Illinois Association of Defense Trial Counsel
Springfield, Illinois | www.iadtc.org | 800-232-0169
IDC Quarterly | Volume 21, Number 4 (21.4.M1)

The IDC Monograph

By: Jana L. Brady
Heyl, Royster, Voelker & Allen

Theresa Bresnahan-Coleman
Langhenry, Gillen, Lundquist & Johnson, LLC

Kimberly A. Ross
Cremer, Spina, Shaughnessy, Jansen & Siegert, LLC

Geoffrey M. Waguespack
Cremer, Spina, Shaughnessy, Jansen & Siegert, LLC

James H. Whalen
Williams, Montgomery & John, Ltd.

Jennifer A. Winking
Scholz, Loos, Palmer, Siebers & Duesterhaus LLP

Back Away from the "Like" Button: The Potential for Employers' Liability in the Age of Social Networking

I. Introduction

It is hard to imagine that employees retain a right of privacy when they post minute-by-minute updates concerning everything from the intricacies of their breakfast to the results of their annual physical exam on their favorite social networking website, such as Facebook or Twitter, for all to view. This is particularly so when viewed in light of prior rulings by the United States Supreme Court that support the proposition that disclosure to a third party confutes any claim or expectation of privacy.[1] There are walls, blogs, chat rooms, and listserves galore for employees to talk about everything from their personal lives to their jobs to their friends and colleagues. How are employers supposed to know when they are prohibited from using information seemingly out there in the public realm to make employment-related decisions?

Although an overwhelming majority of the laws that grant employees various rights of privacy in the workplace were promulgated before legislators could have contemplated the advent of social networking, the provisions exist nonetheless, and employers need to be cognizant of the way in which they monitor, utilize, or otherwise become involved in the use of social networking sites by employees. Employers should be cautioned

to document in writing, to distribute, and to enforce the company's policies concerning social networking, so as to diminish any claim or expectation of privacy.[2]

The circumstances under which an employer may lawfully investigate an employee's conduct outside of the workplace are defined by various Illinois and federal statutory and constitutional provisions. Very few of the statutes, however, specifically state how they would be applicable to the social media context. Instead, it is necessary to extrapolate from the language of each law how it may be applied in this context. Claims against employers could arise out of common law principles as well.

This Monograph seeks to provide both the practitioner and the employer with an understanding of the legal morass that currently constitutes the interplay between laws concerning employment and both the longstanding privacy laws and more recent laws developed due to the explosion of technology in the workplace. This Monograph primarily focuses on the Illinois laws that protect employees' privacy and the extent to which employers can and should monitor employees' social networking activities. Next, this Monograph provides an overview of the laws of the United States and their effect on an employer's ability to monitor and to use information gleaned from employees' postings in social networks. Finally, this Monograph explores the activity of the National Labor Relations Board, which kicked into high gear as this Monograph was nearing completion in late summer and early fall of 2011. Perhaps by the end of this Monograph, both the practitioner and the employer will be better equipped to spot in advance, and to avoid, the dangers that lurk within the laws governing the modern workplace and to have a better chance of conquering the new frontier that is being forged during this age of social networking.

II. Laws Affecting Privacy of Employees in Illinois

A variety of statutes in Illinois, complemented by common law, serve to protect employees' privacy in the workplace. The simple act of an employer viewing an employee's social network postings could entangle an employer in a costly legal snare created by those laws, if the employer discovers certain types of information about an employee through such a posting. As discussed below, employers should consider seriously the risks of viewing such information versus the benefits it could provide. This section provides an overview of the laws affecting employees' privacy in Illinois, identifies some of the potential legal problems that could arise as a result of viewing an employee's social networking postings, and suggests some practical solutions that might serve to insulate an employer from some of the concerns that could arise.

A. Illinois Constitution

Article 1, Section 6 of the Illinois Constitution[3] protects a right to privacy and prohibits the interception of communication by eavesdropping devices or other means.[4] This right to privacy, however, applies to invasions by the government or public officials only.[5] The right to privacy applies to employees who work for the state, but does not include private sector employees. That right extends to unreasonable searches and seizures only.[6] Illinois courts apply the two-pronged reasonableness analysis set forth in United States Supreme Court Justice John Marshall Harlan's concurrence in *Katz v. United States*,[7] and used for the analysis of the Fourth Amendment to the United States Constitution. Even with a constitutional protection of privacy for public employees, however, courts generally have been unwilling to find employees' expectations of privacy reasonable.[8] Therefore, the protections for employees have come primarily from statute.

B. Illinois Statutes and Common Law

1. Personnel Records Review Act

Generally, employers are entitled to intrude on an employee's personal life no more than is necessary to further the employer's legitimate business interests. This restriction is exemplified by Illinois' Personnel Records Review Act[9] (PRRA), which applies to businesses with five or more employees. The PRRA prohibits employers from gathering or keeping "a record of an employee's associations, political activities, publications, communications or nonemployment activities, unless the employee submits the information in writing or authorizes the employer in writing to keep or gather the information."[10]

The PRRA includes a provision that allows for a private right of action by employees who claim a violation of their rights under the act—that is, if the Department of Labor does not file its own complaint.[11] If an employee is discharged based upon information compiled in violation of this statute, the employee may attempt to file a retaliatory discharge suit on the theory that the gathering of such information is against public policy.

The prohibition on information gathering, however, does not extend to

> activities that occur on the employer's premises or during the employee's working hours with that employer which interfere with the performance of the employee's duties or the duties of other employees or activities, regardless of when and where occurring, which constitute criminal conduct or may reasonably be expected to harm the employer's property, operations or business, or could by the employee's action cause the employer financial liability.[12]

Illinois courts, however, have not interpreted this aspect of the PRRA, much less in the context of social networking. If the employer elects to gather such information, the PRRA requires that a record be kept in the employee's personnel record.

Thus, an employer faces a conflict between the different aspects of the PRRA. On the one hand, an employer cannot keep any records regarding an employee's associations, political activities, and the like. On the other hand, if the employer does become aware of other types of activities during work or on the employee's premises that interfere with the performance of the employee's duties, then the employer must keep a record in the employee's personnel file.

It would seem, therefore, that the PRRA does not prohibit employers from viewing Facebook or other social media websites and using the information they gather in their decision-making process regarding whether to hire, retain, or fire that individual. The PRRA prohibits only keeping a record of the activity. Further, the law excludes keeping records on employee conduct that involves criminal activity that may harm the employer's interests, activities that interfere with the performance of the employee or other employees, or could cause the employer financial liability. The exceptions are important, because it is entirely within the realm of possibility for an employee to file a lawsuit for negligent hiring or retention if the employer fails to discover information that is readily available to the public via Facebook or other Internet sites. Because of other pitfalls regarding the viewing of an employee's social media pages that will be discussed elsewhere in this Monograph, employers must hope that Illinois courts never will require them to learn about an employee's background through social media.

2. Right to Privacy in the Workplace Act

Other laws that touch upon the privacy rights of Illinois employees include Illinois' Right to Privacy in the Workplace Act[13] (RPWA), which makes it unlawful for an employer to refuse to hire or to discharge any individual, or otherwise to disadvantage any individual, because "the individual uses lawful products" (that is,

alcohol, tobacco, etc.) "off the premises of the employer during nonworking hours."[14] The prohibition does not apply in certain contexts, such as when the employee's use of the product impairs the employee's ability to perform assigned duties.[15] It, however, does not protect the privacy of the employee as to use of the products, because it permits the employer to charge different premiums to those employees who use certain lawful products outside work for health or other insurance as long as it reflects the differential rate charged to the employer. Employers should also note that the RPWA expressly applies to an employee's use of "products" only—it does not address other conduct or activities of employees, which was included in the original language of the RPWA, but not adopted.[16]

The RPWA further prohibits employers from inquiring in an application for employment "or in any other manner" as to whether prospective employees filed a claim for or received benefits under the Workers' Compensation Act[17] or Workers' Occupational Diseases Act[18] at any time.[19] The RPWA allows employees to file a private right of action for damages based upon a violation of the act, or if the employer retaliates against the employee for asserting rights under the act,[20] and the employer could be found guilty of a petty offense for the violation.[21]

3. Eavesdropping Act

Some may argue that monitoring an employee's social networking site is akin to eavesdropping. The Illinois Eavesdropping Act[22] (IEA) defines an "eavesdropping device" as including any device capable of intercepting electronic communications,[23] and prohibits the interception, retention, and use of electronic communications, unless it is done with the consent of all parties to the electronic communication.[24] The IEA allows an aggrieved party to file a civil suit for compensatory and punitive damages and injunctive relief.[25] It also makes any evidence obtained in violation of the IEA inadmissible in any civil, criminal, or administrative proceeding, including potentially a wrongful termination or retaliation suit.[26] The IEA is limited to devices used to hear or record oral conversations or to intercept electronic communications, and includes data transmitted by wire. The interception of electronic data traffic, such as Facebook, Twitter, or LinkedIn, for review by an employer conceivably could fall under this Act because the data is transmitted by wire.

4. Human Rights Act

The Illinois Human Rights Act[27] (HRA) makes it a civil rights violation for an employer to inquire into or to use the fact of an arrest or criminal history record information ordered expunged, sealed, or impounded as a basis to refuse to hire a candidate or to treat an employee differently than other employees.[28] The HRA does not, however, prohibit an employer from using information obtained by other means to find out if a candidate actually engaged in conduct for which he was arrested.[29] The HRA does not authorize or prohibit the use of drug testing, but employers may test employees who have been in rehabilitation and may prohibit the use of drugs by employees.[30]

5. Employee Credit Privacy Act

Another law in Illinois that touches upon privacy rights that theoretically could affect employees in the context of social media is the Employee Credit Privacy Act[31] (ECPA), which went into effect on January 1, 2011. Under the ECPA, employers are prohibited from inquiring into, obtaining reports on, or making hiring, firing, or retention decisions based on an employee or an applicant's credit information, including one's credit history or credit report. [32] The IECPA defines "credit history" as "an individual's past borrowing and repaying behavior, including paying bills on time and managing debt and other financial obligations."[33] Therefore, an employer could violate the IECPA if it learned from an applicant's social networking page that the applicant is in debt or has not paid bills on time, and thus decides not to hire the applicant. There are exceptions, however,

for individuals with certain job duties, including employees with unsupervised access to over $2,500 in cash or marketable goods, those who manage or direct the company, jobs requiring bonding or security, or those who have signatory power over assets of $100 or more.[34]

6. Illinois Common Law

Employers should also be aware of a litany of potential common law actions concerning privacy available to employees in Illinois. Invasion of privacy claims consists of four distinct causes of action: 1) intrusion upon the seclusion of another; 2) public disclosure of private facts; 3) publicity that places another in false light before the public; and 4) misappropriation of another's name or likeness. Only the first three are relevant to the employment context, and Illinois recognizes all three as causes of action (misappropriation is superseded by statute, 765 ILCS 1075/1).

The elements of intrusion upon the seclusion of another involve the following: (1) the unauthorized intrusion or prying into the individual's seclusion; (2) the intrusion must be offensive or objectionable to a reasonable person; (3) the matter upon which intrusion occurs must be private; and the intrusion must cause anguish and suffering.[35] Application in the employment context could include an employer's online searches of employees, sexual harassment, drug screening, and surveillance and monitoring of employees.

In *Burns v. Masterbrand Cabinets*,[36] the court held that the tort of intrusion into seclusion is actionable where a private detective working for an employer entered an employee's home under false pretenses seeking personal information. In *Benitez v. KFC National Management Co.*,[37] the court recognized a claim for intrusion into seclusion of another when employees alleged that supervisors and co-workers placed peep holes in a women's bathroom. Thus, this tort theoretically could be used if an employer uses surreptitious methods to view or monitor an employee's use of Facebook or social media outside of work or at work if the employee had a reasonable expectation of privacy.

The elements of a claim for public disclosure of private facts are where publicity was given to disclosure of private facts; the facts were actually private, not public; the matter was such as to be highly offensive to the reasonable person; and the matter was not of legitimate public concern.[38] The exception to the claim is where the recipient of the disclosed facts has a "natural and proper interest" in those facts.[39] Further, the "public" requirement is flexible. If the disclosure is only to a small group, it might still constitute the "public" if the plaintiff has a special relationship to them.[40]

The elements of a claim for publicity that places another in a false light are as follows: the defendant's actions placed the plaintiff in a false light; the false light would be highly offensive to the reasonable person; and the defendant acted with actual malice.[41] In the employment context, a claim for false light publicity could apply to an employer's publishing false information about the employee publicly, such as posting on the employee's Facebook wall.

Defamation is another common law claim that would be available to employees in the employment context. Illinois, however, recognizes a qualified privilege for some communications that otherwise would be defamatory. The privilege could limit the availability of the action to some employees. Qualified privilege protects honest communications of misinformation in certain circumstances where there is an interest of the person making the defamatory statement or an interest to whom the statement is published or an involved third party.[42] Such communications, even between employer and employee, may be protected.[43] Once a qualified privilege is shown, the plaintiff must show a "direct intention to injure or a reckless disregard of the defamed party's rights and the consequences that may result."[44] The privilege can limit the ability of the employee to recover for defamation if the employer had an interest in the matter with which the false statement was concerned. The publication requirement is satisfied if the statement is communicated to another who is not the plaintiff, including others inside of the workplace.[45] Statements made in connection with the administration of the Unemployment Act are absolutely privileged.[46]

Intentional infliction of emotional distress is also recognized as a claim aggrieved employees can pursue against their employers. Courts, however, are reluctant to find the elements of the claim met in the employment context.[47]

Also, for public employees, the Local Governmental and Governmental Employees Tort Immunity Act[48] limits recourse to employees. The act provides immunity to governmental bodies for libel, slander, or provision of information.[49] This statute eliminates causes of action for defamation, invasion of privacy through publicity that places another in a false light, and invasion of privacy through public disclosure of private facts for employees of public entities.[50]

The bottom line is that any number of social media outlets being operated by or posted to by employees can contain information in them that an employer would otherwise be prohibited from specifically seeking out. For instance, while an employer might want to view a prospective employee's Facebook page to find out about prior employment to double check references, the employer could unwittingly view something it otherwise is prohibited from acting on or keeping a record of, such as the employee's political affiliation or the fact that an employee previously filed a claim for employment discrimination.

C. Federal Privacy Laws: An Overview

The federal rules governing privacy were enacted well before social media came into being and therefore say little about how individuals' privacy is to be protected in employment contexts dealing with social networking sites. Surprisingly, not many cases have addressed these laws' applicability to social media, although what does exist provides useful guidance. Employment law practitioners should be knowledgeable of these laws and how they have been interpreted by the courts to best advise their clients of the appropriate action to take when dealing with issues involving social networking sites. Below is an overview of several federal statutes that could be applicable in the social media context.

1. The Privacy Act of 1974

The Privacy Act of 1974[51] (Privacy Act) protects from disclosure certain federal government information pertaining to individuals. The Privacy Act defines the "records" it protects as

> any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or photograph * * * *[52]

The Privacy Act does not apply to records that are not maintained by any federal agency.[53] It mandates that no federal agency "shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains."[54] Certain exceptions apply and concern specific government activities.[55] One such exception is the disclosure of protected information pursuant to court order.[56]

The Privacy Act has limited applicability to social networking site content, as there is no federal agency responsible for maintaining content produced on social media sites such as Facebook. Moreover, no federal cases have yet addressed the act in the context of social media. Thus, even though individuals' private information can be produced pursuant to court order, such an order can relate to federal information under the Privacy Act only. Consequently, although employment law practitioners should be mindful of the Privacy Act generally, they must look elsewhere for guidance on what federal law applies to govern the production of private information in the context of social media.

2. Electronic Communications Privacy Act and Stored Communications Act

The Electronic Communications Privacy Act[57] (ECPA) was enacted in 1986 to amend the federal Wiretap Act and to extend privacy protection to electronic communications.[58] Title I of the ECPA contains its main provisions. It specifically prohibits the intentional interception, use of a device to intercept, disclosure, or use, of the contents of an electronic communication.[59] The ECPA defines "electronic communication" as "any transfer of signs, signals, writings, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce."[60] It protects electronic communications that are stored temporarily incidental to the electronic transmission itself and that are stored for purposes of backup protection—but it does not define what "stored" means.[61] In *U.S. v. Councilman*,[62] the United States Court of Appeals for the First Circuit ruled that e-mail messages are protected under the ECPA while they are in transient storage on their way to their final destination, such that any unauthorized interception of those messages constitutes an offense under the act.[63] Still, such protection is outdated in the age of social media, where electronic communications can be accessed anytime from any computer.[64]

The Stored Communications Act[65] (SCA), contained in Title II of the ECPA, addresses the disclosure of stored wire and electronic communications records held by "electronic communication service" providers and "remote computing service" providers.[66] It was enacted because "the advent of the Internet presented a host of potential privacy breaches that the Fourth Amendment does not address."[67] It limits the government's right to compel providers to disclose information in their possession about their customers and subscribers, and it limits the right of an Internet service provider to disclose information voluntarily to the government about customers and subscribers.[68] The SCA also has been held to apply to private employers, even when they do not provide electronic communications services to the public.[69]

The SCA concerns two different types of services: "electronic communication service" and "remote computing service." "Electronic communication service" means "any service which provides to users thereof the ability to send or receive wire or electronic communications."[70] Social networking websites have been held to be electronic communication service providers under the SCA.[71] The SCA prohibits such a provider from "knowingly divulg[ing] to any person or entity the contents of a communication while in electronic storage by that service."[72]

"Remote computing service," on the other hand, means "the provision to the public of computer storage or processing services by means of an electronic communications system."[73] An "electronic communications system," as opposed to a "service," is defined as "any wire, radio, electromagnetic, photoelectronic or photooptical facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications."[74] The SCA prohibits such a provider from "knowingly divulg[ing] to any person or entity the contents of any communication which is carried or maintained on that service."[75] A person who provides neither an electronic communication service nor a remote computing service can disclose or use with impunity the contents of an electronic communication unlawfully obtained from electronic storage.[76]

The requirements for requesting disclosure of electronic information are different under each service and specifically apply to government entities. Electronic communications that have been in storage through an electronic communication service provider for 180 days or fewer must be requested through a search warrant.[77] Electronic communications that have been in storage through an electronic communication service provider for more than 180 days, or that have been in storage through a remote computing service for any length of time, need only a subpoena with notice to the subscriber in order to be produced.[78] The SCA does not allow for subpoenas in a civil case to access a user's stored communications or data.[79]

Both the ECPA and the SCA have been interpreted differently by the courts on the issue of "interception" and "storage." In *Konop v. Hawaiian Airlines, Inc.*,[80] an airline pilot sued his employer for accessing without

authorization his private website where he had posted criticisms of his employer, and the Ninth Circuit concluded that access to the protected section of the website did not constitute a violation of the ECPA, because there was no interception of electronic communications but rather access to stored electronic information that occurred only after the electronic communication already had been transmitted.[81] Access of that stored information, however, constituted a violation of the SCA because the log-in credentials used to access the protected site were not utilized by the authorized users, but rather by an unauthorized third-party.[82]

The United States Court of Appeals for the Seventh Circuit, in *U.S. v. Szymuszkiewicz*,[83] distinguished *Konop* on the nature of the timing required for there to be an interception that violates the EPCA. In that case, the defendant allegedly set up a rule in his supervisor's Outlook e-mail account to have every e-mail message she received forwarded to him so that he could monitor e-mail messages sent to his supervisor about him.[84] The Seventh Circuit affirmed the defendant's jury conviction, holding that he was correctly prosecuted under the ECPA rather than the SCA.[85] The defendant intercepted the supervisor's e-mails at the server side and thus "caught" the messages "in flight" to their final destination, but the communication, after being copied, would have been made within a second to the supervisor, and this was certainly contemporaneous for purposes of the ECPA.[86] The court thus ruled that there was no timing requirement regarding an "interception" under the ECPA.

In *Pure Power Boot Camp v. Warrior Fitness Boot Camp*,[87] the plaintiffs claimed that the defendants stole the plaintiffs' business model, customers, and internal documents; breached employee fiduciary duties; and infringed on the plaintiffs' intellectual property.[88] During discovery, the defendants filed a motion, under the ECPA and the SCA, to preclude the use or disclosure of 34 of one of the defendant's e-mails from his personal e-mail accounts, which were obtained by one of the plaintiffs (that defendant's former employer) from the plaintiff-employer's computers after the defendant-employee had ceased working for that plaintiff; the plaintiff-employer was able to access the e-mails because the e-mail log-in information for the defendant-employee's personal accounts was saved on the work computer.[89]

The district court ruled that only the SCA was applicable to the action, noting that the majority of courts that have addressed the issue have determined that the "e-mail stored on an electronic communication service provider's system after it has been delivered, as opposed to e-mail stored on a personal computer, is a stored communication subject to the SCA."[90] The court noted that usually "employees have no expectation of privacy in their workplace computers, where the employer has a policy which clearly informs employees that company computers cannot be used for private e-mail activity, and that they will be monitored."[91] In such cases, the employer does not need consent to search an employee's computer files.[92]

In *Pure Power Boot Camp*, however, even though the plaintiff-employer had a policy in place that curtailed employees' expectations of privacy in their work computers and work e-mails, the defendant-employee did not store any of the contested communications on the plaintiff-employer's computers, and did not send or receive those personal e-mails on the company e-mail system or computer—rather, they were located on, and accessed from, third-party communication service provider systems.[93] The plaintiff-employer could have access to the defendant's personal accounts only if the defendant had given consent.[94] The court found that, at most, by leaving his log-in credentials saved to his work computer, the defendant-employee might have given consent to the plaintiff-employer to view his password for his personal e-mail account, but that he did not give her consent to use it and that he did not consent for her to guess that this same password also provided access to his other personal e-mail accounts.[95] As a result, the plaintiffs were precluded from using the e-mails as evidence, but they were not precluded from using the e-mails for impeachment purposes if the defendants opened the door.[96] The court also determined that the ECPA did not apply, because that statute concerns the interception of electronic communications that have not yet been delivered or are intercepted contemporaneously when received by the intended recipient.[97] Because the plaintiff-employer did not access and print the e-mails contemporaneously with their transmission, she did not violate the ECPA.[98]

In *Shefts v. Petrakis*,[99] the plaintiff, who was the founder, president, and CEO of the defendant company, sued individual employees of the company, including one of the members of the board of directors, alleging

violations of the ECPA and SCA, among other things, for monitoring his e-mails and text messages sent over the company's network without his authorization.[100] In fact, the defendants had installed monitoring software on all of the company's computers, including the computer used by the plaintiff, after suspecting that the plaintiff was sexually harassing other employees and violating his fiduciary duties.[101] The board of directors also ratified, after this software was installed, the adoption of an employee manual, which stated that the company owned the rights to all data and files in any company computer or information system, that the company reserved the right to monitor all e-mail messages and use of the Internet on company computers, and that no employee could access another employee's computer without prior authorization from the board of directors.[102]

The plaintiff filed a motion for summary judgment, and the district court found that an "intercept" under the ECPA occurred of the plaintiff's text messages when the monitoring software acquired and logged the messages on a separate server.[103] The court also found, however, that the plaintiff consented to the logging of his text messages because he was involved, as a member of the board of directors, with the purchase and installation of the monitoring software server and knew that e-mails sent from his Blackberry would be stored on the company's network via this software server.[104] Further, while there was a question of whether the plaintiff gave his implied consent for his text messages to be logged, the court said the company's employee manual was clear that the plaintiff's electronic communications on company equipment was subject to archiving at all times, and included personal and private messaging systems.[105] Consequently, the court denied the plaintiff's summary judgment motion on his ECPA count.[106]

Additionally, the court denied the plaintiff's summary judgment motion on the count alleging violation of the SCA.[107] The parties did not dispute that the text messages and e-mails monitored by the defendants were "electronic communications" under the SCA, that the defendants intentionally accessed them, or that the company is an entity providing an electronic communications service by virtue of the fact that it is a private employer providing e-mail service to its employees.[108] As a result, and because the court found that the defendants were authorized under the employee manual to access and monitor the plaintiff's communications, the court ruled there was no violation of the SCA.[109]

Finally, in *Crispin v. Christian Audigier, Inc.*,[110] the plaintiff, an artist, sued various licensees for breach of an oral license to use his artwork in garments.[111] The defendants issued subpoenas to social networking sites, including Facebook and Myspace, for information on the plaintiff's subscription to the sites, as well as to access all of his communications on those websites.[112] The court held that Facebook postings and MySpace comments are not protectable as a form of temporary, intermediate storage because there is no in-between step after a message is sent and before it is received.[113] The court also held, however, that wall postings and comments are stored for backup purposes on the wall or comment space, because there is nowhere for them to go once they are posted.[114] For these reasons, the court ruled that the social networking sites Facebook and MySpace are electronic communication service providers with respect to wall postings and comments, and that such communications are in electronic storage. It also ruled, in the alternative, that these websites are remote communication service providers with respect to wall postings and comments, because their content is accessible to a limited number of users selected by the poster.[115] The court concluded that this content, therefore, was not private and could be produced in discovery. The plaintiff's private communications contained on these websites, however, could not be produced.[116]

These cases illustrate that maintaining privacy in one's electronic communications is dependent upon how the communication is made and how it is obtained. Important considerations include whether the communication is "intercepted" prior to arriving at its final destination, and whether the interceptor is authorized to view the electronic content. Further, to the extent that social networking sites can be considered electronic communication service providers, as well as remote communication service providers, such a determination can have significant ramifications in discovery. Employment law practitioners should pay close attention to how clients' employee manuals are drafted regarding monitoring computer usage, and should

advise that they be revised as necessary, so that clients are not found to be in violation of either the ECPA or the SCA.

3. Federal Rules of Evidence and of Civil Procedure

Although there is a dearth of case law interpreting the ECPA's applicability to social networking sites, several courts have dealt with the issue of privacy and social networking under the Federal Rules of Evidence and the Federal Rules of Civil Procedure when resolving discovery disputes. These cases make clear that an individual's expectation of privacy while using social networking sites varies depending on the nature of the information sought.

In *Mackelprang v. Fidelity National Title Agency*,[117] the plaintiff alleged sexual harassment under Title VII against her former employer, as well as various state law claims, including constructive discharge.[118] After her employment ended, the plaintiff allegedly set up two different MySpace accounts that depicted opposing views of her as single and childless, and as married with children.[119] The defendant served a subpoena on MySpace to produce all records for these two accounts, including all e-mail communications.[120] MySpace produced certain public information, but refused to produce private e-mail communications without a search warrant or a letter of consent to produce by the owner of the account.[121] The plaintiff refused to execute a consent letter, claiming the information sought was irrelevant and constituted an invasion of privacy.[122] The court denied the defendant's motion to compel without prejudice, holding that the defendant could pursue the discovery of relevant and discoverable private e-mail communications by issuing limited requests for production of relevant communications.[123] The court said that the defendant was engaged in a fishing expedition because it was basing its request for all e-mail communications on mere suspicion or speculation as to what information might be contained in the private messages.[124] In refusing to grant the defendant's blanket request for all communications, the court noted that "[c]ourts applying Rule 412 [of the Federal Rules of Evidence][125] have declined to recognize a sufficiently relevant connection between a plaintiff's non-work related sexual activity and the allegation that he or she was subjected to unwelcome and offensive sexual advancements in the workplace."[126] Further, the court found that "the probative value of such evidence [non-work related sexual activity and allegations of harassment] does not substantially outweigh its unfair prejudicial effect to [the p]laintiff."[127]

In *EEOC v. Simply Storage Management, LLC*,[128] the EEOC filed a complaint on behalf of individuals who alleged that their defendant-employer was liable for sexual harassment by a supervisor.[129] The court held a discovery conference at the EEOC's request, because the parties could not agree on the proper scope of discovery as it related to the defendant-employer's request for all content from the individuals' Facebook and MySpace pages.[130] The EEOC objected to the production of all social networking site content on the basis of relevancy and invasion of privacy, as well as for being overbroad and unduly burdensome.[131] The court ruled that some social networking site discovery was appropriate, so long as it was time-and-content-specific for the issues at hand.[132] Noting that the Federal Rule of Evidence 26 standard for discovery is broad, the court commented that "[d]iscovery of [social networking site content] requires the application of basic discovery principles in a novel context," but that ultimately, "the challenge is to define appropriately broad limits * * * on the discoverability of social communications in light of a subject as amorphous as emotional and mental health."[133] The court further noted that, although privacy concerns might be relevant to the question of whether requested discovery is burdensome or sought for a proper purpose, "a person's expectation and intent that her communications be maintained as private is not a legitimate basis for shielding those communications from discovery."[134]

The court cited two Canadian cases to buttress this point: *Leduc v. Roman*[135] and *Murphy v. Perger*,[136] in which the courts held that a requesting party is not entitled to access all non-relevant material on a site, but that simply locking a profile from public access does not prevent discovery either.[137] The court also stated that any concerns the individuals had about their private information being discovered and embarrassing them were

outweighed by the fact that the production would be of information that they already had shared with at least one other person through private messages or with a larger number of people through postings.[138]

Under the Federal Rules of Evidence and the Federal Rules of Civil Procedure, as well as under the ECPA and the SCA, employment law practitioners must be cognizant of privacy concerns when dealing with information obtained from social networking sites. In the course of litigation, counsel should craft discovery requests carefully so as not to set off a firestorm about privacy, but that are broad enough to encompass all relevant, discoverable information.

D. Warnings to Employers

While there are a multitude of potential causes of actions that employees can pursue among the various Illinois statutes and common law, as well as the federal laws, there are no laws in Illinois that specifically and unequivocally prohibit employers from viewing content regarding employees and potential employees on the Internet, whether through a simple Google search, or through the use of a specific social media platform such as Facebook, Twitter, or LinkedIn. Although no specific prohibitions exist, and no Illinois court has yet interpreted any of the statutes above to specifically prohibit employers from using the Internet in reference to employees and potential employees, this lack of prohibition does not necessarily mean an employer doing so is advisable. Employers can run into pitfalls at every turn with social media.

Therefore, the next section of this article will focus on whether, and if so, to what extent an employer can monitor an employee's social media postings while on and off the clock. It will also discuss whether and to what extent an employer can screen candidates for job openings by reviewing the candidate's social media pages, though the analysis as to whether dealing with an employee or a potential employee requires similar considerations. At the outset, however, it must be stated that nothing contained in this article can or should be taken as legal advice. This analysis is only general in its application and there are far too many facts to analyze in each employment scenario to apply such general concepts to specific situations. Instead, the analysis will provide some thoughts and talking points to consider when discussing such issues with employers.

Even though employers often act in a manner that would be ill-advised if the employer first contacted an employment lawyer and sought advice before acting, this fact, of course, does not mean that the employer's actions violated any law (either statute or common law). The problem is that the majority of employers are not well-versed in all the laws that potentially affect their business, or their employees in particular. While one would hope that most employers are familiar with the "big" concepts like discrimination based on protected classifications and wage and hour laws, the fact is that far too many employers are entirely unfamiliar with the lesser-known, but equally as important laws. The average employer likely violates the law potentially on a daily basis, usually unknowingly or unintentionally. Unfortunately, a lack of knowledge of a law, and to a certain extent, the lack of intention to violate the law, usually does not allow an employer to escape the consequences should someone (or a governmental entity) decide to pursue the issue.

Even where an employer does not directly violate the law, however, proving there was no violation can be costly and difficult. Even when employers win, they can and usually still lose, due to the expense of litigation and the negative publicity that often accompanies a case. Because of all the pitfalls facing the average employer, and because the average employer is not nearly as well-versed in all the laws as it should be, erring on the side of caution and advising against certain practices often is best. The social media context should be no different, especially as this field is such an emerging area of employment law. Some day, the Illinois legislature, or even Illinois courts, might provide more guidance to help employers know what they can and cannot do in the context of social media. Until then, employers must be cautioned (and cautious) at every turn.

There are multiple ways in which an employer can become privy to the contents of an employee's social media publications. Gaining access to the social media pages also depends on whether the employee has set the page for public viewing, or whether it is private until the employee gives permission for someone to view the page. Taking the example of a Facebook page set to private, an employer could send a friend request to the

employee and the employee could accept. This scenario leads to two possible conclusions: either the employee truly wished for the employer to be able to view his Facebook page, or the employee felt pressured to accept the request. Can an employer take an adverse action against the employee if the employee does not accept the friend request? Another situation could arise where an employee allows the friend request of a co-worker and then a manager of the employee views information posted to the employee's social media page through the co-worker's account. One scenario that seemingly would be prohibited is where an employer seeks to be friends with an employee under false pretenses, such as by using a fake name. Would these surreptitious means of acquiring information about an employee violate the law? What if the employer used the information to take an adverse employment action against the employee?

No matter what the employer's motivation in sending the request or the employee's motivation in accepting the request, the employer now has access to everything the employee posts on his personal Facebook page. In what ways can the employer act on the information and in what ways must the employer ignore the information?

The fact is that just as it is impossible to "unring a bell," it may be just as difficult for an employer to ignore what it reads on an employee's social media page. Perhaps the employee complained about being arrested the previous week for public urination; or perhaps the employee posts a photo in which he is smoking a cigarette; maybe he blogs about going to a rally for a particular political candidate. It seems that many social media users often have no real internal filter when it comes to divulging things on the Internet, especially when they think their "friends" are the only ones reading the postings. One might be tempted to argue also that it is the employee's own fault for allowing the employer to view the information in the first place. Unfortunately, none of the state or federal statutes take into consideration how the employer learned of the protected information. Rather, the laws are much more focused on the fact that the employer learned the information and then acted upon it. In the above scenarios, an adverse action taken for the arrest could violate the Illinois Human Rights Act. An adverse action taken due to the cigarette smoking could violate the Illinois' Right to Privacy in the Workplace Act. An adverse action taken against the employee due to his support of a particular political candidate could violate the Illinois' Personnel Records Review Act. Although many Illinois employers may believe the adverse actions may be justified and legal, how many are actually aware of these laws?

Certainly, employees (and all users of social media) have to learn how to take responsibility for their own use of social media and must learn to filter what they post. There are no friendship confidentiality laws akin to the "attorney-client" privilege. Whatever a person posts should be considered to be fair game to be discovered by the rest of the world, even though the rest of the world is not "friends" with the person who posted the personal information. How many stories have we heard of where people post that they are going out of town and then their houses get robbed? It is fair enough to argue that if someone does not want another person to learn something, then that information should not be posted on a social media page. Social media websites even provide such warnings to their users.

The scenarios potentially go on and on. So, one must ask why an employer would ever want to take the risk and even view the information posted to the Internet in the first place? Although employers should be cautioned about doing anything to limit an employee's rights and conduct outside of the work environment, employers do have the right to act upon certain information they come across, even when it comes from social media. Some examples where an employer could act upon an employee's postings on the Internet include the following: an employee divulging confidential information about the company; an employee divulging personal information about another employee; an employee misrepresenting the company or its products or services; an employee defaming or disparaging another employee. When developing policies on these topics, it is extremely important to consider potential liability under the National Labor Relations Act (discussed below), which especially recently, has been enforced in quite a Draconian manner in the context of employers taking adverse employment actions against employees expressing opinions about their employers.

Suppose a company is doing work for its client on a project with some public opposition due to environmental concerns. One of the company's employees (who has no responsibility for the client's project) posts to her Facebook page (on her own time and from her own computer) her personal opposition to the client's project. The company has several concerns, including that the employee may take important confidential documents in the company's possession about the client's project, or that the company's client could find out about the employee's public opposition to the project, thereby jeopardizing the company's relationship with its client. What, if anything, can the company do?

The company certainly could start by having a non-confrontational conversation with the employee and could tell the employee that, although the company is not telling her what she can do or what she has to believe, the company is concerned that her public expression of her opinion is detrimental to the company's business and cannot be allowed. But suppose that the employee refuses to stop posting. Can the employer issue a harsher sanction, such as a suspension or termination? The answer is likely in the affirmative, especially if the employer can show that the employee's comments were jeopardizing the company's business. But just because the employer may be justified in the termination does not mean that the employer will not have to face defending itself in court.

The above scenarios apply to those already employed. What about checking out a potential employee's social media postings? In this scenario, if the candidate's account is not public, then it will no doubt be more difficult to view postings through legitimate means, as the employer should not gain access through false pretenses. But if the candidate's account is public, or if the employer has another legitimate way to gain access, such as if the candidate is "friends" with a current employee, then nothing under Illinois law likely prohibits the employer from viewing the contents. This situation, however, leads to similar questions as above, which is whether the employer *should* view a candidate's page. The potential for viewing or learning about a prospective employee's legal conduct outside of the work setting, prior criminal history, poor credit history, sexual orientation, or political affiliation, just to name a few, can lead to serious questions of whether this information was taken into consideration during the hiring process (or at any other point during employment).

Although an employer can make certain decisions based on illegal characteristics just by looking at an employee or his resume (such as race, national origin, or age), or just by speaking to the employee during an interview (and hearing an accent), and can therefore subject the company to potential litigation, these are the more obvious scenarios of which most employers already are aware. The bigger problems come when the employer takes actions or makes decisions based on facts or traits that it does not realize would be illegal. That situation is more likely to occur when viewing personal information about an employee (or prospective employee) that is beyond the typical job application and resume.

There is quite possibly very legitimate information that the employer would be interested in knowing, such as prior job history or experience, more about the employee's skills, how the employee expresses himself. A skilled interviewer should be able to gather this information without viewing an employee's social media pages, such as through a thorough interview process, a request for a writing sample and following up by checking with prior employers. Further, if an employer later learns that the employee lied during the interview process, even if the information about the lie came from the employee's social media page, the employer might be able to terminate employment due to the lie (assuming that the subject of the lie was not something the employer was not entitled to know in the first place).

III. Beyond Privacy Issues: Additional Legal Implications of Social Media for Employers

In 2011, the power of social media became apparent to the world during the popular uprisings in the Middle East. Ordinary Egyptian citizens brought social media to bear in their revolution against Egyptian

strongman Hosni Mubarak, using Facebook and Twitter to organize protests and to report the situation to the outside world, unfiltered and in real time. The toppling of Mubarak's decades-old regime with the help of social media demonstrated for the world that Twitter, Facebook, and blogs transcend ordinary Internet zeitgeist, and could carry enormous implications for anyone using this technology to communicate.

Given the fluid, immediate and potentially potent nature of social media, employers would be wise to consider the legal implications of social media in the workplace, beyond employee privacy. The appeal of social networks to businesses is obvious. Companies might have an interest in creating and maintaining a presence in one or more of these social networks to build a brand, attract new customers, keep existing customers, and gain valuable data for marketing their products and services. Social networks allow companies to communicate with large numbers of people almost instantly and without the costs associated with a traditional print and broadcast media campaign, affording them publicity and access to consumers on an unprecedented scale. In the past, companies had to rely upon marketing data and a little bit of luck to place advertisements in print and broadcast media, hoping to connect with their target market during the right television show or radio broadcast. With mobile access to email and social networks, there is a greater likelihood that companies will connect with their target market anytime, anyplace. Now, a company can communicate the arrival of a new product directly to thousands of individuals within its target market, who themselves might share information with a "friend" over a social network; or a company can alert customers to the particular danger of a product, directly and rapidly, without the mainstream media acting as a middleman.

The appeal of social media, of course, is not limited to companies, as individuals enjoy an unprecedented increase in connectivity with friends, family, companies and co-workers, as well as the democratization of publication, as they now have access to a giant digital soapbox. Naturally, many of these individuals work for companies that are hoping to establish a social media presence and leverage these social networks into profits. Now, an employee who is only a novice computer user can easily maintain his or her own blogs or personal Facebook pages or post to the company Facebook page, and post to these pages from almost anywhere that Internet access exists, whether on a smart phone, a Blackberry, or a company-issued laptop. Most of the readers of this article probably maintain a profile on at least one of the social media platforms; Facebook, Twitter, LinkedIn, MySpace, or write a blog. Personal and work time continue to bleed further into one another with handheld and remote access. The ease and volume of connectivity make social networks powerful and potentially dangerous tools. It is at the intersection of these points where the wild frontier of social media in the law begins.

Statistics bear out that social media is here to stay and will become more firmly entrenched as a form of entertainment and communication. In an August 2010 survey, Nielsen found that social networking accounts for almost 23% of all Internet activity, with email accounting for 8.3% of Internet activity.[139] Between August 2008 and March 2009, Facebook increased from 100 million users to more than 200 million users.[140] According to Facebook.com, the total number of active users of Facebook had increased to more than 750 million by July 2011.[141]

Naturally, the workplace is not immune from the expansion of social networks. According to a recent survey by the Proskauer International Labor & Employment Group, 76% of businesses use social networking for business, and of those businesses, 45% do not have social networking policies.[142] A 2010 survey showed that half of all employees admitted that at least once a week they ignore corporate policies prohibiting social media in the workplace, and 27% said that they change settings on corporate devices to access prohibited applications.[143] Approximately 51% of the total workforce access Facebook at work for an average of 15 minutes per visit and two-thirds of those workers access Facebook during working hours.[144]

The proliferation of access to the Internet and the unassailable importance and growth of social networks has created a slew of issues for companies to address. Some of these issues are immediate and easy to grasp. Employers have to consider how access to and use of the Internet and social networks during work hours at the office affects the productivity of employees. Employers also must consider the computer security risks that arise when employees expose the company network to malware and viruses. And, of course, employers now

have to be aware of the legal implications of social media on their business. These legal issues are not limited to employee privacy.

Social media has created a new forum for familiar legal issues, such as discrimination, the Fair Credit Reporting Act, negligent hiring/retention, defamation, false advertising, and tortious interference. Naturally, the law has been slow to respond to the capabilities and challenges posed by social networks. Often times, a problem is not recognized until it already has become a problem. As a result, existing statutes and common law are going to be applied to litigation where social media is an issue. Until specific laws are passed or courts issue a consistent line of opinions, companies and their attorneys may be faced with uneven results when considering how to deal with social media. In the meantime, employers should consider how social media can implicate these long-standing legal concepts, and should establish and implement company policies to address these issues. This section is intended to highlight traditional legal concepts that could be implicated in the context of social media and the employer-employee relationship.

A. Employment Discrimination and Related Issues

Social networking websites could create a new breeding ground for claims of employment discrimination. These websites can be a tempting source of information for employers that are trying to cross-check an applicant's resume or check up on the activities of a current employee who has repeatedly called in sick. Viewing a social media page is a cheap, easy way of gathering large amounts of personal information about a prospective or current employee, often provided by the employee's own fingertips. A hiring employer can confirm information contained on a resume (for example, major; *alma mater*; and prior employer) and learn information not typically apparent from a piece of paper (gender; pregnancy; and religious affiliation, for example). Further, an employer can check up on current employees to see how they are promoting the company's products or services on social media.

Although this exercise could be mere benign fact-checking, the information observed by employers on social networking websites could support a claim of employment discrimination also. Consider that before the advent of social media, an employer would not necessarily be able to learn personal information about an applicant's sexuality or religious beliefs based upon an application or a résumé, or even perhaps an interview (certainly not without raising an applicant's suspicions). Now, an employer can learn about this sort of information with a few keystrokes and Google. Employers might access and consider this sort of personal information (even inadvertently) from social media when making hiring and firing decisions. In doing so, an employer could run afoul of numerous statutes and common law principles.

Employment lawyers and their clients undoubtedly are familiar with Title VII of the Civil Rights Act of 1964, which establishes that "[i]t shall be unlawful employment practice for an employer * * * to fail or refuse to hire or to discharge any individual, or otherwise to discriminate against any individual with respect to his compensation, terms, conditions, or privileges of employment, because of such individual's race, color, religion, sex, or national origin."[145] This principle has long been recognized in Illinois.[146] If a prospective employer learns an applicant's nationality from Facebook, and then decides not to hire the applicant because he was born in a Middle Eastern country, the applicant would have a potential claim against the employer based upon Title VII.

Employers are also surely familiar with the Americans with Disabilities Act of 1990[147] (ADA) and the Age Discrimination in Employment Act of 1967[148] (ADEA). The ADA protects individuals with disabilities and who are qualified to do a job from job discrimination on the basis of their disabilities.[149] If a prospective employer learns from a blog that an applicant suffers from a disability and then decides not to hire the applicant because of the disability *even though* that applicant is qualified to do the job, the applicant would have a potential claim against the employer based upon the ADA. The ADEA prohibits discrimination against current and prospective employees because of age and protects individuals over 40 years old.[150] If a prospective employer learns an applicant's birth date from MySpace, and then decides not to hire the applicant

because that applicant is over 40 years old, the applicant would have a potential claim against the employer based upon the ADEA.

In recent years, Congress enacted another law that protects prospective and current employees from discrimination based upon their genetic information. The Genetic Information Nondiscrimination Act of 2008[151] (GINA) prohibits an employer from discriminating "against an individual on the basis of the genetic information of the individual in regard to hiring, discharge, compensation, terms, conditions, or privileges of employment."[152] In an unusual moment of Congressional prescience, GINA also reaches into social media, as it also prohibits the deliberate acquisition of genetic information of an individual or a family member of the individual by "conducting an Internet search on an individual in a way that is likely to result in a covered entity obtaining genetic information" (although there are some exceptions to this general prohibition).[153]

As set forth above, it is easy to see how social media fits within the framework of these existing discrimination laws. But what must a plaintiff-employee do to prove employment discrimination? In Illinois, to establish a *prima facie* case of employment discrimination, the plaintiff must show that (1) he is a member of a protected class; (2) he was meeting his employer's legitimate business expectations; (3) he suffered an adverse employment action; and (4) the employer treated similarly situated employees outside the class more favorably than he.[154] A materially adverse employment action is "one that significantly alters the terms and conditions of the employee's job."[155] Adverse employment actions include situations such as denial of promotion, reassignment to a position with significantly different job responsibilities, or an action that causes a substantial change in benefits.[156] If a *prima facie* case is established, a rebuttable presumption arises that the defendant-employer unlawfully discriminated against the plaintiff.[157] To rebut the presumption, the employer must articulate—not prove—a legitimate, nondiscriminatory reason for the decision.[158] Then, if the employer articulates such a reason, the plaintiff, by a preponderance of the evidence, must prove that the employer's reason was untrue and was a pretext for discrimination.[159]

Once a plaintiff-employee establishes a *prima facie* case of an unfair employment practice, the burden shifts to the defendant-employer, who may demonstrate that even absent that prohibited motivation, it would have taken the same action against the complaining party for legitimate business reasons.[160] Merely proffering a legitimate business reason for the adverse employment action is not sufficient to end the inquiry, because it must be determined whether the reason advanced is *bona fide* or pretextual.[161] If the employer advances a legitimate business reason and is found to have relied upon that reason in its decision making, then the case is characterized as a dual-motive case, and the employer must demonstrate by a preponderance of the evidence that the employee would have been terminated notwithstanding the prohibited motive.[162]

In Illinois, a defendant-employer can be held liable for the wrongful actions of an agent that caused a plaintiff-employee's injury, even if the principal does not itself engage in any conduct in relation to the plaintiff.[163] Federal statutes also make employers liable for the discriminatory acts of their "agents," and supervisors are agents of their employers.[164] Illinois has a statute that holds employers responsible for harassment even if it results from conduct by non-employees and non-managerial staff if the employer is aware of the harassing conduct, and fails to take reasonable corrective measures.[165]

The application of these statutes in the social networking context is clear. Suppose an employee posts discriminatory statements about a co-worker on the employer's Facebook page, during work hours and using a company-issued computer. Or consider the situation where a company's salaried manager posts such statements about a subordinate on the manager's own webpage, which identifies the manager as an employee of the company. Under the above laws, an employer could find itself liable for the discriminatory conduct of its employees. Scenarios like those above could encourage employers to check up on the social networking pages of its employees, especially its supervisory or managerial personnel.

The impact of social media might be felt at the hiring stage or at the termination of the employer-employee relationship. An employer considering an applicant for employment might conduct informal background checks by reviewing social networking sites for pages maintained by the applicant. For example, a prospective employer looking to hire a new graduate might take a peek at his or her Facebook pages—only to find pictures

of the new graduate engaged in drunken collegiate revelry. Or, an employer might learn from Twitter that an employee attends meetings of a controversial religious group every Wednesday night. Similarly, an employer might learn that an applicant is genetically predisposed to a debilitating disease that could result in significant time off of work. An employer might consider the content of the social media described above and decide not to hire a particular applicant or to terminate an employee. By considering some of the information above in deciding not to hire an applicant or to terminate a current employee, an employer might expose itself to a potential claim of discrimination in violation of Title VII, the ADA, or GINA.

In a survey conducted by Cross Tab Marketing Services in December 2009, 79% of hiring managers and job recruiters in the United States had reviewed online information about a prospective employee.[166] This survey also found that 75% of U.S. companies had policies that required employees in charge of hiring to research applicants on the Internet.[167] There is no law that prohibits an employer from performing this kind of background check.[168] Nevertheless, employers who search social networking sites to perform a background check on an applicant should consider the risks of doing so. Employers should take care when searching social media websites for information about applicants, because they might learn information about the applicant's race, age, gender, sexual orientation, religious affiliation, genetic makeup, or disability, which could place the applicant within a protected class under federal or state law, and which could be used by a plaintiff to support a claim of employment discrimination.[169]

So, what if that company decides not to hire a particular applicant based in part on the content of a Facebook page or a Tweet? If that applicant were a member of a protected class and the decision not to hire the applicant was based, even in part, upon some discriminatory reason related to the content of a social media page, then an employer could have subjected itself to liability for employment discrimination. An employer must be able to articulate a legitimate, nondiscriminatory reason for its decision not to hire the applicant.

To avoid the appearance of discrimination and to provide support for this legitimate, nondiscriminatory reason, prospective employers should have a clear, consistent policy in place governing the use of information obtained from social media in hiring decisions. An effort should be made to instruct those employees tasked with hiring authority on how to uniformly obtain and consider information from social media. For example, if a manager has reviewed an applicant's Facebook page during the application and interview process, then it would be wise to document exactly what was reviewed and considered. In the event that this information forms even part of the basis for a decision not to hire a particular applicant, an employer should retain this information to support a legitimate business reason for its decision. Another option might be to assign an employee the job of reviewing and filtering an applicant's social networking information to a person other than the one making the hiring decision. This filter could minimize the appearance of any reliance on the information found on a social media page in regard to the applicant being a member of a protected class. Removing itself one step further, an employer might want to consider outsourcing this task to a company that specializes in performing these kinds of background checks and can sift through the content of an applicant's social networking pages for information that is useful to the prospective employer and not discriminatory. Clear procedures and documentary support of a legitimate, nondiscriminatory reason found in the social media relied upon when deciding not to hire an applicant could provide strong evidence against claims of discrimination.

Employers also might benefit by being up front with applicants about their intention to review social media content concerning the applicant. An employer could find out whether an applicant maintains a Facebook or LinkedIn account and let the applicant know that this information will be considered up front. Doing so could help establish a legitimate, nondiscriminatory reason for the decision not to hire from the start. Some employers, like the City of Bozeman, Montana, have gone so far as to ask applicants to consent, in writing, to an Internet-based background check and require applicants to provide their passwords to social network pages.[170]

Taking a slightly different approach, the Obama administration issued a seven-page questionnaire to individuals seeking high-ranking government positions, including 63 requests for information, including any

aliases or "handles" used by applicants on the Internet, any e-mails that might embarrass the president-elect, and any blog posts and links to Facebook pages.[171] Other employers might be tempted to surreptitiously access these pages by posing as a "friend," but there may be other dangers as well, besides the obvious ethical pitfalls.[172] A sound approach would be obtaining the consent of the applicant in advance and providing the applicant with a clear explanation of what will be searched and what information will be considered.

These same laws and considerations apply equally to terminating employees based upon social media content.[173] Just as with claims of discrimination in hiring, employers must be able to articulate a legitimate reason for terminating an employee. Employers that have a written contract with an employee should insert or incorporate existing policies into the contract which address how the content of a social media page will impact the status of his or her employment. An employer might be able to rely upon a moral clause in the contract to justify termination based upon the content of a social media page.

Of course, most employer-employee relationships are at-will, providing employers with greater latitude in termination decisions. Under Illinois law, an employee hired without a fixed term is presumed to be an at-will employee whose employment may be terminated for any cause or reason, provided the employer does not violate clearly mandated public policy.[174] Generally, an Illinois employer may fire an at-will employee for any or no reason.[175] As always, an employer must be able to articulate a *bona fide* legitimate business reason for terminating an employee to avoid liability for discrimination.[176] If an employer terminates an employee based upon the content of his or her social networking page, the employer should retain documents to support that legitimate business reason. Employers operating in states outside of Illinois should also be aware that some states have passed laws that prohibit employers from terminating employees for lawful off-duty activities.[177]

Because most employment is at-will, social media usage can be detrimental for the incautious employee. Even a cursory Google search yields numerous stories about employees fired for the content of their social networking pages. For example, in 2009, the Philadelphia Eagles fired employee Dan Leone for posting on his Facebook page that "Dan is [expletive] devastated about [former Eagles player Brian] Dawkins signing with Denver...Dam Eagles R Retarted!!"[178] Courts sitting in jurisdictions outside of Illinois have heard cases where employees were fired based upon e-mails or content posted on a social networking site.[179] While these are not cases of discrimination, they are powerful examples of how seemingly insignificant actions in the social media realm can affect the employment relationship, either resulting in termination or potentially litigation.

Although the situation for employers might seem dire—and in an abundance of caution they may be thinking of avoiding employees and applicant's social media pages altogether—individuals asserting discrimination claims still have to establish that they are members of a protected class, meet the employer's legitimate business expectations, and show that the employer relied upon a particular piece of information on a social networking page (such as religious affiliation or pregnancy) in violation of applicable law, among other things. If the employer has documented its hiring or firing decision, has a procedure in place concerning the use of social media in hiring and firing, and has documented the specific social media content relied upon in taking an adverse employment action that does not take into account characteristics of the plaintiff's alleged protected class, then the employer likely will have established strong evidence to support its defense.

B. Issues Related to the Fair Credit Reporting Act

Employers must not only be aware of discrimination issues when searching the content of an applicant's or current employee's social networking websites. They must also consider whether they are required to disclose the results of these searches under state or Federal consumer protection laws.[180]

In addition to the relatively new requirements of the IECPA (discussed above), employers also must consider the impact of the Fair Credit Reporting Act[181] (FCRA) on social media background checks of applicants. If an employer hires a company to perform a background check on an applicant, the company is subject to the requirements of the FCRA.[182] This background check could include a review of the applicant's

social networking pages, which could find its way into a consumer credit report. The FCRA regulates consumer credit reports, which are defined as follows:

> [A]ny written, oral, or other communication of any information by a consumer reporting agency, bearing on a consumer's credit worthiness, * * * general reputation, personal characteristics, or mode of living which is used or expected to be used or collected * * * for the purpose of serving as a factor in establishing the consumer's eligibility for * * * employment purposes.[183]

A consumer reporting agency is permitted to send a consumer credit report to "a person which it has reason to believe * * * intends to use the information for employment purposes."[184] A consumer report, however, may be provided for employment purposes only "if information from the consumer report will not be used in violation of any applicable Federal or State equal employment opportunity law or regulation."[185] To obtain an applicant's consumer credit report, a prospective employer must first obtain the written authorization of the applicant or in those cases where "a clear and conspicuous disclosure has been made in writing to the [applicant] at any time before the report is procured."[186] If the employer makes an adverse decision, such as denying employment, based on the report, the employer must disclose it to the applicant.[187]

Based upon the provisions discussed above, it is easy to see how a consumer report that includes a search of an applicant's or a current employee's social networking pages prepared by a reporting company could run afoul of the FCRA, such as an employer declining to hire an applicant or terminating an employee because the consumer report contained information from the applicant's or current employee's Facebook page that the individual did not pay his or her bills on time. If an employer makes this kind of adverse employment decision based upon the report, then the employer must disclose the basis for the decision to the individual.

C. Negligent Supervision/Hiring

Social media has created another dilemma for employers: how much checking up on a current or prospective employee's social media content must they do when making hiring and firing decisions, in order to discover information that if known should be acted upon to avoid liability in certain situations? An employer may find itself liable for failing to check on an applicant or current employee and ultimately get sued for negligent hiring or supervision, where a plaintiff alleges that a defendant-employer knew or should have known about an applicant's or a current employee's violent propensities or discriminatory views on race. In Illinois, claims for negligent hiring and negligent retention require a plaintiff to establish the following: 1) that the employer knew or should have known that the employee had a particular unfitness for the position so as to create a danger of harm to third persons; (2) that such particular unfitness was known or should have been known at the time of the employee's hiring or retention; and (3) that this particular unfitness proximately caused the plaintiff's injury.[188] Social media pages containing information about an employee's propensities provide plaintiff's with strong arguments that an employer knew or should have known of these propensities.

But the question remains: to what extent must an employer attempt to gain such information? The current state of the law is unclear. An employer, however, must keep in mind the legal pitfalls and risks associated with surreptitiously obtaining such information, as discussed above. Further, employers must weigh the risks of requiring employees and applicants to allow the employer access to otherwise private social networking pages that might reveal information upon which employment decisions cannot be made versus the benefit of being able to review those pages for information that would allow an employer to prevent or to better defend against a negligent hiring or negligent retention claim.

In the right situation, the employer very well could find itself in a "Catch 22" of sorts. An employer could be sued by the very employee it terminated or by the applicant it refused to hire in order to avoid a potential negligent retention or negligent hiring claim, because in addition to the information contained on the social networking site that led to the adverse decision, the site also disclosed information about the person's religious

affiliation and the person against whom the action was taken is claiming discrimination. On the other hand, if the person's actions led to a negligent hiring or a negligent retention claim against the employer, and the employer failed to request access to the site, the employer could be held liable under certain circumstances for not knowing the information about the person when it reasonably should (and could) have. Because of the easy availability of information on the Internet about prospective and current employees, a free, fast search of social media to check up on a prospective or current employee, might be convenient, but nonetheless risky. Designating an individual to perform this function and providing specific guidelines for this function could be the best way for employers to protect themselves from falling victim to claims of negligent hiring or retention.

D. Defamation

Another area of concern for employers is the posting of defamatory content via social media by employees. The very real potential exists for employers to defame competitors, fellow employers or even customers via social media. In Illinois, to establish defamation, a plaintiff must show that the defendant: (1) made a false statement about the plaintiff; (2) made an unprivileged publication of that statement to a third party; and (3) damaged the plaintiff by publishing the statement.[189] An allegedly defamatory remark is "published" when it is communicated to someone other than the plaintiff, including internal communication within a company.[190] Two categories of defamation *per se* are particularly relevant in the context of employment law: (a) words that impute an inability to perform or a lack of integrity regarding the plaintiff's office or employment duties; and (b) words that prejudice the plaintiff or allege lack of ability in his or her trade, profession, or business.[191]

The ease, speed, and breadth of communication over social networks means that employees can publish defamatory statements with a few keystrokes and in a moment's time. The individual employee who posts the defamatory statement is not the only potentially liable party. If management signed off on the content of the employee's post, then the company also might be exposed to potential liability for defamation. A straightforward solution to this problem would be for employers to prohibit employees from posting anything on the company website, on social networking sites, or elsewhere that purports to have been approved by the company.

The defamation lawsuit brought by clothing designer Dawn Simorangkir against musician and actor Courtney Love is a good example of the defamatory potential of social networks. Simorangkir sued Love in Los Angeles Superior Court for libel, among other things, based upon MySpace and Twitter posts by Love. The posts included various accusations about Simorangkir, such as a history of assault, burglary, and dealing cocaine. Love settled the lawsuit in March 2011, and paid Simorangkir $430,000.[192] Shortly after settling the Simorangkir suit, Love was named as a defendant in another lawsuit brought by her former attorney, Rhonda Holmes.[193] Love had hired Holmes to recover money that she believed had been stolen from her late husband Kurt Cobain's estate, but terminated the relationship.[194] Love attempted to rehire Holmes, but Holmes declined. Love wrote via Twitter that "I was f---ing devastated when Rhonda J Holmes Esq of San Diego was bought off."[195] Love may have posted these statements in fits of anger. Love "published" these allegedly false statements by posting to her social media pages—a simple act that could be accomplished by a computer novice. Unfortunately for her, there was no way to retract her statement, once she clicked the "send" button, thereby "publishing" the statement to her presumably large following on social media. The simplicity of this damaging act highlights the challenge for employers attempting to avoid claims of defamation. Again, employers should consider seriously establishing and implementing policies that limit or prohibit unauthorized posts by employees within the scope of their employment or purporting to have been ratified by the employer.

E. False Advertising

Besides what employees are tweeting about other individuals or competitors, employers should be aware of what their employees are saying about the company's own products or services over social networks. The FTC has put in place new guidelines that govern the use of endorsements and testimonials in advertising.[196]

These guidelines make it clear that employees endorsing their employer's products or services have a duty to disclose to their audience their relationship to an employer at the time they give the endorsement or testimonial.[197] This duty is applicable even if an employee posts the testimonial or endorsement on a personal blog, as opposed to a website created and maintained by the employer.[198] Employers could face fines of up to $11,000.00 for each violation of these new provisions.[199] These new guidelines may inspire employers to designate an employee to scour the Internet for postings by employees. In light of these penalties, an employer should establish a policy that governs the posting of information online about the company, and may want to prohibit such posts without express, written authorization from a designated supervisory employee on behalf of the company.

F. Tortious Interference

Employers should also be aware of the potential impact of social media on existing and potential business relationships. In Illinois, there are two relevant legal concepts in this regard: tortious interference with a contractual relationship, and tortious interference with a prospective economic advantage. In a claim for tortious interference with a contractual relationship, plaintiff must establish the following: "(1) the existence of a valid and enforceable contract between the plaintiff and another; (2) the defendant's awareness of the contract; (3) the defendant's intentional and unjustified inducement of a breach of the contract; (4) a subsequent breach by the other, caused by the defendant's conduct; and (5) damages."[200] For a plaintiff to prevail on a claim for tortious interference with prospective economic advantage, he must establish the following: (1) a reasonable expectancy of entering into a valid business relationship; (2) the defendant's knowledge of the expectancy; (3) an intentional and unjustified interference by the defendant that induced or caused a breach or termination of the expectancy; and (4) damage to the plaintiff resulting from the defendant's interference.[201]

Just as with defamatory content or false advertising, statements that could induce the breach of a contract could be posted by an employee to Facebook or Twitter and distributed within seconds, causing a customer to try to get out of a contract or even avoid entering into a contract with the employer. In another scenario, imagine if a key employee who is privy to sensitive information intentionally posts that information to his Twitter account and ends up preventing a competitor-company from getting a big, new contract. The employer could find itself faced with a claim of tortious interference with prospective economic advantage, if the employee was acting within the scope of his or her employment. Again, employers should establish a policy that governs posting information online about the company, as well as about its customers and competitors.

G. Other Issues

As social media continues to fortify its presence in the mainstream, the legal issues facing employers will get fleshed out in the courts and the legislatures. Of course, other issues will arise as the full impact of social media becomes known in our daily lives and in the law. Social media may affect jurors, as it will allow them to engage in real time communication about the trial, to disclose potentially sensitive trial information, or perhaps to communicate (even unintentionally) with attorneys, witnesses, and parties to lawsuits.

Social media also could have an impact on class action lawsuits. It can provide plaintiff's attorneys with an inexpensive and effective method for obtaining class representatives and to swell the size of class membership.[202] By creating a social networking page, a plaintiff's attorney has more efficient, cheap access to potential plaintiffs than the limitations of print media, radio, and television would allow. Potential plaintiffs actually might search for keywords that lead them to the plaintiff's attorney's webpage, or a link to the attorney's webpage could be circulated until it finds the appropriate plaintiff or group of plaintiffs.

An entirely new area of discovery has been opened up with the proliferation of social media. Now, parties to lawsuits inquire about websites, blogs, and web pages maintained by their opponents. They might have to

subpoena the website provider to obtain information about their opponent's web postings. The classic example is of the plaintiff who claims severe injuries that prevent him from doing his favorite activities (say, golf, for example), but whose MySpace page boasts of his recent big weekend on the golf course with his friends. Clearly, defense attorneys treasure these kinds of finds, and for the plaintiff's attorney these postings are a nightmare.[203] For their part, employers must take steps to preserve the content of their social media pages once litigation is threatened. If that litigation concerns an employer's social media in any way, preservation is essential to avoiding a claim for spoliation of evidence.[204] An employer should work with its technology department to implement a policy to preserve evidence related to the company's social media in connection with a litigation hold, should a suit be threatened or filed.

H. Suggestions for Employers

Realistically, employers cannot keep track of all social networking activity by employees or anticipate all of the legal issues that could arise. Policing the web for discriminatory or defamatory content posted by employees could be enormously time consuming and likely very expensive; so too could training employees about how to utilize social media content in hiring and firing decisions. Employers must measure these costs against the costs of potential liability that may result from social media content on the Web.

All is not lost for employers, however. A written internal policy is a cost effective and straightforward method for reducing liability risks associated with social media. Establishing a clear policy now could prove to be useful later, when an employer is faced with a discrimination or defamation lawsuit. If an employer terminates an employee based upon social media, a clear, even-handed policy in an employee handbook could serve as powerful evidence of a legitimate business interest for an employer. Similarly, a policy requiring written authorization for posting could be a defense to claims of agency between an alleged defaming employee and the employer.

Some changes can be made based upon existing policies. For example, if an existing employee handbook contains an anti-harassment policy, you could recommend that the employer add a few sentences to make clear that the anti-harassment policy includes activity on social media. Otherwise, employers should consider incorporating some of the following guidelines and principles into their employee handbooks:

- Prohibit or limit employees from including corporate logos, service marks, and trade marks on their social networking pages, unless given specific, written authorization permitting them to do so;
- Prohibit or limit employees from mentioning the company on their social networking pages, unless given specific, written authorization permitting them to do so;
- Incorporate use of social media into existing harassment, discrimination, confidentiality, and other company policies;[205]
- Require a written acknowledgement by employees that they are responsible for the content of their Internet postings during work hours, when using employer-owned computers and smart phones, and whenever their posting associates them in any way with the employer (including any private page that specifically identifies them as an employee of the company);
- Limit employee access to social media during the scope of work and when using employer-provided equipment;
- Prohibit employees from using their work email addresses when signing up for or creating social media pages;[206]
- Require employees to post a disclaimer that any commentary posted on social media pages are those of the individual and not the employer, in the event that an employee does identify his or her employer on his or her social networking page;[207]
- Establish that any unauthorized social media content about the company posted by employees will be considered a posting on the employee's "personal time;"[208]

- Make sure that employees are informed that a violation of the company's social networking policy could lead to discipline, including termination;[209]
- Enforce the policy.

IV. The National Labor Relations Act

The National Labor Relations Act[210] (NLRA) was enacted in 1935 for the purpose of protecting the rights of employees and curtailing certain private sector labor and management practices that discouraged organization of employees.[211] Its history is tied to the unionization of the workplace. The rate of union membership, however, has been on a steady decline over the past 25 years.[212]

The NLRA creates the National Labor Relations Board (NLRB), and authorizes the NLRB to carry out and enforce the provisions of the act.[213] The NLRB is to be comprised of five members.[214] During a 27-month period from January 1, 2008 until March 27, 2010, however, three seats were vacant. In June 2010, the United States Supreme Court held that two members of the NLRB are not permitted to exercise the NLRB's authority.[215] The Court concluded that a quorum of at least three members is required for NLRB decisions, according to § 153(b) of the NLRA.[216] At that time, a large number of cases were pending on appeal in the federal courts and were returned to the NLRB for consideration by at least a three-member panel.

Amidst much controversy, President Barack Obama exercised recess appointments to place Craig Becker and Mark Pearce on the NLRB in March 2010. There were strong opinions concerning the appointment of Craig Becker, whose nomination had been rejected previously by the Senate.[217] The NLRB currently consists of three members: Chairman Mark Pearce, Craig Becker, and Brian Hays.[218] President Obama has nominated Terence Flynn to fill the vacant seat and has re-nominated Craig Becker.[219] Member Becker's term expires December 31, 2011.[220]

As of the writing of this Monograph, Lafe Solomon is serving as Acting General Counsel.[221] The general counsel is independent from the NLRB and is responsible for investigation and prosecution of unfair labor practice cases, as well as supervision of NLRB field offices.[222] Since his appointment, the general counsel's office has issued several memoranda to the regional directors, which instruct them on several important topics, such as pursuing remedies and including default language in settlement and compliance agreements.[223] These Memoranda appear to demonstrate a desire for the Regional Directors to be more aggressive in their approach with unfair labor practices.

A. Change in Focus

Although the number of unionized workers is decreasing, the NLRB and General Counsel remain active and appear to be expanding their authority in the area of unfair labor practices. On August 30, 2011, the NLRB published a Final Rule in the *Federal Register*, requiring that employers post a notice of NLRA rights in the workplace.[224] As the NLRA applies to most private employers,[225] this requirement will have significant impact. The proposed posting would identify employee rights under the NLRA and give employees information on where to file charges. In conjunction with the proposed rule are severe sanctions imposed for failure or refusal to post the notice. The sanctions include an independent violation of the prohibition of the employer's interference with employees' exercise of the right to engage in certain protected activities, resulting in an unfair labor practices charge, and the possibility that failure to post a notice of rights is found to be evidence of antiunion animus.[226] Further the Final Rule mandates that non-compliance might toll the statute of limitations for filing unfair labor practice charges, exposing employers to complaints that otherwise would

have not been timely filed, unless the complaining employee, despite the failure by the employer to post a notice of rights, had actual or constructive notice that the employer's conduct complained of is unlawful.[227]

More significantly, the NLRB arguably is expanding its authority through the interpretation of the rights afforded by the NLRA. One area of recent insurgence involves an employee's use of social media, in particular the social networking site, Facebook. The NLRB has begun pursuing employers for terminations of employees for their use of Facebook.[228]

The social media cases involve the interpretation of Section 7 of the NLRA.[229] Section 7 of the NLRA states as follows: "Employees shall have the right to self-organization, to form, join, or assist labor organizations, to bargain collectively through representatives of their own choosing, and to engage in other concerted activities for the purpose of collective bargaining or other mutual aid or protection * * * *"[230]

As it relates to social media, the terms "concerted activity" and "other mutual aid or protection" are the most important. The definition of "concerted activity" has long been the subject of case law. The term itself implies activity by or on behalf of more than one person. There are several social media cases identified by the General Counsel in which the employee's activity in using social media did not rise to the level of "concerted activity."[231] The NLRB's test is whether the activity is engaged in with or on the authority of other employees, and not solely by and on behalf of the employee himself.[232] The NLRB looks at whether the employee had discussed postings with his co-workers, whether responses were posted by co-workers, and whether there were attempts to initiate group action. In the cases in which the NLRB did not find concerted activity, the postings consisted of gripes or comments about what happened during work, but did not engage in any group discussion.[233]

"Mutual aid or protection" traditionally has been interpreted as meaning that the employee's comments must in some way be tied to the terms and conditions of employment in order to be protected.[234] As discussed below, "terms and conditions of employment" has been broadly interpreted to include everything from complaints about a supervisor to the type of food served to potential buyers of luxury automobiles. The NLRB's pursuit of cases involving social media began with the matter involving American Medical Response of Connecticut, Inc. This section reviews that case and the others involving Facebook that have followed, including the first of the Facebook cases to be decided by an Administrative Law Judge after a hearing.

1. American Medical Response of Connecticut, Inc.

On November 2, 2010, the Office of General Counsel of the NLRB issued a press release concerning its complaint against American Medical Response of Connecticut, Inc (AMR), alleging that AMR illegally fired an employee over Facebook comments.

The employee was a union employee who was on Facebook at her home computer when she posted negative remarks about her supervisor on her personal Facebook page. The posting drew responses from co-workers, which led to further negative comments by the employee. According to the press release, AMR terminated the employee for her Facebook postings, because they violated the company's Internet policies.[235] The NLRB took the position that the Facebook postings constituted protected concerted activity under the NLRA.[236] Ultimately, the matter settled, with AMR agreeing to not discipline or discharge employees for discussing their wages, hours, and working conditions.[237]

2. Build.com

On April 27, 2011 the NLRB issued a news release that it had approved a settlement with Build.com concerning a complaint alleging that an employee was terminated for having posted comments about Build.com, which drew responses from other employees.[238] Unlike the AMR complaint, these employees were not represented by a union.[239] As part of the settlement, the employer agreed to post a notice stating that

employees have the right to post comments about terms and conditions of employment on their social networking pages without fear of punishment.[240]

3. Knauz BMW

Among the more significant complaints that evidence the NLRB's expansion of its authority is the recent issuance of a complaint by the NLRB against Knauz BMW (Knauz), a Chicago area dealership. In 2011, Knauz terminated car salesman Robert Becker for allegedly writing posts to his Facebook page that criticized the dealership, specifically for the quality of the food and beverages provided at an event promoting a new BMW model.[241] Those comments essentially criticized the boss for being cheap in providing customers only hot dogs and water at a sales event.[242] Other Knauz employees had access to Becker's Facebook page and expressed concern that the quality of the food and beverages at the event could have a negative effect upon their sales and commissions.[243] Becker removed the posts at the request of his employer, but nevertheless was fired a few days later.[244]

On May 24, 2011, the NLRB advised that a complaint had been filed against Knauz, alleging unlawful termination of an employee for posting photos and comments on Facebook that were critical of the dealership.[245] The complaint further alleged that the dealership fired Becker to discourage other employees from engaging in similar discussions about their wages and the conditions of their employment, which would violate the NLRA.[246]

The *Chicago Tribune* characterized the NLRB's position in the Knauz case as a sharp turn against employers.[247] The *Tribune* points out that posting on a social networking page is not the equivalent of water cooler conversation that the NLRB is trying to protect, but rather is more akin to a publication of the comments, because of the potential reach of Facebook and social media.[248]

Nevertheless, the NLRB has held firmly its position that Facebook comments are a discussion of the terms and conditions of employment. The NLRB takes the position that the nature of the comments will not cause them to lose protection under the NLRA.[249] Certainly, it is anticipated that subject of the comments posted on Facebook will be an issue at the hearing in this case, which has not occurred as of the writing of this Monograph.

4. Hispanics United of Buffalo

The NLRB continues to advise of new complaints issued concerning employee activity on Facebook. Its press release of June 28, 2011, tells of a complaint issued in New York against Hispanics United of Buffalo (HUB).[250] HUB purportedly fired five employees who participated in Facebook exchanges relating to working conditions, work load, and staffing levels.[251] This Facebook case when before an Administrative Law Judge (ALJ), and is the first to have resulted in an ALJ decision following a hearing.[252]

In the first ruling of its kind, the ALJ found that the discharge of the employees was unlawful.[253] Because the ALJ determined that the employees' discussion on Facebook was protected concerted activity involving a conversation amongst coworkers about their terms and conditions of employment, the ALJ found HUB to be in violation of Section 7 of the NLRA.[254] HUB was ordered to reinstate the five employees, who were awarded backpay.[255] The company also was required to post a notice at its facility, concerning employees' rights under the NLRA and the violations found by the ALJ.[256]

5. Bay Sys Technologies LLC

A complaint was issued against Bay Sys Technologies LLC (Bay Sys) concerning an employee's termination and the employee's Facebook activity. Bay Sys withdrew its answer and the NLRB issued a decision granting the Acting General Counsel's Motion for Default Judgment on August 2, 2011.[257] The

employees had posted comments to other employees' Facebook pages on the website about the company not having issued their paychecks on time. A newspaper then published the Facebook conversation. In its decision, the NLRB listed conduct that it held violated the NLRA in that it interfered with employees rights to engage in protected concerted activity guaranteed under Section 7 of the NLRA.[258] The conduct cited by the NLRB included the following: expressing disappointment that employees took complaints to a newspaper, telling employees that they breached their nondisclosure agreements, threatening employees with legal action, implying that employees would be discharged unless they took certain action, questioning employees regarding their activity, and telling employees they should find another job if they had complaints.[259]

B. Concerted Activity and Mutual Aid or Protection in the Context of Social Media

The social media cases pursued by the NLRB have involved a posting by one employee with responses from other employees or postings by several employees. The analogy put forth by the NLRB is that these postings are essentially conversations by employees facilitated by the use of social media, and thus qualifies as "concerted activity." Being analogous, however, does not mean that they are the same. Certainly, there are implications triggered by posting on a social networking site that are not present in any other setting. In particular, the sheer number of persons with access to the information is substantially different than "water cooler talk," for example, and is significantly so.

Although the term "mutual aid or protection" suggests that comments must in some way be tied to the terms and conditions of employment in order to be protected, the position of the NLRB in the *Knauz* case suggests that the NLRB will be taking an expansive view on the definition of the term.[260] In broad strokes, the NLRB appears to be concluding that most complaints will implicate terms and conditions of employment and thus will be within the protections afforded by the NLRA. Although a memorandum from the General Counsel identifies cases in which the NLRB did not find "protected concerted activity" in postings on social networking sites, those cases tended to be related more to the question of whether there was group involvement in the postings than the type of complaint that was posted.[261] Therefore, the NLRB appears to be placing greater emphasis on whether social networking posts are triggering a response than on the content of the postings. This application of the NLRA to social media should trouble employers and their counsel alike.

C. Suggested Employer Practices, in Light of Recent Trends within the NLRB

Employers would be wise to update their policies to reduce the potential for violations of the NLRA. In particular, employers should review their Internet usage policies to ensure that their policies are not overly broad. In the matter involving AMR, the company's Internet use policy prohibited making disparaging comments regarding the company or depicting the company in any way on the Internet without the company's permission. The NLRB took the position that AMR's policy interfered with an employee's right to engage in protected concerted activity on its face.[262]

All policies requiring the employer's permission to discuss work or the workplace online should be revised and amended to ensure compliance with the NLRA's granting of the right to participate in concerted activity for the purpose of mutual aid or protection. Insight into the General Counsel's analysis of policies can be found in the office's official memorandum concerning social media cases.[263] That memorandum certainly suggests that an employer's policies should be written narrowly and should restrict only that which is necessary to serve a legitimate business interest. Policy statements, such as prohibitions against posting of confidential information, might be found to be overly broad, given the NLRB's current trends. Merely prohibiting disclosure of "confidential information," for example, might be insufficient to avoid liability under the NLRA. Consequently, employers should define in their policies what constitutes the "confidential information" that is not to be disclosed. Any policy that attempts to restrict employees from discussing their employment using social media will be a violation.

As noted in the *Bay Sys Technologies* decision, the NLRB reprimanded the employer for merely suggesting the possibility of a breach of their non-disclosure agreement when questioning the employee's actions.[264] In light of the NLRB's approach, employers should review their non-disclosure agreements as well as any confidentiality policies. Non-disclosure agreements and confidentiality policies should not be overreaching and should be based on a sound business purpose that does not interfere with the employees' ability to discuss the terms and conditions of their employment. The employer's desire to maintain confidentiality must be tempered with the employees' rights to engage in protected concerted activity under the NLRA.

In addition to reviewing and re-writing policies, an employer might consider adopting a policy that affirmatively states that the company complies with the NLRA and all other federal, state, and local laws, and that no company policy is intended or would be enforced for the purpose of preventing or restricting any activity protected by the NLRA.

Lastly, and perhaps most importantly, is the need for employers to educate management on any changes in their policies and approaches to situations involving employees engaged in the use of social media. Social media continues to grow and expand rapidly. To thrive and survive, employers will need to be prepared to address the problems that social media could cause in the workplace in a manner that is consistent with the NLRA.

V. Conclusion

Employers may look at their employees' social networking sites and postings. But doing so is not without risk to the employer. Finding particular pieces of information about an employee or a potential employee could trigger serious legal consequences for an employer under certain circumstances, given the variety of both well-known and lesser-known laws potentially applicable to the interplay between social media and the workplace. Employers and their counsel should consider whether viewing or monitoring employees' social network postings is worth the risk of exposure to legal liability. If viewing or monitoring such postings is worth the employer's risk, then the employer should consider whether the use of a third-party to filter out the type of information that can lead to legal problems is a viable option for that employer. Finally, although having written policies regarding employees' use of social media and disclosing the fact that such use will be monitored, employers and their counsel must be sure to draft policies that are not so overbroad that they interfere with employees' rights under federal statutes, with the rights afforded under the NLRA being of significant concern.

(Endnotes)

1 *See generally O'Connor v. Ortega*, 480 U.S. 709 (1987) (holding that teachers have no reasonable expectation of privacy in communications in their classrooms, as required to challenge audio monitoring under the Fourth Amendment to the Unites States Constitution, U.S. Const. amend. IV).

2 An employee's expectation of privacy in material stored in an office computer depends upon the employer's policy regarding computer use and any other relevant office practices, procedures, and regulations. *See, e.g., United States v. Angevine*, 281 F.3d 1130, 1134-35 (10th Cir. 2002).

3 Ill. Const., Art. I, § 6.

4 Ill. Const., Art. I, §§ 6, 12.

[5] *People v. Smith*, 72 Ill. App. 3d 956, 964, 390 N.E.2d 1356 (1st Dist. 1979) (challenging the sufficiency of a warrant based in part on monitoring conducted by the phone company to determine if the defendant had been defrauding the phone company, alleging the monitoring was an invasion of his privacy under the Illinois constitution).

[6] *Dafour v. Mobile Oil Corp.*, 301 Ill. App. 3d 156, 161, 703 N.E.2d 448 (1st Dist. 1998).

[7] *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (analyzing U.S. Const. amend. IV); *see also People v. Neal*, 109 Ill. 2d 216, 486 N.E.2d 898 (1985); *Thornton v. University Civil Service Bd.*, 154 Ill. App. 3d 1016, 507 N.E.2d 162 (5th Dist. 1987).

[8] *Neal*, 109 Ill. 2d at 216; *Thornton*, 154 Ill. App. 3d at 1016.

[9] 820 ILCS 40/0.01, *et seq.*

[10] 820 ILCS 40/9.

[11] 820 ILCS 40/12.

[12] 820 ILCS 40/9.

[13] 820 ILCS 55/1, *et seq.*

[14] 820 ILCS 55/5(a).

[15] 820 ILCS 55/5(b); s*ee also* 820 ILCS 55/5(c); 820 ILCS 55/20.

[16] Kim L. Kirn, *Workplace Privacy in Illinois: A Review*, 83 Ill. B.J. 454, 457-58 & n.53 (1995) (citing Right to Privacy in the Workplace Act, Senate floor debate on HB 1533, House Amendment Number 1, offered May 1, 1991).

[17] 820 ILCS 305/1, *et seq.*

[18] 820 ILCS 310/1, *et seq.*

[19] 820 ILCS 55/10; *Carter v. Tennant Co.*, 383 F.3d 673 (7th Cir. 2004).

[20] 820 ILCS 55/15(c) & (f).

[21] 820 ILCS 55/15(e) & (f).

[22] 720 ILCS 5/14-1, *et seq.*

[23] 720 ILCS 5/14-1(a).

[24] 720 ILCS 5/14-2; *see also* The Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-2522.

[25] 720 ILCS 5/14-6.

[26] 720 ILCS 5/14-5.

[27] 775 ILCS 5/1-101, *et seq.*

[28] 775 ILCS 5/2-103.

[29] 775 ILCS 5/2-103(b); *C.R.M. v. Chief Legal Counsel of Ill. Dep't of Human Rights*, 372 Ill. App. 3d 730, 866 N.E.2d 1177 (1st Dist. 2007).

[30] 775 ILCS 5/2-104(c)(3).

[31] 820 ILCS 70/1, *et seq.*

[32] 820 ILCS 70/10.

[33] 820 ILCS 70/5.

[34] 820 ILCS 70/10(b)(1)-(7).

[35] *Melvin v. Burling*, 141 Ill. App. 3d 786, 789, 490 N.E.2d 1011, 1013–14 (3d Dist. 1986) (citing W. Prosser, Torts § 112, at 832-34 (3d ed.1964)); see also W. Keeton, Prosser & Keeton on Torts § 117, at 854–67 (5th ed.1984).

[36] *Burns v. Masterbrand Cabinets*, 369 Ill. App. 3d 1006, 874 N.E.2d 72 (4th Dist. 2007).

[37] *Benitez v. KFC Nat'l Mgmt Co.*, 305 Ill. App. 3d 1027 (2d Dist. 1999).

[38] *Cordts v. Chicago Tribune Co.*, 369 Ill. App. 3d 601, 603, 860 N.E.2d 444, 447 (1st Dist. 2006).

[39] *Cordts*, 369 Ill. App. 3d at 603.

[40] *Miller v. Motorola, Inc.*, 202 Ill. App. 3d 976, 560 N.E.2d 900 (1st Dist. 1990).

[41] *Salamone v. Hollinger Int'l, Inc.*, 347 Ill. App. 3d 837, 844, 807 N.E.2d 1086, 1093 (1st Dist. 2004).

[42] *Kuwik v. Starmark Star Mktg. & Admin.*, 156 Ill. 2d 16, 26-29, 619 N.E.2d 129, 133-35 (1993).

[43] *Larson v. Decatur Mem'l Hosp.*, 236 Ill. App. 3d 796, 799, 602 N.E.2d 864 (4th Dist. 1992).

[44] *Kuwik*, 156 Ill. 2d at 30.

[45] *Goldberg v. Brooks*, 409 Ill. App. 3d 106, 110, 948 N.E.2d 1108, 1113 (1st Dist. 2011).

[46] 820 ILCS 405/1900.1.

[47] *Vickers v. Abbott Labs.*, 308 Ill. App. 3d 393, 410, 719 N.E.2d 1101, 1115 (1st Dist. 1999).

[48] 745 ILCS 10/1-101.

[49] *Id.*

[50] *Id.*

[51] The Privacy Act of 1974, 5 U.S.C. § 552a.

[52] *Id.* § 552a(a)(4).

[53] *See id.* § 552a(f).

[54] *Id.* § 552a(b).

[55] *Id.* § 552a(b)(1)-(12).

[56] *Id.* § 552a(b)(11).

[57] Electronic Communications Privacy Act, 18 U.S.C. § 2510.

[58] *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 874 (9th Cir. 2002).

[59] 18 U.S.C. § 2511(1)(a)-(e).

[60] *Id.* § 2510(12)(A)-(D).

[61] *Id.* § 2510(17)(A)-(B).

[62] *U.S. v. Councilman*, 418 F.3d 67 (1st Cir. 2005).

[63] *Id.* at 79-81.

[64] *See Konop*, 302 F.3d at 874; Miguel Helft and Claire Cain Miller, *1986 Privacy Law is Outrun by the Web*, The New York Times, Jan. 9, 2011, http://www.nytimes.com/2011/01/10/technology/10privacy.html?_r=1&hp=&pagewanted=all (last visited August 12, 2011).

[65] Stored Communications Act, 18 U.SC. § 2701, *et seq*.

[66] *Id.* §§ 2702-2703.

[67] *Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965, 972 (C.D. Cal. 2010) (citing Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1209-13 (2004)).

[68] *Id.* (citing 18 U.S.C. §§ 2702-2703).

[69] *Devine v. Kapasi*, 729 F. Supp. 2d 1024, 1028-29 (N.D. Ill. 2010).

[70] 18 U.S.C. § 2510(15).

[71] *Crispin*, 717 F. Supp. 2d at 980-82, 989.

[72] 18 U.S.C. § 2702(a)(1), (b).

[73] *Id.* § 2711(2).

[74] *Id.* § 2510(14).

[75] *Id.* § 2702(a)(2).

[76] *Id.* § 2702(a).

[77] *Id.* § 2703(a).

[78] *Id.* § 2703(b).

[79] *Crispin*, 717 F. Supp. 2d at 975.

[80] *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (9th Cir. 2002).

[81] *Konop*, 302 F.3d at 872-73, 879.

[82] *Id.* at 879-80.

[83] *U.S. v. Szymuszkiewicz*, 622 F.3d 701 (7th Cir. 2010).

[84] *Szymuszkiewicz*, 622 F.3d at 703.

[85] *Id.* at 706.

[86] *Id.*

[87] *Pure Power Boot Camp v. Warrior Fitness Boot Camp*, 587 F. Supp. 2d 548 (S.D.N.Y. 2008).

[88] *Pure Power Boot Camp*, 587 F. Supp. 2d at 551.

[89] *Id.* at 551-52, 554.

[90] *Id.* at 555 (citing *U.S. v. Councilman*, 418 F.3d 67, 79 (1st Cir. 2005)).

[91] *Id.* at 559-60.

[92] *Id.* at 560.

[93] *Id.* at 570.

[94] *Pure Power Boot Camp*, 587 F. Supp. 2d at 561.

[95] *Id.* at 562.

[96] *Id.* at 571.

[97] *Id.* at 556-57.

[98] *Id.* at 558.

[99] *Shefts v. Petrakis*, 758 F. Supp. 2d 620 (C.D. Ill. 2010).

[100] *Shefts*, 758 F. Supp. 2d at 626.

[101] *Id.*

[102] *Id.*

[103] *Id.* at 630 (citing *U.S. v. Szymuszkiewicz*, 622 F.3d 701 (7th Cir. 2010)).

[104] *Id.*

[105] *Id.* at 631.

[106] *Shefts*, 758 F. Supp. 2d at 631.

[107] *Id.* at 635.

[108] *Id.*

[109] *Id.*

[110] *Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965 (C.D. Cal. 2010).

[111] *Crispin*, 717 F. Supp. 2d at 968.

[112] *Id.*

[113] *Id.* at 989.

[114] *Id.*

[115] *Id.* at 989-90.

[116] *Id.* at 991.

[117] *Mackelprang v. Fidelity Nat'l Title Agency*, No. 2:06-cv-00788-JCM-GWF, 2007 U.S. Dist. LEXIS 2379 (D. Nev. Jan. 9, 2007).

[118] *Mackelprang*, 2007 U.S. Dist. LEXIS 2379, at *2.

[119] *Id.* at *5.

[120] *Id.*

[121] *Id.*

[122] *Id.* at *6.

[123] *Id.* at *25.

[124] *Mackelprang*, 2007 U.S. Dist. LEXIS 2379, at *7.

[125] Fed. R. Evid. 412 (entitled: Sex Offense Cases; Relevance of Alleged Victim's Past Sexual Behavior or Alleged Sexual Predisposition).

[126] *Mackelprang*, 2007 U.S. Dist. LEXIS 2379, at *7.

[127] *Id.* at *18.

[128] *EEOC v. Simply Storage Mgmt, LLC*, 270 F.R.D. 430 (S.D. Ind. 2010).

[129] *Simply Storage Mgmt, LLC*, 270 F.R.D. at 432.

[130] *Id.*

[131] *Id.*

[132] *Id.* at 436.

[133] *Id.* at 434.

[134] *Id.*

[135] *Leduc v. Roman*, 2009 CanLII 6838 (ON SC), *available at* http://www.canlii.org/en/on/onsc/doc/2009/2009canlii6838/2009canlii6838.html (last visited Sept. 25, 2011).

[136] *Murphy v. Perger*, [2007] O.J. No. 5511, 2007 WL 5354848 (S.C.J.).

[137] *Simply Storage Mgmt, LLC*, 270 F.R.D. at 434; *see also Leduc*, 2009 CanLII 6838, at ¶¶ 30-32; *Murphy*, [2007] O.J. No. 5511, at ¶ 20 ("The plaintiff could not have a serious expectation of privacy given that 366 people have been granted access to the private site.").

[138] *Simply Storage Mgmt, LLC*, 270 F.R.D. at 437.

[139] Jill L. Rosenberg, *How Social Networking Is Changing the Face of Employment*, in Employment Discrimination Law and Litigation 2011, Practising Law Institute Litigation and Administrative Practice Course Handbook Series 493 (2011) (citing Nielsen, What Americans Do Online: Social Media and Games Dominate Activity (Aug. 2, 2010), *at* http://blog.nielsen.com/nielsenwire/online_mobile/what-americans-do-online-social-media-and-games-dominate-activity (last visited Sept. 25, 2011)).

[140] Brad Stone, *Is Facebook Growing up Too Fast?*, N.Y. Times, Mar. 28, 2009, at BU1.

[141] Facebook, Statistics (2011), *at* http://www.facebook.com/press/info.php?statistics (last visited Sept. 20, 2011).

[142] Proskauer Rose LLP, More Than 75 Percent of Businesses Use Social Media, Nearly Half Do Not Have Social Networking Policies: Proskauer International Labor & Employment Group Survey Captures Current Attitudes toward Social Networking in the Workplace (July 14, 2011), *at* http://www.proskauer.com/news/press-releases/july-14-2011/more-than-75-percent-of-businesses-use-social-media-nearly-half-do-not-have-social-networking-policies.

[143] Rosenberg, *supra* note 139, at 493 (citing Cisco, *The Demographic Shift: The Role of Collaboration and Social Networks, in* Cisco 2010 Midyear Security Report 10, *available at* http://www.cisco.com/en/US/prod/collateral/vpndevc/security_annual_report_mid2010.pdf (last visited Sept. 25, 2011)).

[144] Rosenberg, *supra* note 139, at 493 (citing Nucleus Research, Inc., Facebook: Measuring the Cost to Business of Social Networking (July 2009), *at* http://nucleusresearch.com/research/notes-and-reports/facebook-measuring-the-cost-to-business-of-social-notworking (last visited Sept. 25, 2011)).

[145] 42 U.S.C. § 2000e–2(a)(1).

[146] *Zaderaka v. Ill. Human Rights Comm'n*, 131 Ill. 2d 172, 178-79, 545 N.E.2d 684 (1989) (citing *McDonnell Douglas Corp. v. Green*, 411 U.S. 792, 802, 93 S. Ct. 1817, 1824 (1973)).

[147] 42 U.S.C. § 12101, *et seq.*

[148] 29 U.S.C. § 621, *et seq.*

[149] 42 U.S.C. §§ 12101-12102.

[150] 29 U.S.C. §§ 621; 630-31.

[151] 29 C.F.R. § 1635, *et seq.*

[152] *Id.* § 1635.4.

[153] *Id.* § 1635.8. The exceptions to the deliberate acquisition of genetic information are replete with contingencies that are too complicated to address in this Monograph. The exceptions are set forth at § 1635.8(b). *Id.* § 1635.8(b).

[154] *Owens v. Dep't of Human Rights*, 403 Ill. App. 3d 899, 919, 936 N.E.2d 623, 640 (1st Dist. 2010).

[155] *Id.*

[156] *Id.*

[157] *Zaderaka*, 131 Ill. 2d at 180.

[158] *Id.*

[159] *Id.*

[160] *Pace Suburban Bus Div. of Regional Transp. Auth. v. Illinois Labor Relations Bd.*, 406 Ill. App. 3d 484, 500, 942 N.E.2d 652, 666 (1st Dist. 2010).

[161] *Id.*

[162] *Id.*

[163] *Sperl v. C.H. Robinson Worldwide, Inc.*, 408 Ill. App. 3d 1051, 946 N.E.2d 463 (3d Dist. 2011).

[164] *See, e.g.*, 42 U.S.C. § 2000e(a) (Title VII); 29 U.S.C. § 630(b) (ADEA); and 42 U.S.C. § 12111(5)(A) (ADA).

[165] 775 ILCS 5/2-102(D).

[166] Marie-Andree Weiss, *The Use of Social Media Sites Data by Business Organizations in Their Relationships with Employees*, J. of Internet L. 16 (Aug. 2011) (citing Cross-Tab Marketing Services, Online Reputation in a Connected World, 10 fig. 2 (Jan. 2010), *at* http://www.slideshare.net/opinionwatch/online-reputation-for-job-seekers-report-crosstab (last visited Sept. 25, 2011)).

[167] *Id.*

[168] *Id.* (citing Molly Thomas, *Snap Judgments*, 19-Dec. Bus. L. Today 6 (Nov./Dec. 2009)). Some states have passed laws that prohibit employment decisions based on any lawful off-duty conduct. *See, e.g.*, Cal. Lab. Code §§ 96(k), 98.6; Colo. Rev. Stat. § 24-34-402.5; N.Y. Lab. Law § 201-d; N.D. Cent. Code § 14-02/4-03.

[169] Rosenberg, *supra* note 139, at 495.

[170] The City of Bozeman had been performing these kinds of background checks for years, but shortly after the policy became an international media story and in response to much negative publicity, the city stopped this policy. Natalie Weinstein, *Bozeman to job seekers: We won't seek passwords*, CNET News, June 20, 2009, *at* http://news.cnet.com/8301-13578_3-10269770-38.html (last visited Sept. 25, 2011).

[171] Jackie Calmes, *For a Washington Job, Be Prepared to Tell All*, N.Y. Times, Nov. 13, 2008, at A1.

[172] This kind of monitoring could get employers into trouble. *See Pietrylo v. Hillstone Rest. Group*, Docket No. 06-5754 (FSH), 2008 WL 6085437 (D.N.J. July 25, 2008) (affirming a jury verdict that an employer who secretly monitored its employees' postings on a private password-protected Internet chat room was in violation of the federal Stored Communications Act and the New Jersey Wiretapping and Electronic Surveillance Control Act).

[173] Besides potentially implicating concerns of discrimination, terminating employees based upon the content of their social media pages can also attract the attention of the NLRB and implicate First Amendment free speech concerns.

[174] *Ross v. May Co.*, 377 Ill. App. 3d 387, 880 N.E.2d 210 (1st Dist. 2007).

[175] *Rabin v. Karlin & Fleisher, LLC*, 409 Ill. App. 3d 182, 945 N.E.2d 681 (1st Dist. 2011).

[176] *Pace Suburban Bus Div. of Regional Transp. Auth. v. Illinois Labor Relations Bd.*, 406 Ill. App. 3d 484, 500, 942 N.E.2d 652, 666 (1st Dist. 2010).

[177] California, Colorado, New York, and North Dakota have passed such laws. *See, e.g.*, Cal. Lab. Code §§ 96(k), 98.6; Colo. Rev. Stat. § 24-34-402.5; N.Y. Lab. Law § 201-d; N.D. Cent. Code § 14-02/4-03.

[178] John Gonzalez, *Cold Eagles Sure Are Thin Skinned*, The Inquirer, Mar. 9, 2009, *at* http://articles.philly.com/2009-03-09/sports/24984311_1_leonard-bonacci-brian-dawkins-lincoln-financial-field (last visited Sept. 25, 2011).

[179] Where an employee of the fire bureau was terminated, in part, for posting official fire bureau photographs and revealing photographs of herself on her MySpace page, the Court of Appeals for the 11th Circuit upheld the termination and held that the employee's posting photographs online was not entitled to First Amendment protection. *Marshall v. Mayor and Alderman of City of Savannah*, Docket No. 09-13444, 2010 WL 537852 (11th Cir. Feb. 17, 2010). The Court of Appeals for the Second Circuit upheld summary judgment in favor of the employer where a 54-year-old employee who suffered from post-traumatic stress disorder alleged discrimination and the court held that the employer's reason for termination was legitimate, non-discriminatory, and not shown to be pretextual, because the employee was fired due to violating company policies by accessing sexually explicit

materials on the Internet while at work. *Pacenza v. IBM Corp.*, Docket No. 09-2025-cv, 2010 WL 346810 (2d Cir. Feb. 2, 2010). Further, there was no showing that the employee was singled out or treated more harshly than similarly situated non-disabled employees. *Id.* Where an allegedly bipolar employee admitted to viewing violent websites on his work computer, including ones that provided information about serial killers, and claimed discrimination after he was fired, the U.S. District Court for the Middle District of Tennessee found that the employer had a sufficient non-discriminatory reason for terminating the employee. *Calandriello v. Tennessee Processing Ctr., LLC*, Docket No. 3:08-1099, 2009 WL 5170193 (M.D. Tenn. Dec. 15, 2009).

[180] *See, e.g.*, Fair Credit Reporting Act, 15 U.S.C. § 1681, *et seq.*; see also Part II.B.5, *supra*, concerning the Illinois Employee Creidt Privacy Act of 2010.

[181] 15 U.S.C. § 1681, *et seq.*

[182] *See generally id.* §§ 1681a-1681d.

[183] *Id.* § 1681a(d)(1)(B).

[184] *Id.* § 1681b(a)(3)B).

[185] *Id.* § 1681b(b)(1)(A)(ii).

[186] *Id.* § 1681b(b)(2)(B)(ii).

[187] *Id.* § 1681a(x)(2).

[188] *Helfers-Beitz v. Degelman*, 406 Ill. App. 3d 264, 939 N.E.2d 1087 (3d Dist. 2010).

[189] *Goldberg v. Brooks*, 409 Ill. App. 3d 106, 948 N.E.2d 1108 (1st Dist. 2011).

[190] *Id.*

[191] *Seitz-Partridge v. Loyola Univ. Chi.*, 409 Ill. App. 3d 76, 948 N.E.2d 219 (1st Dist. 2011).

[192] Kyle Anderson, *Courtney Love Tweets Herself into another Lawsuit, this Time with a Law Firm*, EW.com, May 27, 2011, *at* http://music-mix.ew.com/2011/05/27/courtney-love-lawsuit-twitter-lawyer (last visited Sept. 25, 2011).

[193] *Id.*

[194] *Id.*

[195] *Id.*

[196] 16 C.F.R. § 255.

[197] Scott J. Slavick, *Online False Advertising Risks*, Bus. L. Today, Oct. 2010, *at* http://apps.americanbar.org/buslaw/blt/content/2010/10/article-slavick.pdf (last visited Sept. 25, 2011).

[198] *Id.*

[199] Cecilia Kang, *FTC Sets Endorsement Rules for Blogs*, Wash. Post, Oct. 6, 2009, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2009/10/05/AR2009100503620.html (last visited Sept. 25, 2011).

[200] *Dopkeen v. Whitaker*, 399 Ill. App. 3d 682, 926 N.E.2d 794 (1st Dist. 2010).

[201] *Jim Mullen Charitable Found. v. World Ability Fed'n, NFP*, 395 Ill. App. 3d 746, 917 N.E.2d 1098 (1st Dist. 2009).

[202] A super-sized putative class could hinder class certification, however, given the United States Supreme Court decision in *Wal-Mart Stores, Inc. v. Dukes*, 131 S. Ct. 2541, 2547 (2011), wherein the putative class consisted of 1.5 million people. In that case, the Court held that the plaintiff class could not show that the employer operated under a general policy of discrimination against women with respect to wage earnings. *Id.* at 2555-56. The Court, therefore, held that the putative class could not satisfy the commonality requirement for class certification. *Id.* at 2557.

[203] *See* Bob E. Lype, *Employment Law and New Technologies*, 47-May Tenn. B.J. 20, 23-24 (2011) (citing *Mackelprang v. Fidelity Nat'l Title Agency of Nev., Inc.*, Docket No. 2:06-cv-00788-JCM-GWF, 2007 U.S. Dist. LEXIS 2379 (D. Nev. Jan. 9, 2007) (refusing to permit an employer's request for discovery in a sexual harassment suit, where the defendant-employer sought

discovery of private messages sent by the plaintiff-employee through her MySpace account to impeach the plaintiff's credibility, because the company believed the messages would show that the plaintiff was involved in an extramarital affair, because the discovery was not directly related to plaintiff's employment); *EEOC v. Simply Storage Mgmt, LLC*, 270 F.R.D. 430 (S.D. Ind. 2010) (permitting an employer to discover an employee's social networking activity on Myspace and Facebook, even though the employee's "privacy settings" had been made "private" and the information sought was not available to the general public); and *Romano v. Steelcase, Inc.*, 907 N.Y.S.2d 650 (Sup. Ct. N.Y. 2010) (permitting discovery of the plaintiff's social networking information, including the deleted information maintained by the service providers, finding the plaintiff could not expect a guarantee of privacy over the information)).

[204] Under Illinois law, spoliation of evidence is a form of negligence; proof of spoliation requires a showing that the defendant owed the plaintiff a duty to preserve evidence, breached that duty, and thereby proximately caused the plaintiff to be unable to prove the underlying cause of action. *Brobbey v. Enterprise Leasing Co. of Chi.*, 404 Ill. App. 3d 420, 935 N.E.2d 1084 (1st Dist. 2010).

[205] *Id.*

[206] Rosenberg, *supra* note 139, at 501-02.

[207] *Id.*

[208] *Id.*

[209] *Id.*

[210] 29 U.S.C. §§ 151-169.

[211] *Id.* § 151.

[212] Economic News Release: Union Members Summary, U.S. DOL, Bureau of Labor Statistics, (Jan. 21, 2010) (reporting reduction of union membership rate).

[213] 29 U.S.C. §153.

[214] *Id.* §153(b).

[215] *New Process Steel, L.P. v. NLRB*, 130 S. Ct. 2635, 2638, 2644-45 (2010).

[216] *Id.*

[217] *See* Letter from 47 Senate Republicans to President Barak Obama (Feb. 1, 2001), *available at* http://isakson.senate.gov/press /2011/020211%20Becker.html (last visited Sept. 25, 2011).

[218] *See* http://www.nlrb.gov/who-we-are/board (last visited Sept. 25, 2011).

[219] *Id.*

[220] http://www.nlrb.gov/who-we-are/board/craig-becker (last visited Sept. 25, 2011).

[221] *See* http://www.nlrb.gov/who-we-are/general-counsel (last visited Sept. 25, 2011).

[222] *Id.*

[223] Of particular note are the Memorandum from NLRB General Counsel, GC 11-06, First Contract Bargaining Cases: Regional Authorization to Seek Additional Remedies and Submissions to Division of Advice (Feb. 18, 2011), *available at* http://mynlrb.nlrb.gov/link/document. aspx/09031d4580446db6 (discussing instructions for seeking remedies); and the Memorandum from NLRB General Counsel, GC 11-07, Guideline Memorandum Regarding Backpay Mitigation (Mar. 11, 2011), *available at* http://mynlrb.nlrb.gov/link/document.aspx/09031d458045d136 (discussing guidelines on back pay mitigation).

[224] Notification of Employee Rights Under the National Labor Relations Act, 76 Fed. Reg. 54,006 (Aug. 30, 2011) (to be codified at 29 C.F.R. pt. 104).

[225] 29 U.S.C. § 152.

[226] 76 Fed. Reg. 54,006.

[227] *Id.*

[228] On August 18, 2011, the Office of General Counsel issued a report of the cases that it has addressed that concern social medial within the previous year. Memorandum from the Office of NLRB General Counsel, Div. of Operations-Management, OM 11-74, Report of the Acting General Counsel Concerning Social Media Cases (Aug. 18, 2011) (hereinafter NLRB GC OM 11-74), *available at* http://mynlrb.nlrb.gov/link/document.aspx/09031d458056e743 (last visited Sept. 25, 2011).

[229] 29 U.S.C. § 157.

[230] *Id*.

[231] NLRB GC OM 11-74.

[232] *Id.* (citing *Meyers Industries (Meyers I)*, 268 N.L.R.B. 493 (1984), *rev'd sub nom, Prill v. NLRB*, 755 F.2d 941 (D.C. Cir. 1985), *cert. denied*, 474 U.S. 948 (1985), *on remand Meyers Industries (Meyers II)*, 281 N.L.R.B. 882 (1986), *aff'd sub nom, Prill v. NLRB*, 835 F.2d 1481 (D.C. Cir. 1987), *cert. denied*, 487 U.S. 1205 (1988)).

[233] *Id*.

[234] NLRB, Employee Rights, *at* http://www.nlrb.gov/rights-we-protect/employee-rights (last visited Sept. 26, 2011).

[235] News Release, Complaint Alleges Connecticut Company Illegally Fired Employee over Facebook Comments: Employee Posted Remarks about Supervisor Following Work-Related Incident, Office of NLRB General Counsel (Nov. 2, 2010).

[236] *Id.*

[237] News Release, Settlement Reached in Case Involving Discharge for Facebook Comments, NLRB Office of Pub. Affairs (Feb. 8, 2011).

[238] News Release, Regional News: Build.com Settles Charge of Unlawful Discharge for Comments Posted on Facebook with NLRB Agreement in San Francisco, NLRB Office of Pub. Affairs (Apr. 27, 2011).

[239] *Id.*

[240] *Id.*

[241] Nexsen Pruet, *NLRB Targets "Facebook Firings" and Social Media Policies*, Employment Law Update–July 2011 (June 28, 2011), *at* http://www.nexsenpruet.com/publications-576.html (last visited Sept. 25, 2011).

[242] News Release, Chicago Car Dealership Wrongfully Discharged Employee for Facebook Posts, Complaint Alleges, NLRB Office of Pub. Affairs (May 24, 2011).

[243] Nexsen Pruet, *NLRB Targets "Facebook Firings" and Social Media Policies*, Employment Law Update–July 2011 (June 28, 2011), *at* http://www.nexsenpruet.com/publications-576.html (last visited Sept. 25, 2011).

[244] *Id.*

[245] News Release, Chicago Car Dealership Wrongfully Discharged Employee for Facebook Posts, Complaint Alleges, NLRB Office of Pub. Affairs (May 24, 2011).

[246] Nexsen Pruet, *NLRB Targets "Facebook Firings" and Social Media Policies*, Employment Law Update–July 2011 (June 28, 2011), *at* http://www.nexsenpruet.com/publications-576.html (last visited Sept. 25, 2011).

[247] *The Feds De-friend Business, NLRB off the Wall on Facebook Regulation*, Chi. Trib., June 15, 2011.

[248] *Id.*

[249] News Release, Chicago Car Dealership Wrongfully Discharged Employee for Facebook Posts, Complaint Alleges, NLRB Office of Pub. Affairs (May 24, 2011).

[250] News Release, Complaint Issued Against New York Nonprofit for Unlawfully Discharging Employees Following Facebook Posts, NLRB Office of Pub. Affairs (June 28, 2011).

[251] *Id.*

[252] News Release, Administrative Law Judge Finds New York Nonprofit Unlawfully Discharged Employees Following Facebook Posts, NLRB Office of Pub. Affairs (Sept. 7, 2011).

[253] *Id.*

[254] *Id.*

[255] *Id.*

[256] *Id.*

[257] *Bay Sys Techs. LLC and Dontray L. Tull*, 357 N.L.R.B. No. 28 (Aug. 2, 2011).

[258] *Id.*

[259] *Id.*

[260] News Release, Chicago Car Dealership Wrongfully Discharged Employee for Facebook Posts, Complaint Alleges, NLRB Office of Pub. Affairs (May 24, 2011) (noting that the nature of the employee's comments would not cause the Facebook posting to lose its protection).

[261] NLRB GC OM 11-74.

[262] News Release, Complaint Alleges Connecticut Company Illegally Fired Employee over Facebook Comments: Employee Posted Remarks about Supervisor Following Work-Related Incident, Office of NLRB General Counsel (Nov. 2, 2010).

[263] NLRB GC OM 11-74..

[264] *Bay Sys Techs. LLC and Dontray L. Tull*, 357 N.L.R.B. No. 28 (Aug. 2, 2011).

About the Authors*

Jana L. Brady graduated from Northern Illinois University College of Law in 2003 and has been an attorney with *Heyl, Royster, Voelker & Allen* in its Rockford office since that time. She focuses her practice on the defense of civil litigation and federal practice, particularly in the context of employment law, civil rights, medical malpractice, correctional medicine, insurance coverage and nursing home cases.

Theresa Bresnahan-Coleman is an associate at *Langhenry, Gillen, Lundquist & Johnson, LLC* in Chicago. Theresa concentrates her practice in civil litigation defense, with an emphasis in employment law, municipal civil rights, personal injury, and premises liability. She serves on the IDC Employment Law and Municipal Law Committees and is a member of the Chicago and Illinois State Bar Associations. She received her law degree in 2009 from New England School of Law, where she served as the managing editor of the New England Journal of International and Comparative Law and earned a CALI award in Employee Benefits. Theresa received her master of arts degree in English in 2006 from Loyola University Chicago and her bachelor of arts degree in English and Computer Applications in 2001 from the University of Notre Dame. Prior to attending law school, Theresa worked as an investigator for the Federal Trade Commission.

Kimberly A. Ross is a partner with the Chicago law firm of *CremerSpina, LLC.* She received her J.D. from DePaul University College of Law and her B.A. from the University of Michigan. Her practice areas include employment law and general tort litigation. Ms. Ross was a past Editor in Chief of the *IDC Quarterly*. In addition to the IDC, she is a member of the Defense Research Institute, the Decalogue Society of Lawyers and the Women's Bar Association.

Geoffrey M. Waguespack is the Committee Chairperson of the IDC's Employment Law Committee, and was an associate with the law firm of *Cremer, Spina, Shaughnessy, Jansen & Siegert, LLC*, where he concentrated his practice in employment law and general tort litigation. Prior to joining that firm, Mr. Waguespack served as the judicial law clerk to the Honorable Morton Denlow, Presiding Magistrate Judge for the United States District Court, Northern District of Illinois, and as a research staff attorney for the Appellate Court of Illinois, Second District. He earned his B.A. from the College of William & Mary in Virginia and his J.D. from Loyola University Chicago School of Law. Prior to the publication of this Monograph, Mr. Waguespack joined the law firm of *McGinnis Tessitore Wutscher LLP* as senior counsel.

James H. Whalen is an associate of *Williams Montgomery & John Ltd.* and a member of the firm's tort defense, product liability and commercial litigation practice groups. He focuses his practice on construction, business, commercial, product liability, employment discrimination and premises liability litigation in state and federal courts and before state administrative bodies. Mr. Whalen received a B.A. in history in 2000 from Indiana University, Bloomington, IN, where he also obtained minor degrees in Spanish, economics and business. He received his J.D. in 2004 from the DePaul University College of Law.

Jennifer A. Winking is a partner with the Quincy law firm of *Scholz, Loos, Palmer, Siebers, & Duesterhaus LLP*, where she concentrates her practice on employment law and litigation and workers compensation defense. She has presented for the Illinois State Bar Association on topics

of employment law and workers compensation and is a frequent lecturer on various employment topics, including harassment and sensitivity training. She earned her B.A. from Quincy University as a double major graduating summa cum laude and her J.D. from the University of Missouri-Columbia School of Law.

*The authors would like to thank Bradley C. Nahrstadt, Williams, Montgomery & John., Ltd., Matthew G. Jones, Loyola University Chicago, School of Law, and Joseph V. Pumilia, Heyl, Royster, Voelker & Allen, for their contributions to this Monograph

About the IDC

The Illinois Association Defense Trial Counsel (IDC) is the premier association of attorneys in Illinois who devote a substantial portion their practice to the representation of business, corporate, insurance, professional and other individual defendants in civil litigation.
For more information on the IDC, visit us on the web at **www.iadtc.org**.

Illinois Association of Defense Trial Counsel, PO Box 3144, Springfield, IL 62708-3144, 217-585-0991, idc@iadtc.org