PRIVACY, SOCIAL MEDIA AND THE AMERICAN WORKPLACE:
EMPLOYMENT LITIGATION WILL NEVER BE THE SAME

ERIC L. BARNUM
SCHIFF HARDIN LLP
ONE ATLANTIC CENTER, SUITE 2300
ATLANTA, GEORGIA 30309
EBARNUM@SCHIFFHARDIN.COM
INTRODUCTION

For all its efficiencies and productivity enhancements, technology in this digital age continues to trend well ahead of American jurisprudence. We have found more ways to exchange information about where we are, what we’re doing, where we’re going and what we’ll do when we get there than can possibly be consumed in a rational and thoughtful manner. One can only wonder whether Sting knew the prophecy of his words when he penned the lyrics

Every breath you take and every move you make
Every bond you break
Every step you take, I'll be watching you
Every single day and every word you say
Every game you play
Every night you stay, I'll be watching you

Electronic mail, internet blogging, cellular phone text messaging, instant messaging, social networking and global positioning satellite systems (GPS) are only some of the tools available to employers and employees to help them communicate with customers, clients and co-workers. Managing these tools has proven to be difficult for employers as more companies try to avoid liability for improper use of company information technology. The “now” phase of communicating has created an even more complex set of rules for workplace interaction.

THE NEW ELECTRONIC AGE

Web 2.0

The explosion of blogs, forums, virtual communities and social networking has brought about a new version of the internet with its own set of unique problems for employers today. Traditionally, the internet provided a one-way dissemination of information to users. Information on the internet is no longer just viewed and consumed. The term Web 2.0 describes a new generation of the internet where information is shared, people build relationships, and content is created through collaboration. Web 2.0 allows the internet to become a two-way interaction where users create content rather than simply act as visitors and consumers.

1 Eric L. Barnum is partner at Schiff Hardin LLP, resident in the Atlanta, Georgia office. Mr. Barnum received his law degree from Pacific McGeorge School of Law and his Bachelor of Arts from the University of California, Los Angeles.

2 Taken from "Every Breath You Take", from the 1983 album Synchronicity, written by Sting and performed by The Police.
The applications offered by Web 2.0 attract a diverse group of people including far more than just the stereotypic child or teenager. A study conducted by a marketing company in San Francisco revealed that social media is still dominated by younger users, but older users are flocking to social networking sites, blogs, and forums. This necessarily implies that the nation’s workforce is using Web 2.0 applications with increasing regularity.

Employees use the applications as a social experience. Social networking sites, for example, allow users to make a profile and start connecting with other users. The sites allow the user to include information about everything from pictures of their last vacation to a recent promotion at work. Users can log on from any computer to access their own profiles as well as the profiles of friends. A bad day at work can easily result in a “status update” on Facebook®. As a result, the lines between “work” and “personal” lives blur and make managing employees within the bounds of the law increasingly difficult. Natural questions arise. Should employers filter all electronic communications coming in and out of the workplace on company-owned equipment and networks? Answering this question is not an easy task when considering that cyber-communication and social networking can be very beneficial to an employer trying to reach a vast audience.

The benefits of immediate public viewing are clear for many employers trying to “brand” their corporate image or persona. Employers can use social networking sites to bring together employees or current and potential customers. With social networking, access to information is quicker, but also less formal. Users of all types tend to be less guarded and careless with what they say and the messages (intended and unintended) they send.

The very structure of social networking sites, blogs, and virtual communities pose risks for employers. Some risks include increased complaints of harassment or discrimination, disclosure of confidential information, loss of trade secret protection and, increased exposure to tort lawsuits. With so many forums to communicate, it is only a matter of time before “cybersmearing,” “cyberstalking” and “cyberharassment” dominate the state and federal court employment dockets. Employers should be aware of the possibility that employees (including managers and supervisors) might post offensive language or pictures on social networking sites that can be viewed by co-workers and clients. Employees often comment upon information or pictures on a co-workers social networking site. Those comments can bleed over into direct communication between co-workers about personal social networking pages and information and pictures presented there. These comments can be most “unwelcome”.

**Pervasive Technology and Its Impact on Privacy Laws**

The Evolution of Privacy Law and Technology

Two general areas where privacy law and technology intersect are the government's invasion of an individual's privacy and a commercial organization's invasion of an individual's

---

privacy. 4 Historically, there have always been issues surrounding privacy and technology. The Founding Fathers incorporated the Third, Fourth and Fifth Amendments into the Bill of Rights. 5 The Third Amendment protects privacy by preventing the government from placing soldiers in the homes of citizens. The Fourth Amendment is a broad constitutional limitation on “unreasonable searches and seizures.” The Fifth Amendment protects privacy by preventing an individual from being “compelled in any criminal case to be a witness against himself.” 6

From a historical perspective, the Fourth Amendment has had the most impact on privacy and technology. In the early 1900s, the invention of the telephone brought concerns about wiretapping and privacy. 7 In the 1928 case of Olmstead v. United States, the court decided that the Fourth Amendment did not apply to wiretapping because there was no search or seizure. 8 The Supreme Court overruled Olmstead and further defined the Fourth Amendment in the case of Katz v. United States. 9 In this case, the majority stated that what a person makes available for public consumption is not subject to privacy protections, except possibly in instances where a person is in a public place and reasonably expects privacy. 10 Since Katz, the bounds of the Fourth Amendment have been more narrowly defined.

The Privacy Act of 1974 11 regulates the government's invasion of individual privacy, and is the most comprehensive of the privacy laws. 12 The Act contains provisions for the correction of personal information and limits the use of the data collected. The biggest limitation of the Act is that it only applies to government agencies and government corporations, and not to private companies. The most recent developments in the regulation of governmental invasion of privacy are laws enacted by the United States Congress to increase surveillance as a result of the terrorist attacks of September 11, 2001. 13

---


5 Id. at 28.

6 U.S. Const. amend. III, IV, V

7 Solove, supra footnote 4, at 41-43.


10 Id. at 351-52.


13 Solove, supra footnote 4, at 65-66.
The current body of law governing technology and privacy in relation to non-government actors is derived from many different sources. The driving force behind privacy protections relating to non-government organizations is the Warren and Brandeis article “The Right to Privacy”.

Written in 1890, the article discusses how newspaper companies stepped beyond the reasonable boundaries of individuals' privacy. The article also discusses how cameras could invade personal privacy. The authors argue that common law could be used to regulate privacy. The article leads to the conclusion that a tort standard could be applied to an invasion of privacy. Today, four tort standards are identified and recognized by the vast majority of states. These torts are (1) intrusion upon seclusion; (2) public disclosure of private facts; (3) false light or ‘publicity’; and (4) appropriation.

In response to the emergence of technologies like computers and surveillance, the federal government ramped up legislative activity in the 1970s. Specifically, after 1974, Congress started regulating the private sector by enacting statutes governing the collection of individuals' private information. In the 1980s, some targeted federal regulations affecting technology and privacy emerged, such as the Cable Communications Policy Act of 1984 and the Video Privacy Protection Act of 1988. These statutes restrict the ability of technology-based companies to collect and distribute customer information. Some argue that the Electronic Communications Privacy Act of 1986 is the most important private sector communication statute. This statute governs email, voicemail, and phone calls. Finally, there have been some movements in the private sector to regulate privacy and technology. Organizations like the American Civil Liberties Union (ACLU) and the National Consumers League, who originally did not have a focus on privacy and technology, became involved as privacy issues emerged. For example, the ACLU was founded in 1920 with a focus on preserving individual rights and guarantees, and now has a focus on balancing "the interplay between cutting-edge technology

---


15 Id. at 198.

16 Solove, supra footnote 4, at 37.


18 Id. at 34.


21 Solove, supra footnote 4, at 57-58.


and civil liberties” as it relates to privacy and freedom.24 There are also organizations that were more recently founded that began with a focus on technology and privacy. For example, the Privacy Rights Clearinghouse was founded in 1992 with one of their five goals being to “[r]aise consumers' awareness of how technology affects personal privacy.”25

Technology Privacy Regulation

Currently, many arguments are being made from both proponents and opponents of increased technological privacy about how to regulate the collection and use of data. However, at this point, clear regulatory standards have not been established. Differences arise when there is discussion of exactly who should implement the regulations and how they should be applied. Privacy advocates argue that there should be federal regulations in place; commercial companies argue that the privacy controls should be made through self-regulation; and states argue that privacy regulation should occur at their level.26 As a result, three prominent sources of regulation have emerged: individual state regulations27, targeted federal regulations28, and independent regulatory groups.29

1. State Regulations and Constitutional Provisions for Privacy

In general, many states have focused their privacy and technology legislation on certain areas: employment privacy (drug testing, background checks, employment records), Social Security Numbers, video rental data, credit reporting, cable television records, arrest and conviction records, student records, tax records, wiretapping, video surveillance, identity theft, library records, financial records, insurance records, privileges (relationships between individuals that entitle communications to privacy), and medical records.30


27 See generally id. (arguing that technological privacy concerns are best addressed at the state level).


As the states begin implementing more comprehensive privacy laws that relate to emerging technologies like pervasive computing, there will likely be an intersection of federal and state interests causing federal preemption of state legislation. In the area of state privacy legislation, the federal privacy laws do not typically preempt stronger state laws, but there has been at least one example of federal preemption restricting a state from tougher privacy regulation. In 2003, California enacted the California Financial Information Privacy Act, also known as SB1. This Act gave California consumers the ability to restrict information that their banks gave to other third-party institutions. The restriction was to be implemented as an “opt-out” program for an affiliated institution or an express disclosure for third parties. Because of the strict privacy legislation that was passed, the American Bankers Association sued the State of California claiming that this statute was preempted by federal law. The district court held that SB1 was not pre-empted by federal statutes. On appeal, the Ninth Circuit Court of Appeals reversed:

SB1 is preempted to the extent that it applies to information shared between affiliates concerning consumers’ “credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living” that is used, expected to be used, or collected for the purpose of establishing eligibility for “credit or insurance,” employment, or other authorized purpose.

On remand, the District Court emphasized that the California Financial Information Privacy Act still requires “opt-in” consent from the consumers before their financial data can be sold to third parties. The question still remains of how much involvement preemption will have in the state regulation of privacy and pervasive computing.

SOCIAL MEDIA AND THE NATIONAL LABOR RELATIONS BOARD

On August 18, 2011, the Acting General Counsel of the National Labor Relations Board ("NLRB") issued a report that summarized recent Advice Memoranda in cases involving social media. While these decisions do not have the force of law, they demonstrate how the NLRB's
General Counsel approaches and reviews social media issues under the National Labor Relations Act (the "Act"). It is important to be aware that while the NLRB often handles union-related disputes, these social media issues impact both union and non-union employers.

The two most common social media issues addressed in the report are (1) whether an employee's social media posting or discussion is protected concerted activity, rendering resulting discipline or discharge unlawful, and (2) whether an employer's social media policy is overly broad.

**Protected Concerted Activity**

Under the Act, employees have the right to engage in concerted activity about issues that relate to their terms and conditions of employment. This action is referred to as "protected concerted activity." The NLRB defines "concerted activity" as action taken "with or on the authority of other employees, and not solely by and on behalf of the employee himself."

The report cites the following facts in determining whether an employee's social media posts or messages are "concerted activity:"

1. Whether the employee discussed the posts with co-workers;
2. Whether any co-workers responded to the posts;
3. Whether the social media activity was an outgrowth of employees' collective concerns;
4. Whether the employee was seeking to induce or prepare for group action;
5. Whether the employees met or organized any group action to raise the employer's awareness of the issues in dispute.

These factors do not represent an exhaustive list, but instead illustrate the fact-specific nature of the NLRB's analysis. For example, in *JT's Porch Saloon & Eatery, Ltd.* (July 7, 2011), a bartender, in response to his sister's question on Facebook about his day at work, posted his discontent with the employer's tip-pooling policy. The General Counsel found that while the employee's Facebook comments concerned the terms and conditions of his employment, his comments were not made as part of a concerted effort. No other employees responded to his post and there had been no attempt to initiate group action concerning the employer's tipping policy. Furthermore, the General Counsel found that the employee's conversation with a coworker several months earlier regarding the tipping policy did not give rise to the employee's Facebook comments.

The General Counsel made a similar finding in *Wal-Mart* (July 19, 2011). There, an employee posted comments that were critical of management's treatment of employees. Several coworkers responded to the employee's posts with supportive comments, such as "hang in there." The General Counsel noted that despite the supportive comments from other employees, the employee's discipline was permissible because the comments did not contain language that suggested group action among the employees.
Analyzing Social Media Policies Under the NLRB’s Interpretation

A social media policy violates the Act if it would "reasonably tend to chill employees in the exercise of their rights" under the Act, including the right to engage in protected concerted activity. A policy has this effect if it explicitly restricts these rights, or if it can be shown that (a) an employee would reasonably construe the language of the policy to prohibit protected concerted activity, (b) the rule was promulgated in response to protected concerted activity, or (c) the rule was applied to restrict the exercise of protected concerted activity.

The General Counsel's report identifies a number of provisions that would violate the Act:

1. A prohibition on any communication or post that constitutes embarrassment, harassment or defamation of the hospital or of any hospital employee, officer, or staff member, or that might damage the reputation of the hospital or its staff;

2. A prohibition on talking about company business on personal accounts, and from posting anything that an employee would not want a manager or supervisor to see or that would put his or her job in jeopardy;

3. A prohibition on revealing personal information regarding coworkers, company clients, partners or customers without their consent.

The General Counsel found the provisions in (1) and (2) above to be overly broad, in that they would commonly apply to protected discussions about (or criticisms of) the employer's labor policies or treatment of employees. The prohibition in (3) was found to be overly broad because employees have a right to discuss their wages and other terms and conditions of employment. In a further effort to clarify his position, the acting general counsel on May 30, 2012 issued a third report on social media issues. In the report, the acting general counsel discussed six recent cases in which he found that employer social media policies were overly broad and thus unlawful under the Act since the policies did or reasonably could restrict employees' exercise of Section 7 rights. Examples of policies found to violate the Act include:

- a policy restricting the release of confidential guest, employee or company information, since it did not make clear that employees have the right to discuss their wages and benefits;

- a policy prohibiting offensive, demeaning, abusive or inappropriate remarks, since the policy could be interpreted to proscribe protected communications about an employer's labor policies or treatment of employees;

- a prohibition on commenting on any legal matters involving the employer (including pending litigation), since this could restrict employees from discussing potential claims they may have against the employer;

- a policy requiring employees to notify management of any unsolicited or inappropriate electronic communications received from fellow employees or outsiders, since such a
rule would restrict an employee's right to communicate with fellow employees or an outside entity such as a union about their terms and conditions of employment.

Some states have even enacted laws that restrict the scope of inquiry employers may make of their employees when it comes to accessing workers' social media sites and accounts. Illinois recently passed a law which will make it the second state (joining Maryland) to prohibit companies from demanding an employee's social networking password. Signed August 1, 2012, Illinois' new law takes effect on January 1, 2013, and prohibits an employer from (1) requesting, or requiring, any employee or job applicant to provide his or her social networking password or other account information, and (2) demanding access to an employee's or applicant's social networking account. This prohibition relates to sites such as Facebook, among others. The law applies to Illinois employers of all sizes, is enforced by the Illinois Department of Labor, and ultimately provides a private right of action for individuals to sue employers in state court.

It is important to note that the Illinois law allows employers to continue to monitor employees' use of the company’s network, electronic equipment and e-mail. In addition, companies are still permitted to promulgate and enforce lawful social media and electronic resources policies. At least a dozen other states are considering joining Illinois and Maryland in enacting similar prohibitions. In light of this increased interest in state regulation and in light of the National Labor Relations Board's critical view of social networking policies, now more than ever employers need to be aware of the changing legal landscape related to social media and social media policies.

SOCIAL MEDIA IN LITIGATION\textsuperscript{37}

Claims of ownership of intellectual property; claims of misuse of proprietary information and associated economic harm; claims alleging reputational damage and resulting emotional distress; and claims of workplace harassment or violation of corporate conduct policies proliferate state and federal trial court. As business is transacted more and more using social media, questions will emerge regarding who owns social media and the proper use of social media in litigation.

Following is a brief discussion of various types of claims that often arise in the employment context and how courts have addressed the legal issues presented.

Physical Injury Claims

Discovery of social media is allowed in cases alleging physical injury where (1) the public portion of the social media site displays content relevant to the claim; and (2) the information sought relates directly to the Plaintiff’s physical or mental health, or activities that could be relevant to the claimed injuries. In \textit{Zimmerman v. Weis Markets, Inc.}\textsuperscript{38}, a Pennsylvania court permitted discovery of photos and other non-public material from social networking sites


where the materials contain information that Defendant believed to be relevant in ascertaining the mental and physical state of Plaintiff resulting from a workplace injury). Likewise, in **McMillen v. Hummingbird Speedway, Inc.**\(^{39}\), a Pennsylvania court ordered Plaintiff to comply with Defendant’s discovery request for his MySpace and Facebook accounts where the Plaintiff claimed permanent life impairment, loss and impairment of general health, strength, and vitality, and inability to enjoy certain pleasures of life in a personal injury suit against the Defendant.

Other cases include **Romano v. Steelcase Inc.**\(^{40}\) (permitting discovery of Plaintiff’s “current and historical Facebook and MySpace pages and accounts, including all deleted pages and related information” for her personal injury claims, especially her claim for loss of enjoyment of life) and **Ledbetter v. Wal-Mart Stores, Inc.**\(^{41}\), (holding that subpoenas issued by Defendant to social networking sites are permissible where the Plaintiff claims permanent physical and psychological injuries associated with work).

### Emotional Distress Claims

Discovery of social media is allowed in cases alleging emotional distress where: (1) the public portion of the social media site displays content relevant to the claim; and (2) the information sought relates directly to the Plaintiff’s feelings, emotions, or mental states that could be relevant to the claim of emotional distress. In EEOC v. Simply Storage Mgmt., LLC\(^{42}\), the court ordered all information from Plaintiffs’ social networking profiles and postings related to the Plaintiffs’ general emotions, feelings, and mental states to be produced in discovery where Plaintiffs allege severe emotional trauma against their employer. In **Mackelprang v. Fidelity Nat’l Title Agency of Nevada, Inc.**\(^{43}\), the district court ruled that the content of the MySpace page relating to Plaintiff’s emotional distress could be relevant to her complaint of sexual harassment and was, therefore, discoverable so long as the scope of the discovery was limited to the relevant MySpace communications. See also **Nguyen v. Starbucks Coffee Corp.**\(^{44}\), (granting summary judgment in favor of employer on Plaintiff’s claims for sexual harassment, retaliation, and religious discrimination; defendant introduced Plaintiff’s MySpace comments in which Plaintiff discussed using illegal drugs and thoughts of “going berserk” and shooting everyone); **B.M v. D.M.**\(^{45}\), (statements regarding belly dancing made on social media sites by wife in divorce proceedings were allowed by the court as admissions contradicting her claims of physical disability).

---


\(^{40}\) 907 N.Y.S.2d 650 (N.Y. Sup. Ct. 2010).

\(^{41}\) Case No. 06-CV-01958-WYD-MJW, 2009 WL 1067018 (D. Colo. Apr. 21, 2009).

\(^{42}\) 270 F.R.D. 430, (S.D. Ind. 2010).


Generally speaking, discovery of social media is not allowed if the scope of the discovery is too broad and not sufficiently relevant to the Plaintiff’s claims. In *McCann v. Harleysville Ins. Co. of New York*[^46], the court concluded that the Defendant’s discovery motion for an authorization of the Plaintiff’s Facebook account was overly broad given that the Defendant had not adequately shown the relevance of the sought Facebook content to the Plaintiff’s personal injury claim. In *Muniz v. United Parcel Service, Inc.*[^47], a California court quashed a third party subpoena to obtain social media information from the Plaintiff’s counsel’s Facebook page relating to work on Plaintiff’s case. The Court held that the subpoena was overbroad and vague where the Defendant was only investigating whether attorneys’ fees were reasonable. Likewise, in *Chauvin v. State Farm Mut. Auto. Inc. Co.*[^48], a Michigan court refused to set aside a magistrate judge’s denial of an insurance company’s motion to compel production of a plaintiff insured’s Facebook log-in, password, and names of Facebook friends because the insurance company failed to show that the information was relevant or reasonably calculated to lead to the discovery of admissible information, and amounted “to a fishing expedition at best and harassment at worst”.

Obtaining and Using Social Media as Evidence

1. Publicly-available information

Social media made publicly available by one party is generally discoverable because the party cannot claim a reasonable expectation of privacy. *Zimmerman v. Weis Markets, Inc.*[^49], (granting Defendant’s Motion to Compel where the Defendant, in looking at the public portion of the Plaintiff’s Facebook page, found evidence that the Plaintiff was not embarrassed about showing off his leg scar due to a workplace injury, and holding that the Plaintiff, by voluntarily posting pictures and information on Facebook and MySpace, cannot claim that he has “any reasonable expectation of privacy to prevent [the Defendant] from access to such information”). Information made publicly available by one party that is potentially relevant to that party’s claims can lead the court to find other private social media information discoverable if it is likely that the private information is similarly relevant. *See also McMillen v. Hummingbird Speedway, Inc., supra; Romano v. Steelcase Inc.*[^50], (where the Plaintiff made publicly available portions of her social networking pages containing materials that were apparently contrary to her claims, the private portions of those pages were ruled discoverable given the likelihood that those pages contained further relevant evidence.)

2. Discovery request to party


Discovery requests for social media are normally granted where the Plaintiff’s privacy interests do not outweigh the probative value of the material and the request is tailored so that the information gained through discovery is relevant to the Plaintiff’s claims. The following cases are illustrative:

(1) *Largent v. Reed*\(^{51}\), (ordering Plaintiff to provide Facebook login information based on Defendant’s assertion that Plaintiff’s Facebook profile belied the extent and severity of her claimed physical injuries after an auto accident; “[o]nly the uninitiated or foolish could believe that Facebook is an online lockbox of secrets”).

(2) *Offenback v. L.M. Bowman, Inc.*\(^{52}\), (ordering Plaintiff to produce certain portions of his private Facebook account containing potentially relevant information that may contradict the extent of his alleged damages).

(3) *Bass ex rel. Bass v. Miss Porter’s School*, 738 F. Supp. 2d 307 (D. Conn. 2010) (ordering all 750 pages of Plaintiff’s Facebook content to be produced to the Defendant where the court could find no meaningful difference between subset provided to Defendant and complete set provided to the court).

3. Subpoena to social media site/provider

Subpoenas to social media providers are governed by the Stored Communications Act. Normally, information made publically available by the Plaintiff can be subpoenaed directly from the provider. Where the information is not publically available the provider will usually have to obtain a letter of consent to production from the owner of the account. See, for example:

- *Crispin v. Christian Audigier, Inc.*\(^{53}\), (quashing subpoenas to Facebook and MySpace for Plaintiff’s private messages under the Stored Communications Act and holding that the record was unclear as to whether the Plaintiff’s Facebook wall postings and MySpace comments were available to the general public; noting that if they had been available to the general public, they could be subpoenaed).

- *Ledbetter v. Wal-Mart Stores, Inc.*\(^{54}\), (denying Plaintiff’s protective order, stating that the subpoenas issued to Facebook, MySpace, and Meetup.com were reasonably calculated to lead to the “discovery of admissible evidence as is relevant to the issues in [the] case”).

---


\(^{53}\) 717 F. Supp. 2d 965 (C.D. Cal. 2010).

\(^{54}\) Case No. 06-CV-01958-WYD-MJW, 2009 WL 1067018 (D. Colo. Apr. 21, 2009).
• Mackelprang v. Fidelity Nat’l Title Agency of Nevada, Inc.\textsuperscript{55}, (Defendant served subpoena on MySpace to produce all records from Plaintiff’s accounts; in response MySpace produced publically available information but refused to produce private information.)

4. Creating third party accounts

A third party may create a social media account to “friend” and view a party’s page where the party knowingly consents to the scheme and has knowledge of who the third party is or who the third party represents. In Barnes v. CUS Nashville, LLC\textsuperscript{56}, a case involving a Plaintiff injured while dancing on a bar, a magistrate judge in Tennessee agreed to create a Facebook account specifically for the case, in order to ease the difficulty of discovery of the social media content and expedite further discovery, promising to terminate the Facebook account after reviewing the content for relevant information.

Ethical Issues Regarding the Use of Social Media in Litigation

Most states that have considered the question have some sort of rule prohibiting lawyers from utilizing deception, or directing a third party to utilize deception, in order to “friend” an adverse party, or a witness for an adverse party, to access more than the publically available portion of their social media. Illustrative ethics opinions include:

• The Ass’n of the Bar of the City of New York Comm. On Prof. Ethics, Formal Op. 2010-2 (Sept. 2010) (lawyers and their agents must not use deception in “friending” an individual to obtain information from a social networking website but should rely on informal and formal discovery procedures).

• The Philadelphia Bar Ass’n Prof’l Guidance Comm., Op. 2009-02 (Mar. 2009) (if a lawyer “friends” a witness (with testimony potentially helpful to the lawyer), or directs a third party to do the same, it could potentially implicate various Pennsylvania Rules of Professional Conduct).

• San Diego County Legal Ethics Op., 2011-2 (May 24, 2011) (it is deceptive for attorneys to “friend” a witness or adverse party on a social networking site without revealing their reasons for extending the request; “friending” a represented party violates California Rules of Professional Conduct 2-100).

However, an attorney may view the public portion of the adverse party or a witness for an adverse party’s social media:

• New York State Bar Ass’n, Comm. of Prof’l Ethics, Opinion 843 (Sept. 10, 2010) (a lawyer may view the public portion of a party’s social media site in pending litigation to secure information about the party for use in the lawsuit).


\textsuperscript{56} Case No. 3:09-cv-00764, 2010 WL 2265668 (M.D. Tenn. June 3, 2010).
• Oregon State Bar, Opinion No. 2005-164 (Aug. 2005) (a lawyer may visit an adverse party’s public website to gain information).

At least one bar association has suggested that attorneys may not “friend,” or direct a third party to “friend,” an adverse party or a witness for an adverse party even if the attorney or third party does not engage in deception (e.g., hiding true purpose for “friending;” changing profile to induce party to accept friend request). See New York State Bar Ass’n, Comm. of Prof’l Ethics, Opinion 843, supra (a lawyer may not friend, nor direct a third party to friend, a party to the lawsuit in pending litigation in order to gain information not publically available).

To further drive home the point that electronic and social media are now permanent parts of the employment – and general – litigation landscape, the American Bar Association itself has opined that practicing attorneys have a duty to warn clients of the dangers of electronic communications that may be accessed by third parties. See American Bar Ass’n, Standing Comm. on Ethics & Prof’l Responsibility, Opinion 11-459 (August 4, 2011) (“A lawyer sending or receiving substantive communications with a client via e-mail or other electronic means ordinarily must warn the client about the risk of sending or receiving electronic communications using a computer or other device, or e-mail account, where there is a significant risk that a third party may gain access. In the context of representing an employee, this obligation arises, at the very least, when the lawyer knows or reasonably should know that the client is likely to send or receive substantive client-lawyer communications via e-mail or other electronic means, using a business device or system under circumstances where there is a significant risk that the communications will be read by the employer or another third party.”)

Though judges now universally admonish jurors to refrain from discussing trials on social media, the nationwide lawyers group for the first time is addressing how deeply attorneys, their investigators and their consultants can probe for information that might signal leanings of potential jurors, or unearth juror misconduct during trials. Jurors’ online postings have disrupted many legal proceedings over the years, causing mistrials and special hearings over the effects of Facebook musings, tweets and blog writings about their trial experiences. Lawyers and judges have also been wrangling over how far attorneys can go in assembling a jury with help from online research of jurors’ social media habits.

A few judges have denied lawyers permission to research social media sites as overly invasive while others have allowed it. But the ABA has given attorneys the green light to scan the social media sites of jurors; and may use the internet to research potential jurors absent a court rule making it impermissible. According to the ABA, it is ethical for lawyers to scour online for publicly available musings of citizens called for jury service — and even jurors in deliberations. But the ABA does warn lawyers against actively "following" or "friending" jurors or otherwise invading their private Internet areas. The ABA’s Ethics Committee began reviewing the issue about two years ago and concluded in April 2014 that looking at Facebook posts, Twitter tweets and other information gathered passively is ethical research. The Committee further decided a LinkedIn search was ethically sound, but that decision runs counter to an opinion issued by the New York City Bar Association in 2010 that said any notice sent to a potential juror about a search amounts to an unauthorized communication. In New York County Lawyers’ Association Committee on Professional Ethics, Opinion No. 743 (May 18, 2011) the New York Bar Association found it proper under NY RPC 3.5 for a lawyer to conduct a search
of a prospective juror’s social media, both before and during trial, provided there is no contact or communication with the prospective juror and the lawyer does not seek to “friend” jurors, subscribe to their Twitter accounts, contact jurors in any way, and does not use deceit in reviewing the social media sites. (Emphasis added.)

At least two state bar organizations have addressed online searches of potential jurors. The Missouri Supreme Court requires lawyers to research potential jurors’ litigation history on a Web site that tracks lawsuits in the state. The Oregon State Bar published an opinion last year that's in line with the ABA guidelines, saying lawyers can access publicly available social media information, but can't actively "follow" or "friend" potential jurors. The California State Bar, the biggest state bar in the country, has not addressed the issue.

PRACTICAL CONSIDERATIONS AND BEST PRACTICES

The question for many employers is to what extent should it regulate use of its information technology software and hardware to protect itself from liability? In a 2009 study on policies and data loss risks by Proofpoint, Inc., seventeen percent of employers reported that they had experienced more exposure incidents involving sites like Facebook® and LinkedIn® while eight percent reported terminating an employee for such a violation. While employers appear to be taking a tougher approach with employees, they should not lose sight of the benefits that social networking presents.

Employers can use Web 2.0 to assist in hiring decisions, marketing, and communicating with employees. Many employers are taking advantage of the information available about users and using searches of social networking sites to check out applicants. Employers often make employment decisions based on information found on their applicant’s profile. Many companies are creating their own profiles on Facebook® as a tool for recruiting, marketing to potential clients, and disseminating information to current clients and employees.

The new technological advances, including Web 2.0, also present several potential liabilities for employers. Just as companies can disseminate information for the purpose of marketing and communicating with employees, employees can disseminate confidential employer information including trade secrets and business strategies. Just as text messaging has been used to harass co-workers, Web 2.0 provides countless opportunities for employees to make inappropriate remarks, threats, and harassing statements. Employers must consider their current policies and further consider changing those policies as the technological landscape evolves.

A few simple measures can include:

- Adopt written policies to address social networking as it pertains to your business activities, employees, and information. Social networking policies should be consistent with the organization’s policies and procedures on confidentiality and trade secrets; protection of the organization’s property; harassment and discrimination; privacy of employee/customer information; computer, internet, e-mail systems; and employee privacy

- Publish and notify employees of the policies’ existence
• Train employees on these policies consistent with training on other key policies

• Enforce all policies consistent and uniformly

• Maintain “professional” accounts separate from personal accounts

• Prohibit employees from speaking on behalf of the organization without express authorization or approval

• Consider prohibiting supervisors, managers, administrators and professors from “friending” subordinates or students

Employers who may need to conduct surveillance or otherwise monitor employee activity, such as computer or internet use, should consider the following factors:

• **Prior Notice.** When possible – and without frustrating the objective of the surveillance – employers should provide prior notice to specific employees who may be subject to monitoring. In addition, employers should include the possibility of any monitoring or surveillance in its employee handbooks and policies.

• **Reasonable time, place, and scope restrictions.** Employers who make an effort to minimize the intrusiveness of surveillance or monitoring are less likely to be liable for a privacy violation. Thus, employers should take care to limit the place, time, and scope of surveillance as much as circumstances permit.

• **Employee’s expectations.** An employee’s reasonable expectation of privacy varies depending on the workplace environment. Employers should take extra precaution when conducting surveillance on enclosed or partially-enclosed office spaces, as opposed to more public areas such as hallways or lobby areas.

• **Employer’s business needs.** Employers should make sure that there is a legitimate business need for taking action that may be construed as an intrusion into employee privacy, such as loss prevention, ensuring the safety of others, or maintaining productivity.

With respect to harassment and discrimination policies, employers should consider adopting policies that prevent employees from “posting material that is abusive, offensive, insulting, humiliating, obscene, profane, or otherwise inappropriate regarding the organization, its employees, vendors, suppliers, business partners and competitors.” Further, internet usage policies should include language preventing employers from “engaging in any conduct that may be construed as harassment based on race, ethnicity, color, national origin, religion, sex, sexual orientation, age, disability, or any other legally protected characteristic.”

Confidentiality and trade secret policies should prohibit employees from disclosing or discussing in social networking activities customers, partners or suppliers by name; organization’s confidential information and trade secrets; and information regarding the organization’s clients, affiliates, partnerships. Importantly, employers must train employees on
the confidential information policy. Disparagement and defamation policies should clearly state that employees engaging in social networking and blogging for either personal or professional reasons must remain respectful of the organization, its employees, and vendors, suppliers, business partners and competitors. Further, employees should be prohibited from writing about, posting pictures of, or otherwise referring to any other employee without his or her permission. Employers’ cyber-policies should limit employees’ authority to speak on behalf of the organization. Unless the employee has explicit authorization to do so, he or she may should not use the organization’s name in the online identity (e.g. username, “handle,” or screen name), claim or imply that authorized to speak as a representative of organization, or use the organization’s intellectual property, logos, trademarks, and copyrights in any manner.

Finally, employers should make clear that its employees have no reasonable expectation of privacy on the organization’s computers, email systems, internet, and organization business (also address telecommuting situations). Employers should make sure its employees know that information exchanged on social networking sites can be accessed by the organization.