over from the days of paper, and the degree to which business practices should be dictated by the looming specter of future litigation. Perhaps a record that feels more like an oral communication to the user should be treated more like an oral communication by the courts. But until there is such a reconsideration, it will be left to practitioners to assist businesses in identifying practices that minimize the simultaneous legal risks of both the over- and under-preservation of records, and to establish records retention policies that are defensible in later litigation.

1. *Byers v. Illinois State Police*, 53 Fed. R. Serv. 3d 740 (N.D. Ill. May 31, 2002).
2. See FINRA News Release, Dec. 26, 2013, https://www.finra.org/Newsroom/NewsReleases/2013/P412646.
3. See 18 U.S.C. §1520(a)(2); 17 C.F.R. §210.2-06(a).
4. 8 U.S.C. §§1512(c), 1519, and 1520(b).
5. See, e.g., 42 U.S.C. §§1302(a), 17931; 42 U.S.C. §1320d–1320d(9); 45 C.F.R. Parts 160 and 164.
6. U.S. Dep't of Health and Human Svc., "News Release: HHS settles with health plan in photocopier breach case;,"Aug. 14, 2013, http://www.hhs.gov/news/press/2013pres/08/20130814a.html.
7. Heather R. Huhman, Business Insider, "5 Companies That Transformed Enterprise Communication in 2013," Dec. 3 2013, http://www.businessinsider.com/5-companies-that-transformed-enterprise-communication-in-2013-2013-12.
8. See, e.g., *Arthur Andersen v. United States*, 374 F.3d 281, 297 (5th Cir. 2004) rev'd on other grounds, 544 U.S. 696 (2005).
9. *Zubulake v. UBS Warburg*, 220 F.R.D. 212, 218 (S.D.N.Y. 2003).
10. See, e.g., *VOOM HD Holdings v. EchoStar Satellite*, 939 N.Y.S.2d 321, 324 (1st Dep't 2012); The Sedona Conference, "Commentary on Legal Holds: The Trigger and the Process," 11 Sedona Conf. J. 265, 267 (Fall 2010).
11. See *Zubulake*, 229 F.R.D. at 437 (instructing the jury that it could infer destroyed evidence was adverse to the defendant); *U.S. v Philip Morris USA*, 327 F. Supp. 2d 21, 26 (D.D.C. 2004) (fining defendants $2.75 million for the destruction of evidence); *Telectron v. Overhead Door*, 116 F.R.D. 107, 130 (S.D. Fla. 1987) (entering default judgment against defendant for willful and bad faith document destruction).
12. The Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production, Comment 5.a (July 2005).
13. *Einstein v. 357 LLC*, No. 604199/07, 2009 WL 4543044 (Sup. Ct. N.Y. Cnty., Nov. 12, 2009).
14. See Comm. on Rules of Practice and Procedure, Report of Comm. on Rules of Practice and Procedure 104 (Jan. 3-4, 2013).

Cyber Bullying

« Continued from page 9

Given these parameters, the state bills that have been introduced to provide a private right of action for workplace bullying claims—*not aimed at an employee's protected class*—provide a definition of bullying that requires more than sporadic or occasional bullying. Pending legislation has been modeled on the 2004 "Healthy Workplace Bill" written by Suffolk University Law School Professor David Yamada. His definition of unlawful abusive workplace conduct includes "repeated infliction of verbal abuse such as the use of derogatory remarks, insults, and epithets; verbal or physical conduct of a threatening, intimidating, or humiliating nature; the sabotage or undermining of an employee's work performance; or attempts to exploit an employee's known psychological or physical vulnerability.[5] Similar to the type of hostile work environment that is protected by statute, workplace bullying will need to be "severe and egregious" before giving rise to an actionable claim. A 2007 study conducted by the Workplace Bullying Institute reported that the workplace harassment sought to be prevented by this type of legislation is four times more prevalent than the hostile working environment harassment currently proscribed by statute.[6]

Healthy Workplace bills do not address the various ways one can be bullied and, presumably, if the conduct meets the definition of bullying it is irrelevant whether one is being bullied face-to-face or electronically. However, it is conceivable that certain types of cyber bullying may be difficult to identify, and to impose employer liability in those situations may be grossly unfair. For example, a bully can sabotage or undermine a co-worker's work performance by stealing the victim's password and pretending to be the victim in email communications, or by posting defamatory statements about the employer or changing the victim's online profile to include sexual, racist or other inappropriate posts. Similarly, a co-worker can spread rumors, lies or gossip about the victim through websites or blogs while maintaining anonymity. As a result, a workplace bullying law should avoid employer liability in situations where the technologically sophisticated cyber bullying simply cannot be prevented.[7]

While few may dispute that bullying of any nature can be destructive in the workplace, presently employees are only afforded protections from the most egregious kinds of abuse. For example, an employee who is a victim of an assault (an intentional act by one person that creates an apprehension in another of imminent harm) or battery (an intentional act causing harmful or offensive contact with another) in the workplace may pursue criminal prosecution under most state penal laws, or civil recompense in jurisdictions that recognize a private right of action for assault and/or battery. In addition, while the common law tort of intentional infliction of emotional distress exists in many states, many courts have been reluctant to find those claims sustainable in the workplace.[8] Both federal and state courts have noted that "[i]t is extremely rare to find conduct in the employment context that will rise to the level of outrageousness necessary to provide a basis for recovery for the tort of intentional infliction of emotional distress."[9] Similarly, an employer who knows of an employee's propensity for bullying and does nothing to prevent or stop it before it results in actual harm, could be held liable in states that recognize claims against an employer for negligent hiring or supervision (to the extent these claims are not preempted by worker's compensation statutes).

No state, however, has enacted the kind of sweeping legislation that is directed at eradicating intimidating, humiliating and/or threatening conduct by a co-worker or conduct aimed at sabotaging and/or undermining another's work performance, all of which can have a debilitating effect on the victim. Indeed, people who are bullied at work have been found to experience stress and anxiety that can result in depression, panic attacks, digestive problems and insomnia. Moreover, bullying can result in significant consequences for employers, such as:

- Reduced efficiency, productivity and profitability
- Increased absenteeism and sick and medical leave
- Increased employee turnover resulting in additional recruitment costs
- Poor morale, erosion of employee loyalty and commitment
- Increased workers' compensation claims
- Adverse publicity and negative public image
- Legal costs incurred defending workplace bullying claims (even if such claims are found not be actionable)

Enacting a statute providing a private right of action for bullied employees would likely reduce the incidence of bullying and increase employer awareness of the necessity to prohibit such behavior. However, challengers to such legislation have been strident in their opposition; they fear such a statute would subject employers to a barrage of frivolous lawsuits and threats.

Indeed, throughout the country, employees already have a great deal of leverage against justifiable adverse action being taken by an employer. Too often employees unjustifiably claim that adverse action being taken against them is discriminatory in order to reverse the action, receive severance or increase the amount of severance being offered. Many employers are therefore already reluctant to take adverse action against an employee in a protected class without considerable documentation, even though the action being taken is entirely unrelated to such employee's protected class.

Moreover, opponents fear that legal regulation of workplace bullying will open a floodgate of employee complaints about conduct that does not amount to bullying, and is likely present in any work environment. Such conduct includes criticism of performance, discourteous remarks or acts of frustration, differences in opinion, insensitivity to work demands, and disappointing performance reviews. Accordingly, workplace bullying must be clearly defined to ensure it does not prevent the proper exercise of managerial authority, including decisions relating to job duties, workloads, deadlines, transfers, reorganizations, work instructions or feedback, evaluations, performance management, and/or disciplinary actions.

Indeed, Yamada's examples of bullying behaviors sought to be regulated by law demonstrate the potential overreaching effects of legislation. He includes hostile glares and other intimidating non-verbal behaviors, shouting, exclusion and the "silent treatment," excessively harsh criticism, and unreasonably heavy work demands. Legislation that makes this type of behavior illegal will hamper an employer's ability to conduct business, and may require constant policing of employees' interactions.

Employers cannot ignore **social media as a prevalent forum** in today's world **for workplace bullies.**

While many of the existing "healthy workplace" bills include safeguards designed to weed out frivolous claims, these protections are not foolproof. For example, an employer can escape liability by exercising reasonable care to prevent and promptly correct bullying behavior, and if the employee fails to take advantage of preventive or corrective measures provided by the employer. However, since the proposed legislation allows for attorneys' fees, it is not unlikely that an employee will locate a lawyer to bring or threaten to bring an action for a claimed statutory violation. Thus, there is nothing in the statute that can conclusively prevent an employee from making false claims or exaggerating a benign employee conflict to fit within the statutory definition of workplace bullying.

This is not to say that pervasive and severe workplace bullying, especially when aimed at sabotaging, intimidating, threatening and/or belittling a co-worker or subordinate, should not be prohibited conduct by employers. Given the potentially damaging effects of workplace bullying to an employer's business, employers would be well served to distribute and enforce a written code of conduct that specifically defines and prohibits workplace bullying, encourages reporting of conduct that meets the definition, provides a mechanism for investigating and resolving such complaints, prohibits retaliation for reporting, and imposes corrective action for violations, including termination if warranted.[10]

Employers cannot ignore social media as a prevalent forum in today's world for workplace bullies.[11] Last year's National Labor Relations Board (NLRB) Acting General Counsel's Memorandum on Social Media Policies demonstrates that policies must be carefully crafted to avoid running afoul of the National Labor Relations Act (NLRA). Policy language violates the NLRA if it restricts an employee's right to share and discuss their terms or conditions of employment with both co-workers and outsiders alike. However, social media policies prohibiting employees from engaging in "harassment, bullying, discrimination, or retaliation of co-workers that would not be permissible in the workplace … even if these actions are taken after hours, from home and on home computers" are permissible.[12]

One would be hard pressed to argue against a work environment that promotes respect and civility, and reduces or even eliminates workplace bullying without exposing an employer to unnecessary litigation for everyday behaviors prevalent in most work environments that strive for excellence in performance and productivity. Whether through legislation or simply through greater employer awareness and the enforcement of employment policies, this is a noble goal that employers and employees alike should endeavor to achieve.

1. These protections may be found in Title VII of the Civil Rights Act of 1964; the Age Discrimination in Employment Act of 1967; the Americans with Disabilities Act of 1990, as amended; Title II of the Genetic Information Nondiscrimination Act of 2008; and the Uniformed Services Employment and Reemployment Rights Act of 1994.
2. *Meritor Savs. Bank v. Vinson*, 477 U.S. 57, 67 (1986) (discussing hostile work environment in the sexual harassment context).
3. See *Harris v. Forklift Sys.*, 510 U.S. 17 (1993).
4. *Faragher v. City of Boca Raton*, 524 U.S. 775 (1998).
5. The original version of the Healthy Workplace Bill is set out in David C. Yamada, "Crafting a Legislative Response to Workplace Bullying," 8 EMP. RTS. & EMP. POL'Y J. 475 (2004).
6. The Workplace Bullying Institute is expecting to report results of a 2014 U.S. workplace bullying survey sometime this month (March).
7. If the harasser could be identified, a victim of this type of cyber bullying may be able to seek redress through The Computer Fraud and Abuse Act (the CFAA), a criminal statute that provides a civil cause of action for anyone whose computer system or network has been damaged or accessed without authorization, provided certain requirements are met. Although traditionally thought of as a form of relief for those who fall victim to computer "hackers," the Act has seen increased use in the employer-employee context in connection with the electronic theft of trade secrets.
8. In order to prevail in a lawsuit for intentional infliction of emotional distress, the plaintiff typically must show the following: (1) the defendant intended to inflict emotional distress; (2) the conduct of the defendant was extreme and outrageous; (3) the actions of the defendant were the cause of the plaintiff's distress; and (4) the resulting emotional distress to the plaintiff was severe.
9. *Darboe v. Staples*, 243 F. Supp. 2d 5, 19 (S.D.N.Y. 2003) (applying New Jersey law); *Ogden v. Keystone Residence*, 226 F. Supp. 2d 588, 604 (M.D. Pa. 2002) (applying Pennsylvania law); see also *Porter v. Bankers Life & Cas. Co.*, 2002 U.S. Dist. LEXIS 20627, at *5-6 (N.D. Ill. Oct. 25, 2002) (holding that an employee's claim for intentional infliction of emotional distress requires conduct that is "'so extreme in degree, as to go beyond all possible bounds of decency, and to be regarded as atrocious, and utterly intolerable in a civilized community' … and does not extend to 'mere insults, indignities, threats, annoyances, petty oppressions, or other trivialities'").
10. In some states, the policies set forth in an employee manual may be contractually enforceable, thereby conferring legal rights upon employees who face bullying behaviors.
11. Cyber bullying aimed at an employee's disability resulted in employer liability in *Espinoza v. County of Orange*, 2012 WL 420149 (Cal. Ct. App. Feb. 9, 2012).
12. See http://www.nlrb.gov/news-outreach/news-story/acting-general-counsel-releases-report-employer-social-media-policies.

NLRB

« Continued from page 9

framework set forth in the NLRB's reports on social media policies, the Board has continued to scrutinize employer social media policies and has struck down such policies where they explicitly restrict (or could potentially restrict) an employee's §7 activities. For example, in *Dish Network*,[6] the NLRB adopted an Administrative Law Judge's (ALJ) decision in which the ALJ, consistent with the Board's reasoning in the social media reports, found that the employer's social media policy was unlawful because it violated an employee's §7 rights. Specifically, the ALJ found that the employer's social media policy, which prohibited employees from making "disparaging or defamatory comments about DISH Network," was unlawful because such restrictions on negative commentary about an employer tend to chill an employee's §7 rights. Likewise, the ALJ found that the employer's policy of banning employees from engaging in negative electronic discussions during "Company time" was also presumptively invalid because it failed to clearly convey that union solicitation can still occur during breaks and other nonworking hours at the company.

Similarly, in *Butler Medical Transport*,[7] an ALJ found an employer's social media policy to be unlawful. In particular, the ALJ analyzed the employer's social media policy which, among other things, instructed employees to "refrain from using social networking [sites] which could discredit Butler Medical … ."[8] In reviewing this policy, the ALJ found that the policy was unlawful under the NLRA because employees could reasonably construe the policy to prohibit §7 activity. Specifically, the ALJ found that "[t]he rule on its face is broad enough to prohibit posting and distribution of papers regarding wages, hours and other working conditions [and] [i]t can reasonably be read to apply to non-work time and non-work areas."[9]

As exemplified by these recent decisions, the Board is continuing to review employer social media policies and is more than willing to strike down such policies as unlawful if there is any potential restriction of employees' §7 rights.

Adverse Employment Actions

With respect to employer use of social media to make employment related decisions, the NLRB's decisions in *Karl Knauz Motors*,[10] and *Hispanics United of Buffalo*,[11] detail how the Board will analyze social media-related terminations in the future.

In *Karl Knauz Motors*, an ALJ held that certain Facebook postings by an employee did not constitute protected, concerted activity under §7 and, therefore, the employee's termination was not unlawful.[12] In reaching this decision, the ALJ reviewed the Facebook posts at issue, which included criticism of events held by the employer and making fun of a car accident which occurred on the employer's related property. The ALJ found that since the employer terminated the employee for the comments made about the car accident, the termination was lawful. Specifically, the ALJ found that making fun of a car accident which occurred on a related property had "no connection to any of the employees' terms and conditions of employment" and, therefore, the posts were not protected under §7 of the NLRA.[13]

In *Hispanics United*, the NLRB ordered the employer to reinstate five workers that it previously terminated based on comments the workers posted on their respective Facebook pages. In reaching this decision, the NLRB delineated the standard that it will use when determining whether social media posts constitute protected, concerted activity under §7. The NLRB looked to past precedent, specifically, its two *Meyers Industries*[14] decisions from the 1980s. In these decisions, the Board held that an employee termination violates the NLRA if the following four elements are established: (1) the activity engaged in by the employee was "concerted" within the meaning of §7; (2) the employer knew of the concerted nature of the employee's activity; (3) the concerted activity was protected by the NLRA; and (4) the discipline or discharge was motivated by the employee's protected, concerted activity. In determining whether the activity was "concerted" activity, the NLRB again looked to the *Meyers Industries* decisions, which defined concerted activity as that which is "engaged in with or on the authority of other employees, and not solely by and on behalf of the employee himself"[15] and includes "circumstances where individual employees seek to initiate or to induce or to prepare for group action, as well as individual employees bringing truly group complaints to the attention of management."[16] Applying these definitions, the NLRB found that the Facebook posts were protected, concerted activity because one of the terminated employees specifically solicited comments from her fellow co-workers about perceived complaints from another co-worker. The Board interpreted this solicitation as the employees taking a first step toward group action to defend themselves against accusations that they reasonably believed a co-worker was going to make to management.

With *Karl Knauz Motors* and *Hispanics United* as guidance, the Board has continued to issue orders finding employer workplace decisions premised upon an employee's social media postings to be unlawful. For instance, in *Butler Medical*, the ALJ found that the employer's termination of an employee based upon postings he made on Facebook to be unlawful.[17] In the postings at issue, the employee discussed issues at work, including the condition of the employer's vehicles, and he also suggested that a former coworker contact an attorney about his recent termination from the company. This Facebook conversation was delivered to the employer and the employee was terminated.

The ALJ found that the termination violated the NLRA because the Facebook posting constituted protected, concerted activity.

> With 'Karl Knauz Motors' and 'Hispanics United' as guidance, the **Board has continued to issue orders** finding employer workplace decisions premised upon an employee's social media postings to be unlawful.

Indeed, the ALJ found that since the employee at issue was advising a former coworker to contact an attorney regarding his belief that he was terminated for complaining about the condition of the employer's vehicles, and since the condition of the employer's vehicles was a matter of mutual concern among employees, the employees were making common cause regarding a matter of concern to most employees. Therefore, the Facebook posting was protected, concerted activity and the termination of the employee was unlawful.

Likewise, in *Design Technology Group*,[18] the NLRB found that a termination premised upon a Facebook posting was unlawful because the employees' Facebook conversation was protected, concerted activity. In this matter, the employer terminated a number of employees who took to Facebook to complain about the conduct of a supervisor, the safety of the neighborhood they worked in, and the concerns they had about working late. One employee also mentioned that he could bring in a California labor law book to determine if the employer was violating California law. The Board found these complaints to be protected, concerted activity under §7 because the complaints related to the terms and conditions of employment and, therefore, the termination of the employees was improper.

Best Practices

In light of these recent NLRB decisions, the NLRB has signaled that (i) the Board will continue to review social media policies with a critical eye and will not hesitate to strike down policies as unlawful, and (ii) the Board will continue to take an expansive view regarding whether postings on social media will be considered protected, concerted activity. Given the NLRB's current position, employers are well advised to take certain steps to ensure that their social media policies pass muster, while continuing to protect themselves in situations where an employee has posted unfavorable comments about the employer on social media.

First, given the NLRB's stated position on social media policies, and its provision of a sample policy for employers, employers should review their current social media policy and compare it against the NLRB's sample policy, to ensure that it does not infringe on an employee's §7 rights and that the policy would pass NLRB scrutiny if challenged.

Second, given the NLRB's recent decisions regarding social media-related terminations, employers must be extra cautious when taking adverse action against an employee for postings the employee made on a social media website. This means that employers, before terminating an employee for social media posts, should closely review and investigate the posts at issue to determine if they are indeed related to the employees' terms and conditions of employment. If the social media posts are related to the terms and conditions of employment, terminating the employee for these posts would run afoul of the NLRA.

Finally, if a situation arises where the decision is made to terminate an employee for reasons unrelated to social media postings, but the employee has made social media postings related to the terms and conditions of employment, the employer should make it clear that the termination is not related to the negative social media postings. This can be accomplished by clearly delineating, in a termination letter or otherwise, the reasons for the termination.

In conclusion, given the NLRB's stated intent to continue its focus on social media issues, employers must take care to ensure that their social media policies and practices do not infringe on employee §7 rights.

1. See Abigail Rubenstein, "NLRB Chairman Lays Out Approach to Social Media Cases," Law360 (Jan. 21, 2014, 8:34 PM), http://www.law360.com/employment/articles/502701?nl_pk=28762f1d-ec1c-43a0-b672-eac751481d71.
2. See NLRB, Office of the Gen. Counsel, Report of Acting General Counsel Concerning Social Media Cases (May 30, 2012) (hereinafter NLRB Report), available at http://mynlrb.nlrb.gov/link/document.aspx/09031d4580a375cd.
3. Section 8(a)(1) of the NLRA makes it an "unfair labor practice for an employer to interfere with, restrain, or coerce employees in the exercise of the rights guaranteed in [S]ection 7."
4. See NLRB Report at 3.
5. Id. at 22-24.
6. 359 N.L.R.B. 108 (2013).
7. *Butler Med. Transp.*, 05-CA-097810, JD-58-13 (Sept. 4, 2013).
8. Id. at 7.
9. Id.
10. 358 N.L.R.B. 164 (2012).
11. 359 N.L.R.B. 37 (2012).
12. On Sept. 28, 2012, the NLRB affirmed the ALJ's findings with respect to the employee terminations.
13. *Karl Knauz Motors*, 358 N.L.R.B. at *11.
14. *Meyers Indus.*, 268 NLRB 493 (1983) (*Meyers Industries I*) and Meyers Indus., 281 NLRB 882 (1986) (*Meyers Industries II*).
15. *Hispanics United*, 359 N.L.R.B. at *2 (quoting *Meyers* Industries I, 268 NLRB at 497).
16. *Hispanics United*, 359 N.L.R.B. at *2 (quoting *Meyers Industries II*, 281 NLRB at 887).
17. *Butler Med. Transp.*, 05-CA-097810, JD-58-13 (Sept. 4, 2013).
18. 359 N.L.R.B. 96 (2013).

Face

« Continued from page 11

Publishing would certainly expand the ability of employees to organize and engage in union related activity. In the event that *Register Guard* was overturned, any blanket prohibition of instant messaging with friends and surfing the Internet during working hours would be deemed unlawful as overly broad.

As for public employees, their social media speech is protected by the First Amendment. The Fourth Circuit decided a case in September 2013 that should serve as a warning to public employers who take adverse actions against employees based on their use of social media. In *Bland v. B.J. Roberts*, two employees of the then-elected sheriff, who was in a re-election campaign, engaged in activity on Facebook that cost them their jobs and spurred a lawsuit.[10] The acts consisted of one employee "Liking" the opposing candidate's campaign page on Facebook and the second employee signing onto the same opposing candidate's campaign Facebook page and posting an entry on the page indicating [his] support for his campaign.

The district court granted summary judgment in favor of the employer, concluding that one employee's "merely 'Liking' a Facebook page is insufficient speech to merit constitutional protection" and that the second employee did not sufficiently allege that he engaged in speech because the record did not sufficiently describe what statement he had made on the Facebook page. The Fourth Circuit reversed, holding that, inter alia, "Liking" the campaign page constituted pure speech as well as symbolic expression stating "it is the Internet equivalent of displaying a political sign in one's front yard, which the Supreme Court has held is substantive speech."[11] As for the second employee, the court ruled that a posting on a campaign's Facebook page indicating support for the candidate constituted speech within the meaning of the First Amendment. For the same reasons as applied to the first employee's speech, the court found that the second's speech "was made in his capacity as a private citizen on a matter of public concern."[12]

Under New York Law, both public and private employees are protected by New York State Labor Law 201-d, which provides, in pertinent part:

> [It] shall be unlawful for any employer or employment agency to refuse to hire, employ or license, or to discharge from employment or otherwise discriminate against an individual in compensation, promotion or terms, conditions or privileges of employment because of … (c) an individual's legal recreational activities outside work hours, off of the employer's premises and without use of the employer's equipment or other property.[13]

While there appear to be no reported cases, yet, associating this section with social media, spending time on Facebook is, for many, a type of "recreational" activity that should be covered under the statute.

Even if the employer does not take action against an employee for social media postings, it may still find itself in violation of the law if it simply monitors the employee's social media presence. In one New Jersey case, *Pietrylo v. Hillstone Restaurant Group*,[14] the court found sufficient evidence supporting a finding that employees' managers violated the U.S. Stored Communications Act and the N.J. Wiretapping and Electronic Surveillance Control Act by knowingly accessing a chat-group on a social networking website without authorization.

Conclusion

There is little doubt that statutes and common law will have to adjust to the social media revolution. This was done before when businesses first communicated by mail, then fax and then email, allowing, at times, bad things to be communicated with the click of a key. Lawmakers, courts and businesses will adapt again to our rapidly changing communication environment.

1. Jacquelyn Smith, "How Social Media can Help (Or Hurt) You in Your Job Search," http://www.forbes.com/sites/jacquelynsmith/2013/04/16/how-social-media-can-help-or-hurt-your-job-search/.
2. Assembly Bill No. A00443-B; Senate Bill No. S02434-B.
3. New Jersey Password Protection Law Act 2878.
4. H.R. 537: Social Networking Online Protection Act.
5. Section 7 National Labor Relations Act.
6. *Hispanics United of Buffalo and Carlos Ortiz*, Case 03-CA-027872 (Dec. 14, 2012).
7. *Design Technology Group d/b/a Bettie Page Clothing*, 359 NLRB No. 96 (April 19, 2013) (the NLRB held that an employer unlawfully terminated employees who complained to management about working late hours in an unsafe neighborhood and who later continued their protest on Facebook. The Facebook postings were protected because they "were complaints among employees about the conduct of their supervisor as it related to their terms and conditions of employment and about management's refusal to address the employees' concerns."
8. Price Edwards & Company, Case 17-CA-92794.
9. *The Guard Publishing Company d/b/a The Register-Guard*, 351 NLRB No. 70 (Dec. 16, 2007).
10. *Bland v. Roberts*, 730 F.3d 368, 36 IER Cases 1045, 41 Media L. Rep. 2445 (4th Cir. (Va.) Sept. 18, 2013) (No. 12-1671), as amended (Sept. 23, 2013).
11. Id. at 386.
12. Id. at 389.
13. McKinney's Labor Law §201-d.
14. *Pietrylo v. Hillstone Restaurant Group*, 2009 WL 3128420 (D.N.J. Sept. 25, 2009).

Recruiting

« Continued from page 10

Federal Fair Credit Reporting Act.

Uniform Application of the Social Media Policy. If an employer chooses to screen applicants using social media, it should not do so selectively with some applicants and not others. It would be prudent for an employer to apply the same general protocols when checking social media for all applicants. Such consistency in application will help avoid discrimination claims based on applicants claiming that they were subject to more stringent requirements/checks than applicants of a different race or protected category.

On a related note, an employer should document its efforts to search an applicant's social media and retain copies of all documentation reviewed and considered in connection with the application process. Such documentation will be useful in establishing that the employer applied its policies in a consistent and non-discriminatory manner.

Flip Side: Turning a Blind Eye

Some employers, understandably, may opt to forgo using social media in the hiring process rather than risk a potential claim of discrimination. But this approach is not necessarily without risk. In New York, an employer may be liable to a person injured by an employee who the employer knew, or should have known, had a propensity to engage in the conduct which caused the injury. *Bouchard v. New York Archdiocese*, 719 F. Supp. 2d 255 (S.D.N.Y. 2010). A cause of action for negligent hiring or retention may be established if the employer had knowledge of facts that would lead a reasonably prudent person to investigate that prospective employee. *Richardson v. City of New York*, 2006 WL 3771115 (S.D.N.Y. Dec. 21, 2006).

The law does not require an employer to implement any specific background checks, or even require employers to conduct a criminal background check, except for certain positions where the employee deals with the public or vulnerable populations such as teachers and health care professionals. However, adopting the "hear no evil, see no evil" approach will not always serve to protect an employer from a negligent hiring or retention claim. An employer may, without taking any affirmative action or initiative to investigate, be told by a colleague, friend or other staff member about negative information posted on the Internet or social media site about a prospective applicant or existing employee. Take the extreme example: An employer is told that an applicant or employee purportedly posted that he or she was terminated from their prior employment after coming to work with a gun. In such instances, when the information conveyed to the employer is more than just unflattering, but may reveal a propensity on the part of the applicant or employee to cause harm or injury in the workplace, an employer may not be able to turn a blind eye and should consider conducting an appropriate level of investigation based on the reported information and circumstances.

Conclusion

Social media can be a valuable resource and an effective tool to recruit and screen applicants. However, employers should be wary about randomly checking the social media background of job applicants without first implementing policies and procedures to minimize the potential risk of discrimination or privacy claims by applicants who are denied employment.