



Greater Louisville Inc.
The Metro Chamber of Commerce

WHITE PAPER **The Evolving Electronic Workplace**

Contributed by: **Fisher & Philips LLP**
Published: **June 2011**

I. The Use Of Social-Networking Sites To Screen Applicants

Recent studies suggest that the use of social-media sites, such as Facebook, MySpace, or LinkedIn, is an increasingly popular tool used by employers to screen potential job applicants. Because an increasing supply of information about individuals has been posted on the Internet, employers have the ability to obtain a wealth of details about potential applicants and their personal lives, including, for example, potential reading preferences, as reflected on an Amazon.com “Wish List.”

Further, encouraging current employees to “tweet” about job openings on Twitter may prove to be an inexpensive and quick way to locate a new hire. Information posted on social-media sites can prove to be useful tools in spotting resume fraud, immature tendencies that are incompatible with the workplace, or similar red flags. Also, in many instances, it is difficult for applicants to establish whether a prospective employer ever viewed their online profiles, as many sites do not provide information to site users about who has viewed their profile. Given the number of resumes employers commonly receive for advertised job openings, eliminating resumes of job applicants who can be seen doing inappropriate things on social-media sites has understandably proven to be a popular, and cost-effective way to screen applicants during the hiring process.

Nevertheless, employers who rely on social media as a hiring tool should recognize that there are potential risks inherent in relying on such sites. First, studies of prominent social-media sites have found them to lack racial diversity. Accordingly, hiring practices that rely heavily on recruiting through social-media sites or that require screening through these sites have the potential to give rise to claims of race discrimination. Moreover, the information that can be obtained through these sites may turn out to be information that employers cannot, by law, rely on in making an employment-related decision. Finally, as potential applicants are becoming more savvy about protecting their online identities, you should resist the temptation to attempt to evade privacy measures applicants have taken in an effort to shield their personal information from the public.

A. Beware Of Possible Discrimination Issues

Recent surveys of sites such as LinkedIn suggest that a significant number of users on these sites are white and between the ages of 20 to 40. Thus, heavy reliance on social-media websites during a recruiting process could result in a hiring process subject to challenge on the disparate impact grounds. Over reliance on social-media websites as a recruiting tool can result in an impermissibly homogenous applicant pool. Accordingly, employers that utilize social-media sites to screen applicants or to obtain resumes should avoid using these sites in a way that limits applicant pools by excluding groups that may remain underrepresented on these sites. Other sources of applicants should also be considered.



B. Receiving “Too Much Information” About Potential Candidates

Many employers have invested significant time and effort into implementing hiring practices that scrupulously avoid the possibility that an applicant could claim that a hiring decision was based on a legally impermissible reason. Employers generally do not ask for information about marital status, families or children, sexual identity or orientation, religious beliefs, disabilities, or union affiliations during the hiring process in order to reduce the possibility that a rejected applicant would file a discrimination suit. Nevertheless, employers that use publicly-available information on the Internet, such as Facebook profiles, risk undermining the legality of their screening processes because these profiles are often riddled with information that an employer may not rely upon to make a hiring decision.

In many instances, these profiles contain information that an employer would have no legitimate business reason to consider during the hiring process, as individuals will post photos of themselves with their immediate families, provide information about marital status, sexual orientation, pregnancies, disabilities, and religious affiliations, or comment on other aspects of their personal lives in ways that could be considered protected characteristics under applicable anti-discrimination laws.

In order to reduce the risk of possible claims, carefully consider how you intend to screen candidates when using online profiles, and the job-related purpose of the information being obtained. Steps to consider may include having the actual social-media profiles reviewed by someone who is not a decisionmaker in the hiring process. Also, limit information from these sites to legitimate hiring considerations, such as cross-checking dates of hire and college degrees listed on resumes against LinkedIn profiles, or by reviewing recommendations from prior employers that may have been posted.

By limiting the access of decisionmakers to job-related information contained on social-media sites, you may be in a better position to fend off a claim that an applicant was denied a position because you considered information that was protected by state or federal law.

C. Potential Privacy Claims

Finally, if you rely on information gathered from social-media websites be sure to obtain this information in a lawful manner. For example, if obtaining reports about applicants through third-party vendors, ensure that this information has been gathered in a manner consistent with the Fair Credit Reporting Act, or other background check requirements that may apply.

In addition, do not use techniques, such as creating “dummy” profiles, in order to obtain access to information that an applicant has taken steps to prevent access by the public, or otherwise utilize pretext to investigate applicants. Be cognizant of state laws in certain states that prohibit employers from taking an adverse employment action based on information suggesting that applicants were engaged in lawful conduct during non-working hours, such as smoking, drinking alcohol, or engaging in consensual sexual activities.

To reduce the risk of possible adverse claims, develop written policies that define who will conduct applicant screenings using these sites (preferably employees who lack decisional roles in the hiring process), and prohibit attempts to obtain non-public, restricted-access information from social-media websites. In these ways, in the face of potential claims alleging wrongful use of information from such sites, you will be better prepared to show what information was actually considered, and the legitimate business purpose for obtaining the information that was gathered.

II. Social Networking and the National Labor Relations Act

Congress had no idea in 1935 when it passed the National Labor Relations Act (NLRA) that employees would one day be able to “virtually” communicate with co-workers, express their opinions about management, and participate in organizing activities. Nevertheless, the current National Labor Relations Board takes the position that the NLRA was intended to protect such conduct.



A. Concerted Activity

The NLRA establishes and protects the right of employees to engage in “concerted activity.” Generally speaking, concerted activity occurs when two or more employees act together for their mutual aid and protection. The Board has long recognized that concerted activity includes employees discussing with one another, and collectively with their superiors, the terms and conditions of their employment.

It has also recognized that concerted activity includes employees openly criticizing their employer and management, provided the criticism does not rise to the level of disloyalty, recklessness, or malice, and does not unduly interfere with the employer’s business interests.

Finally, concerted activity includes participating in pro-union organizing activity without fear of retaliation. The evolution of social-networking sites such as Facebook, Twitter, and YouTube has forced the Board to consider whether the principles under which these activities were found to be protected are applicable in the digital age.

B. Facebook

Facebook has over 500 million users worldwide. It is the premier social-networking site. Facebook describes itself as “a social utility that helps people communicate more efficiently with their friends, family *and coworkers*.” Consequently, it is not surprising that Facebook has caused unfair labor practice concerns.

1. American Medical Response Of Connecticut

The NLRB’s Connecticut Regional Office (Region 34) issued a complaint in October 2010 against a Connecticut ambulance service, American Medical Response of Connecticut, (AMR) alleging that one of its union-represented emergency medical technicians was unlawfully fired after criticizing her supervisor on Facebook. The complaint also alleged that the company’s blogging and internet policy was overbroad and therefore had the effect of “chilling” employees in the exercise of their rights under the NLRA.

a. Facts

The Board explained in a press release announcing the complaint that the employee posted harsh and negative comments about her supervisor on her personal Facebook page after her supervisor addressed a customer complaint with her. This prompted the employee’s Facebook “friends” (some of whom were co-workers) to post inquisitive and supportive replies. The postings got back to the supervisor, and the employee was subsequently terminated. The company maintains that the employee’s Facebook posting played no role in her termination, and that she was terminated because of patient complaints.

b. Outcome

AMR settled the complaint in February 2011. Under the terms of the settlement, which the Board publicly disclosed, the company agreed to revise its blogging, Internet, and communication policies to ensure they do not improperly restrict employees from discussing their wages, hours, and working conditions with co-workers and others while not at work.

The company further agreed that it would not discipline or discharge employees for engaging in such discussions. The allegations involving the employee’s discharge were reportedly resolved through a separate, private agreement between the company and the employee.

c. Implications

While this marked the Board’s first reported charge against an employer for firing an employee who complains about a supervisor on Facebook, it was not the Board’s first attempt to protect employee speech through electronic media. The Board had previously held that employees have the right to engage in free speech as a form of “concerted activity” for their “mutual aid and protection” through website postings and emails. But employees are generally not protected when



their speech is clearly personal in nature and is disloyal, reckless, or malicious, or if it unduly interferes with the employer's business interests.

Although the Board was not advancing a novel theory of liability against AMR, the tremendous attention that social-networking websites such as Facebook have received in recent years makes this case stand out and gives employers cause for concern. The Board's complaint serves as a strong reminder that employers should proceed cautiously before disciplining or discharging employees for expressing criticism over the Internet. You should review your electronic communication policy to ensure that it is not overbroad.

2. Student Transportation Of America

The Board will likely get a chance to revisit this issue in light of a recent unfair labor practice charge filed against a Connecticut bus company, Student Transportation of America (STR).

a. Facts

Unlike the *AMR* case, the charge against the bus company does not allege improper discharge, but rather alleges that STR unlawfully maintained and enforced overbroad communication policies. Specifically, the charge attacks the following language from the company's employee handbook:

- "This handbook and the information in it should be treated as confidential."
- "The use of electronic communication and/or social media in a manner that may target, offend, disparage, or harm customers, passengers, or employees; or in a manner that violates any other company policy."
- "Disruption of the workplace operations caused by deliberate actions and/or statements, causing serious morale problems among fellow employees and/or undermining supervision, company policies or rules. Making demeaning/derogatory statements about the company, fellow employees or its customers."

b. Likely Outcome

Based on the settlement reached in *AMR*, the Board is likely to find the above language in the bus company's policy overbroad as well.

C. Social Networking During A Union Campaign

Social-networking websites are beginning to play a greater role in union organizing campaigns. Unions are increasingly taking advantage of social media as a means of organizing and communicating with employees. Employers, on the other hand, are finding that social-networking sites merely increase their risk of receiving an unfair labor practice charge. It is clear that social networking works more to the union's advantage.

1. How Unions Are Using Social-Networking Sites

Almost every union has a website. But with the evolution of Facebook, YouTube, and Twitter, unions now have a much more personal and direct way to target and influence their intended audience.

A 2008 survey by Cornell University revealed that 54% of the surveyed unions were using Facebook to help workers connect and share opinions and ideas during organizing campaigns. And with the NLRB taking a more active approach to protecting rights of those who use electronic media to express opinions, union reliance on Facebook to reach out to workers will likely increase.



Unions also frequently use YouTube to broadcast their message to a wide audience that they would not otherwise be able to reach collectively. In the past, unions expended considerable resources traveling around the country to organize. Now, from a central location and at minimal expense, they can broadcast their message and receive feedback.

Unions also use Twitter as a means of quickly sharing news and organizing information, and they use text messaging the same way. Text messaging also allows unions to circumvent employer policies prohibiting or restricting Internet access during work hours. Indeed, many unions are now requesting cell phone information, as well as email information, on authorization cards.

2. Why Employers Are Cautious Of Social-Networking Sites

Employers appear to be using social media in the organizing context much less frequently than unions. Given the Board's recent attacks on overbroad social-networking policies, retaliatory terminations, and improper surveillance, companies are reluctant to extend their anti-union message through a medium that invites public comment and provides a permanent record.

To the extent companies are inclined to use social media to influence workers, YouTube will likely be the preferred method of communication. Recently, Hyatt Hotels Corporation released a YouTube video directed at employees in the midst of a 17-month bargaining dispute. In the video, an actor communicates messages such as, "The union is using you as a bargaining chip in a dispute that has nothing to do with you or us." While Hyatt's use of YouTube is not in the organizing context, the same principles apply.

YouTube allows a company the ability to convey a single message to all of its employees at their homes – something that would otherwise be prohibited under the NLRA. It can also be a more cost-effective way of communicating, as it does not require the company to call a mass meeting during work time. But there are downsides.

First, anyone – not just employees – can access a video posted on YouTube. Thus, union organizers would be privy to the company's anti-union speeches. Moreover, YouTube, like Facebook, invites public comments. Accordingly, organizers and pro-union employees can easily comment "publicly" on the employer's message.

D. Steps You Can Take

The first step employers can take is to draft narrowly-written policies that protect their interests, but at the same time allow for protected employee expression. The NLRB complaint notwithstanding, employer social-media policies can continue to prohibit the same kind of communications that have been traditionally prohibited around the water cooler. That is, harassing, discriminatory or defamatory speech should be specifically prohibited. Communications that reveal confidential or proprietary information or company trade secrets should also be prohibited, as should confidential client information, such as medical records (in the case of a hospital or other healthcare employer) or other protected information.

Before taking action against an employee for "disparaging" speech, consider whether the communication could be considered "concerted activity" under the NLRA. Policies that are broadly drafted, such as policies that prohibit employees from discussing their workplaces in general, and supervisors and managers in particular, are probably overbroad and may be deemed a violation of the NLRA. Some possible indicators of "concerted activity" to consider are whether the post is directed at other employees and whether the post encourages or suggests that fellow employees work toward improving working conditions. The communication may be explicit or implicit.

If the post is somehow related to previous employee or group activity, particularly if initiated by a "spokesperson," this also could be construed as concerted activity. If the answer to any of these inquiries is "yes," proceed with caution before taking disciplinary action.



Likewise, policies that prohibit employees from discussing pay¹, work schedules, hours, physical safety, dress and appearance codes, or work assignments may be construed as communications “for the mutual aid and protection” of employees, and may be protected under the NLRA. If a post purports to alert the public to health and safety conditions or violations in the workplace, urge employees to take some action, or vote a certain way on pending legislation, or criticize an employer’s policies, those communications may also be protected, and employers should proceed carefully before taking disciplinary action.

This does not mean that all concerted communications are acceptable, however. In order to be protected, such communications must be reasonable; they are not protected if they are “unduly and disproportionately disruptive.” The “disloyalty” exception to the protection of concerted activities under the NLRA carves out from protection speech that disparages an employer’s business or is patently disloyal. But in light of the recent NLRB complaint, such exceptions should be narrowly construed.

In addition to NLRA concerns, employers must also be mindful of state laws that protect employees’ legal, off-duty activities from discipline. Such laws were initially drafted to protect employees who smoked or engaged in other legal, but perhaps distasteful-to-the-employer activities, in their time off work. Recently, creative plaintiff-side attorneys have been pushing the application of these laws, initiating a range of actions perhaps not even conceived at the time the statutes were drafted, such as protecting employees’ rights to use medical marijuana, as well as protecting employees’ rights to express themselves in social media. Although they vary by state, the laws typically limit the actions an employer can take against employees who engage in legal activity on their own time, however unpleasant that activity might be to the employer.

Social-media policies should define the scope of permissible communications and should cover all internet-based communications, including personal blogs, Twitter, social-networking site posts, LinkedIn, and chat forums. While employees may discuss their wages and other working condition information, they may not disclose confidential or proprietary information, trade secrets, protected health information, or other private customer information.

Under Federal Trade Commission rules, employees must disclose their employment relationship to an employer whenever communicating information about that employer, and can be prohibited from using company logos. Employees should make clear that they are expressing their own opinions, and not those of the company or its management.

E. Conclusions

The fundamental advantage that employers have over unions during organizing campaigns is control. Unions are increasingly relying on alternative methods of communication because they are restricted as to when, where, and how they can meet with employees. Employers, on the other hand, have a great deal of control over those elements. Moreover, employers are at a much greater risk for unfair labor practice charges arising out of the use of social media during organizing campaigns, including charges alleging surveillance and retaliation. Thus, it is not surprising to see social-networking websites having a greater positive impact on union organizing activity.

III. The Stored Communications Act

The Stored Communications Act (SCA) is a federal statute that makes it illegal for an individual or an entity to intentionally access, without authorization, private electronic communications that are stored with an electronic communications provider or service. The SCA expands the protections of the previously enacted Electronic Communications Act, and creates privacy protections in electronic communications such as emails and discussions in chat rooms. Courts have held that social-networking sites, internet-based email services such as Gmail and Hotmail, and web-hosting providers fall within the SCA’s protections.

¹ In addition to the NLRA, some states have specifically outlawed such prohibitions.



A. Unlawful Access To Employee Forum

Increasingly, employees are taking to the internet to vent (or rant) about their employers, supervisors, and co-workers. If the rantings are posted on a publicly-accessible Internet page, employers have a right to view, access, and take action based on the postings, subject to the limitations discussed in other sections of this paper. But a recent decision by a Federal Court in New Jersey, however, underscores the risk faced by employers if supervisors or managers improperly gain access to online venting. In *Pietrylo v. Hillstone Restaurant Group d/b/a Houston's*, two former restaurant employees were awarded damages after managers accessed a private online chat room and used information obtained from the forum to terminate the employees.

The creator of the chat room was a server at a restaurant and, in his personal time, maintained a MySpace page which included a private chat group called the Spec-Tator. The Spec-Tator was a forum for Houston's employees to "talk about all the crap/drama/and gossip occurring in [their] workplace, without having to worry about outside eyes prying in . . ." According to the lawsuit, users of the Spec-Tator used the chat room to discuss wages and other issues related to their employment.

Several co-workers were invited to access the forum and provided a password. No members of management were invited or permitted to access the forum, the server maintained the forum in his off-duty time, and the forum was never accessed using the employer's computer or network. Management learned about the forum and requested that a greeter, who had been granted access to the Spec-Tator, provide her password to the site. Management accessed the forum on multiple occasions, reviewed the posts, and terminated two employees for content that was posted in the forum.

The two employees filed suit against Houston's alleging that the restaurant's managers violated the Stored Communications Act (SCA) and state law when they accessed the Spec-Tator. At trial, Houston's argued that the managers did not violate the SCA because they were given a password to access the chat room by a member of the group and, therefore, access to the forum was authorized. The jury found that the employee had not provided her password voluntarily, but rather provided it under duress because she felt compelled to provide the password to her manager to avoid getting into trouble. Furthermore, the Court determined that there were reasonable grounds for the jury to determine that the managers intentionally accessed the Spec-Tator despite their knowledge of the employee's discomfort with their use of her password.

B. SCA Protections Are Expansive

A decision by a Federal Court in New York demonstrates that the courts are willing to interpret the protections of the Stored Communications Act broadly and in favor of the protection of employees' privacy rights and expectations.

In *Pure Power Boot Camp v. Warrior Fitness Boot Camp*, an employer accessed the work computer of a former employee and log into the employee's Hotmail account because the employee had left his username and password stored on the computer. The employee had accessed the Hotmail account while at work. Therefore, when the employer pulled up the Hotmail page, the username and password were automatically populated. Notwithstanding the finding that the password was stored on the employer's computer and the website had been accessed at work, the Court found the employer's access of the account violated the Stored Communications Act.

C. Exercise Caution

The jury's verdict in *Pietrylo* and the findings of the New York Court demonstrate that employers should tread with caution when accessing an employee's restricted web page. If the employee takes steps to limit access to such information, or to make such information private, gaining access by using someone else's credentials may violate the SCA.

If you believe that you need to access a private website, consider whether the risk of access outweighs the necessity. If you receive consent to access a private or restricted site, document the access in a signed acknowledgement.



IV. The Legal Implications of Using GPS to Track Employees

As many employers have discovered, there are many benefits to the use of global positioning system (GPS) technology in their businesses. GPS devices use a satellite-based electronic system to identify the location of objects in real time. Tracking devices have become relatively inexpensive, and may be installed into cellular telephones, PDA devices, automobiles, identification badges or key fobs, among other locations. Recently, for example, a criminal in New York City was convicted of robbery based on evidence obtained from the GPS tracking device, which had been installed in the getaway van – a vehicle owned by a medical transportation company.

Other employers have relied on GPS tracking data to discipline employees who have claimed to have been working when GPS data showed that the employees were engaged in non-work-related activities. Companies that maintain fleets of delivery vehicles have been able to use GPS tracking to increase efficiency, lower fuel costs, and address other customer issues. In short, employers in some industries may be able to use GPS tracking to increase productivity or customer service, promote responsible employee behavior, or reduce labor costs.

Despite all of these potential benefits, employers considering the use of GPS devices should proceed with caution in order to reduce the risk of potential privacy considerations, labor relations issues, and wage-hour concerns that this sort of monitoring has the potential to create. Judicial views on the use of GPS data are evolving, and courts have not yet provided a consistent message on the question of whether GPS monitoring implicates any privacy rights.

Employers with unionized workforces should also be wary of creating possible unfair labor practices claims. Finally, to the extent that employees subject to GPS monitoring are entitled to receive overtime compensation under applicable state or federal laws, employers will want to ensure that GPS tracking records do not suggest that employees were engaged in working activities during time periods that they were not receiving compensation.

A. Employee Privacy Rights

Many employees are naturally concerned about their employers' ability to track their whereabouts and movements across the course of the day. Broadly speaking, courts remain divided on the question of whether the use of GPS tracking creates a privacy concern – some courts have held that a person's location is inherently public information, while other courts have noted that a person's location can be used to obtain information about an employee's private personal habits, such as whether an employee visited a hospital, rehabilitation center, or religious institution.

Currently, federal appellate courts have split on the issue of whether the Fourth Amendment requires a warrant before law enforcement authorities may use GPS devices to track an individual's movements. While criminal precedents and governmental-monitoring cases are not directly binding in the private context, case law interpreting Fourth Amendment requirements could provide guidance to courts that may be grappling with the question of what is an employee's reasonable expectation of privacy with respect to spatial privacy.

In order to reduce the risk of a potential claim, employers using GPS tracking should provide a clear written policy to all employees subject to monitoring. As with other privacy-related claims, the dissemination of a written policy may be sufficient to demonstrate that the employee in question consented to GPS monitoring, and, accordingly has no legal claim based on an invasion of privacy. Moreover, at least one state – Connecticut – has an express statutory requirement to notify employees of possible GPS monitoring. In California, it is a possible misdemeanor to use a device to track the movement of another without prior consent.

Of particular importance, GPS-related policies should indicate whether and to what extent the employer may obtain information about employees during non-working hours, *e.g.*, an employee driving a company-owned vehicle on a day off. Because employees may object to being monitored outside of normal working hours, employers implementing GPS policies should strongly consider whether to include instructions to employees about how to turn off monitoring devices that they may be carrying during off hours.

Employers should also consider creating controls to prevent unauthorized access to GPS data in order to avoid possible claims arising from deliberate "snooping" – or even stalking – by their employees. For example, GPS monitoring



may disclose for the first time to an employer that an employee has a possible disability or religious affiliation that would otherwise have remained unknown to the employer. The employer, in turn, could face possible discrimination claims based on having learned information about an employee that otherwise would not have been available.

Similarly, to the extent that GPS tracking shows that an employee has a tendency to engage in risky behavior, such as speeding, or drinking and driving, an employer may face a claim for negligent supervision for failing to act on such evidence. Moreover, many states prohibit employers from disciplining employees based on their conduct during non-working hours. Again, the risk of such claims may be reduced by careful consideration of when to turn GPS devices “off” in order to decrease the chance of learning information about employees that has no benefit to employers.

B. Monitoring Unionized Employees

Employers with unionized workforces face potential additional liability under the National Labor Relations Act. Employees may claim that GPS monitoring devices are being used by management in order to impede union activities by allowing management to track possible organizing activities. Moreover, the use of such monitoring devices may be found to be a mandatory subject of bargaining in some instances.

Unions seeking workforce recognition may seize upon inadequate GPS policies or arguably overzealous monitoring activities in order to bring unfair labor practices charges at the outset of an organizing campaign. These considerations further highlight that employers should use caution when installing devices that have the potential to track employees outside of normal work activities or in ways that have not been thoroughly explained to affected employees. As with other technology-related issues, the potential labor-related implications of GPS devices remains a moving target that has the potential to create disputes.

C. Potential Wage And Hour Issues

Use of GPS monitoring devices has the potential to create wage-hour headaches, especially with respect to hourly employees. Already, employers have been subject to claims that employees who check emails on weekends or use other electronic devices during non-working hours need to be paid for these activities. Although the issue has not yet been addressed by a court, employers should recognize that employees whose activities are subject to electronic monitoring by an employer may be viewed as being engaged in compensable work activities, regardless of the intent of the employers.

On the other hand, employers who allow employees to turn off monitoring devices during non-work hours may, in some case, be able to suggest that employees are not entitled to compensation after employees voluntarily disable GPS equipment as part of a “clocking out” process. These concerns again underscore the importance of carefully considering the use of GPS technology, and the distribution of clear written policies to employees that include information about when these devices may be used by employers, and when employees have the right to turn off monitoring devices.

V. State Privacy-Related Tort Claims

How and when you may legally monitor or access your employees’ communications is largely regulated by federal laws such as the Stored Communications Act, the Federal Wiretap Act, and even the National Labor Relations Act. But some states, including Connecticut and Delaware, also have in place state laws that require employers to provide notice to employees prior to monitoring communications. Other states, such as Massachusetts, Pennsylvania, and New York, currently have legislation pending to implement similar laws.

In either of these regulatory schemes – federal or state – the punishment for an employer who improperly monitors an employee’s communications is levied in the form of a civil or criminal fine and injunctive relief (i.e., an order for an employer to cease its improper conduct). These monetary penalties are designed to punish the employer for engaging in improper conduct and to deter the employer from engaging in such conduct in the future. However, those penalties are not paid to the employee. Therefore, employees who believe that they have been personally harmed as a result of an employer’s alleged misconduct may turn instead to state tort law for a remedy.



A. Violation Of Privacy Rights

The basis for any tort action against an employer for accessing or monitoring an employee's communications rests on violation of the employee's privacy rights. Thus, an employee's claims against an employer focus more on the impact of improper access or monitoring and less on the actual method that the employer used. The most commonly used tort actions against an employer for improper monitoring of communications are: 1) intrusion into the privacy of another; 2) appropriation of one's name or likeness; 3) wrongful publication of private facts; or 4) placing one in a false light. Although these four tort claims are referred to differently from state-to-state, the basis for each of them is the same. Specifically, each of these tort claims arise from an employee's expectation of privacy in the information or facts that have been disclosed or used in an improper manner.

The most commonly used privacy-related tort against an employer for monitoring communications is intrusion into the privacy of another. This claim is typically established by an employee who proves that an employer intentionally intruded, either physically or otherwise, into the solitude or seclusion of the employee or his or her private affairs. The employee's right is violated at the time of the wrongful intrusion, and not when he or she learns of it or experiences some form of harm. Every intrusion by an employer is not actionable, so in order to establish a cause of action against an employer for invasion of privacy, the employee must prove that there was a reasonable expectation of privacy in the information that is accessed or monitored.

Because the key to employees' claims of invasion of privacy is proving their expectation of privacy, it is vital that an employer maintains a policy regarding use of company-owned devices to communicate. An employer may avoid liability for invasion-of-privacy claims where it has effectively communicated its policies on the use of electronic communications, putting employees on notice that they should not have a reasonable expectation of privacy in communications made using company-owned computers or other devices.

And when the communication at issue is made during work hours, employees have faced difficulties establishing that an employer's monitoring of communications is unreasonable as the communication was made during a time when the employer is paying the employee to work, and providing the equipment to do so.

B. Wrongful Termination

Often, the harm that an employee suffers as a result of an employer's improper access or monitoring of an employee's communications is not merely an infringement on privacy, but termination. Most states recognize some form of tort claim for wrongful termination based on public policy. Typically, employees are successful in maintaining such a cause of action where the employer violated a law in terminating the employee.

Thus, where an employer violates federal or state law in monitoring or accessing an employee's communications, and then terminates the employee based on information that it obtained from the communication, the employer may face liability for wrongful termination. States such as California, Colorado and New York have state laws that prohibit an employer from terminating an employee for engaging in lawful conduct while off duty.

C. Infliction Of Emotional Distress

Most states also recognize some form of action for an employer's intentional or negligent infliction of emotional distress. This cause of action is typically proven where the employer knowingly or recklessly engaged in conduct that it reasonably knew would inflict emotional harm on an employee. In those states that recognize this cause of action, the employee has a difficult burden of showing not only that the employer knowingly or recklessly engaged in such conduct, but, more importantly, that the conduct was extreme, outrageous, or so intolerable that a reasonable person could not be expected to endure it.

In the employment context, an employer's merely accessing or monitoring an employee's communications would not likely rise to the level of conduct necessary to meet this burden. However, if an employer knowingly violates an employee's privacy and then intentionally publicizes private information to others in order to harass an employee, a court



could find that the employer's conduct was sufficient to establish a claim – even if the employee had no expectation of privacy in the information.

VI. Monitoring Employee Email And Voicemail Communications

Modern technology makes the workplace more efficient and productive than in years past, and also makes it easier for employers to keep an eye on what employees are doing. Federal and state laws, as well as common-law privacy rights limit employers' legal rights to monitor employees' oral and electronic communications, both at the time the communications are sent and afterward.

A. Federal Law Protects Communications During Transmission

Any contemporaneous monitoring of “wire, oral or electronic communications” (which includes email and voicemail) is subject to the federal Wiretap Act, as amended by the Electronic Communications Privacy Act of 1986 (EPCA).

The Wiretap Act generally prohibits the interception, disclosure or intentional use of wire, oral or electronic communications, including those that occur in the workplace, subject to certain exceptions. However, it does not create a general right to privacy in all telephone or email communications.

1. Wire, Oral And Electronic Communications Are Defined Broadly

Under the Wiretap Act, “wire communications” include telephone calls and voicemail. An “oral communication” occurs when the individual uttering the communication expects it to be a private conversation. “Electronic communications” include the transfer of information (writing, images, signals, sounds, data, etc.) by electronic means – such as email, pagers, mobile telephones and text messages.

“Interception” is the aural or other acquisition of the contents of any oral, wire, or electronic communication, through the use of any electronic or mechanical device. Interception must happen at the same time that the communication is being transmitted. For example, intercepting a call with a tape recorder connected to a switchboard without an employee's knowledge is a violation of the Act.

a. Exception: Prior Consent

There is no violation of the law if one or more parties consents to the taping or interception before it occurs. Whether an employee has consented may be based in part on what notice the employer has provided about the monitoring it intends to do in the workplace. In all cases, employers must be sure that employees do not have an expectation of privacy.

b. Exception: Business Extension

It is not a violation of law for employers to monitor their own telephone lines in the ordinary course of business. This exception allows an employer to electronically monitor, using a telephone extension, any business-related communication without the employee's knowledge or consent. Of course, employers should have a valid business justification for doing so, and should avoid monitoring personal calls.

c. Exception: Provider Interception

Providers of wire or electronic communications services may intercept or use communications in the normal course of employment if necessary to provide the service or to protect the rights and property of the provider. This is an unsettled area of law, but some cases have held that an employer that maintains an internal email system may be a “provider.”



2. State Wiretapping Acts May Impose More Stringent Requirements

In addition to federal law, all states except Maine and Vermont and the territory of Puerto Rico have laws mandating notification and consent for monitoring by private employers. Some state laws are similar to federal law, but others are more restrictive. For example, in some states, prior consent of all parties – not just one – is required before telephone conversations can be monitored or recorded. Be sure to check state and local laws for any additional requirements that may apply before implementing a monitoring program.

3. Penalties

Violation of the Wiretap Act is a felony punishable by a fine or imprisonment. The Act also provides a civil cause of action to anyone whose communications are unlawfully intercepted. Prevailing plaintiffs can recover statutory damages of \$10,000, \$100 per day of violation or actual damages, whichever is greatest; plus punitive damages and attorneys' fees.

B. Federal Law Also Protects Communications After Transmission

Federal law prohibits the intentional interception, use, and disclosure of an “electronic communication.” Generally, employers do not violate the statute when reviewing employee emails in the workplace transmitted through the employer’s email system. An “interception” within the meaning of the statute does not take place if an individual gets a copy of the email once it is stored in the network computer. In addition, the federal Stored Communications Act regulates access to stored email communications.

1. “Ordinary Course Of Business”

Under the Electronic Communication Privacy Act, employers have the right to access employees’ stored emails in the ordinary course of business if the messages are maintained on an email system provided by the employer.

2. Communications Provider

The Stored Communications Act more broadly permits employers to access stored emails on email systems provided by the employer. However, note that employers may not use passwords stored on the employer’s system to gain access to employee messages hosted on third-party servers, such as Web-based private email accounts (Gmail, Yahoo) and social-media accounts, such as Facebook.

3. Common-Law Privacy Considerations

Besides federal and state laws specifically addressing the privacy of email, voicemail and other forms of communication, be mindful of privacy rights and other sources of protection, as in the case of personal communications protected by the attorney-client privilege. State constitutional provisions and common law may provide additional protections to employees where the employer has not taken adequate steps to reduce employees’ expectations of privacy in the workplace.

C. Employer Liability For Electronic Communications

An employer can be held responsible for the content of electronic communications under both the National Labor Relations Act (NLRA) and Title VII of the Civil Rights Act. Moreover, both Title VII and the NLRA require employers to protect employees against illegal harassment.

1. Harassment Prohibited By Discrimination Laws

Under Title VII, an employer can be held liable for the harassing actions of its employees if it knew or should have known of the offensive behavior but failed to act to remedy the situation. The EEOC and the courts have made it clear that employers are expected to stop harassment before it rises to the level of a violation of federal law.



If employees complain as a group about unlawful harassment, this may constitute “concerted activity” protected by the NLRA. An employer who fails to take effective measures to stop retaliation against employees who have made concerted complaints about harassment would also be guilty of violating the NLRA.

2. Email And Union Organizing Campaigns

Employees’ ability to use employer-provided email systems for union organizing efforts is an unsettled area of law, with constant tension between employees’ rights to engage in protected activity and employers’ rights to manage the business.

A 2007 decision of the NLRB held that employees do not have a statutory right to use employer e-mail systems for union-related activity. The now-Democrat-controlled Board may revisit this issue in the near future and expand employees’ rights, however.

Employers can prohibit use of their systems for “non-job related solicitations.” But employers should not monitor email and voicemail merely to determine whether and to what extent union activity may be occurring.

VII. The Eye In The Sky: Video Surveillance Of The Workplace

Adopting the use of video surveillance in the workplace can be a very effective way for employers to monitor employee performance, increase security at the workplace, and reduce theft of its property. In fact, employee surveillance is becoming a routine practice for more and more employers. Increasingly cheaper emerging technologies make it possible to monitor the workplace at a negligible cost. But with the increasing use of the technology, more and more employee privacy concerns have emerged.

According to a recent survey conducted by the American Management Association, approximately half of the companies surveyed use video monitoring to prevent theft, violence and sabotage. Only 7% use video surveillance to track employees’ on-the-job performance. Most employers notify employees of anti-theft video surveillance (78%) and performance-related video monitoring (89%). With this increased use of monitoring, employers must ensure that they are complying with any applicable laws governing same.

A. Employees’ Privacy Rights

Traditionally, employees have had few rights when it comes to protecting their privacy at the workplace. But as the use of video monitoring becomes more prevalent in our society, our legal system is being challenged with issues that have never been faced to this magnitude before. Legal cases are starting to emerge now as more employers begin monitoring employees using video surveillance and other electronic surveillance methods.

The general standard currently being used to judge privacy rights cases is that individuals are entitled to a reasonable expectation of privacy. Determining what constitutes a reasonable expectation is not clear cut. As more cases are tried, we will likely begin to see laws that are more specific regarding an individual’s right to privacy.

1. Video Surveillance Gone Too Far

Generally speaking, monitoring employees with video cameras likely won’t violate employees’ privacy rights. Still, at the very least, make sure that you don’t step over the line of reasonable privacy concerns by monitoring areas where employees have a reasonable expectation of privacy, such as dressing rooms and bathrooms.

In addition, labor unions may negotiate limitations on video recordings of unionized workers. In 1997, the National Labor Relations Board ruled that surveillance was subject to mandatory bargaining, meaning a union must agree to any monitoring of unionized workers. This includes the use of hidden cameras.



2. Additional Protections For Employees

Some states have also passed laws that deal with workplace privacy, including the use of cameras and video equipment. In California, for example, it's a crime to install a surveillance mirror (one that can be seen through from only one side and looks like a mirror on the other) in a restroom, shower, fitting room, or locker room. In Connecticut, employers may not operate surveillance equipment in areas designed for employee rest or comfort, such as restrooms, locker rooms, or employee lounges.

Among the restrictions set by states are those that:

- prohibit video monitoring in changing areas;
- require employer notice of monitoring practices; or
- make it illegal to record a conversation without consent of both parties.

B. Audio Recording

The most legally safe route is to use soundless video recording. Refraining from video surveillance with audio recording will keep employers clear from any possible violations of the federal Electronic Communications Privacy Act. Video cameras that also capture audio recordings may be subject to laws relating to audio recording, including wiretap and eavesdropping laws.

VIII. Lessons From The Supreme Court's *Quon* Decision

On June 17, 2010, the U.S. Supreme Court unanimously held that a public employer's search of an employee's text messages was reasonable and did not violate the employee's constitutional rights. The decision, *City of Ontario v. Quon, et. al*, marked the first time the Supreme Court had considered the privacy protections applied to text messages. The Court's analysis helped to define the boundaries of privacy protections in electronic communications. The decision's affirmation of an employer's right to conduct reasonable searches in furtherance of legitimate workplace objectives was a victory for employers in the era of the electronic workplace.

A. Use Of Company Pagers Nothing To LOL About

Since 1999, the City of Ontario, California, had a written "Computer Usage, Internet and Email Policy" which restricted employees' use of city-owned computers and associated equipment and programs, such as email. The policy, like many employers' policies, warned employees that they had no expectation of privacy in network activity and that the employer reserved the right to monitor and log all online activity.

Additionally, the policy strictly prohibited employees from using "inappropriate, derogatory, obscene, suggestive, defamatory, or harassing language in the email system." Sergeant Jeff Quon, an employee of the City Police Department, signed a statement acknowledging he had read and understood the policy.

Technology continued to evolve after the adoption of the policy and in 2001, the City obtained pagers with text-messaging capabilities and issued them to members of the SWAT team, including Sergeant Quon, so team members could more rapidly and effectively coordinate responses to emergencies. At the time, team members were verbally informed that all pager messages were considered email messages and, therefore, subject to the Computer Usage, Internet and Email Policy. Thereafter, employees received a memorandum expressly stating that messages sent on pagers were considered email messages and subject to the policy.

The pagers issued to SWAT members had a monthly character limit and a supervisor who had "fiscal responsibility" for the department oversaw the bills. The supervisor reminded Quon that messages sent on the pagers could be audited and adopted an informal practice whereby if an employee exceeded the character limit, he or she was



expected to pay the overage amount. The supervisor stated that if the overage amount was paid, he would not audit or review the messages.

Sgt. Quon exceeded his character limit on multiple occasions and each time paid for the overage. Ultimately, the supervisor grew tired of being the “bill collector” and the Chief of Police decided to audit the messages of two officers who exceeded the character limit to determine if overages were caused because the character limit set by the City was too low or if it was due to personal use of the pagers.

The City obtained and reviewed the transcripts for two months of messages. The supervisor determined that many of Quon’s messages were not work related and some were sexually explicit. The supervisor reported his findings to the Police Chief and Quon’s supervisor. After reviewing the transcripts, the Police Chief referred the matter to the internal investigations division and an investigator undertook an internal affairs review.

Prior to reviewing the text messages, the investigator redacted all messages sent or received while Quon was off-duty. Thereafter, he reviewed the content of the messages sent during work time and determined that in one month only 57 of 456 messages sent during work hours were work related. Several of the personal messages contained sexually explicit communications between Sgt. Quon and three individuals: his wife, a female co-worker with whom he was romantically involved, and another officer. Based on the investigation, Quon was found in violation of City rules and disciplined.

B. Legal Battle Reaches The Supreme Court

Soon after Sgt. Quon learned that his employer had reviewed his personal text messages, he and his messaging partners filed suit against his employer, several employees of the City, and the wireless company that provided the texting service. Quon asserted he had a reasonable expectation of privacy when sending the text messages and the City’s search was unreasonable. A jury found in favor of the City, and Quon appealed.

The U.S. Court of Appeals for the Ninth Circuit reversed the jury’s determination. The Court of Appeals determined that the City’s policy and practice of not auditing messages if overages were paid created an expectation of privacy in the content of employee’s messages. After finding that Sgt. Quon had a reasonable expectation of privacy, the Ninth Circuit analyzed whether the search was reasonable and determined the City’s search was not because it was not the “least intrusive” means to determine if Sgt. Quon was exceeding the character limit for work-related reasons. Accordingly, the court found that the search was unreasonable and, therefore, unlawful.

C. The Supreme Court’s Ruling

Searches and seizures of public employees’ property are subject to the Fourth Amendment. A public employer’s searches for work-related purposes are judged by a standard of reasonableness. Prior Supreme Court decisions suggested a two-step analytical framework for determining whether an employer’s search was unconstitutional. First, the Court had to consider the operational realities of the workplace to determine whether an employee had a reasonable expectation of privacy. Second, if the employee had a reasonable expectation of privacy, then an employer was permitted to conduct a search for “non-investigatory, work-related purposes, as well as for investigations of work-related misconduct,” if the search was reasonable.

In its decision, the Supreme Court noted that the parties disagreed whether Quon had a reasonable expectation of privacy. The Supreme Court expressly declined to determine whether Quon had a reasonable expectation of privacy. Eight of the Justices concluded that the judiciary “risk[ed] error” by defining the constitutional protections of privacy in electronic communications before the role of technology in our society has become clear. The Court noted, “[r]apid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior. ... At present, it is uncertain how workplace norms, and the law’s treatment of them, will evolve.”

The Court determined that a broad ruling on the scope of employees’ privacy expectations in employers’ technological equipment would be premature because society’s expectation of privacy in technology is still evolving.



Therefore, the Court presumed that Quon had a reasonable expectation of privacy and focused its decision on whether the search was reasonable.

The Court's decision not to issue an opinion defining or clarifying the standard for determining when an employee has a reasonable expectation of privacy in electronic communications means the law in this area remains unsettled and will continue to develop as technology develops. Importantly, the Court's opinion signaled that whether an employee has a reasonable expectation of privacy in electronic communications will be shaped, in part, by society's evolving perception of privacy in the era of social networking, text messages, and blogging.

D. Court Finds The Purpose Of The Search Was Legitimate and Reasonable

Generally, warrantless searches are unlawful under the Fourth Amendment. But the Supreme Court has recognized that an employer's search, when conducted for a non-investigatory, work-related purpose or for investigation into work-related misconduct is reasonable and permissible if two conditions are met: 1) The search was "justified at its inception" by a legitimate, work-related purpose; and 2) "[T]he measures adopted are reasonably related to the objectives of the search and are not excessively intrusive." The Supreme Court held that the search conducted by the City of Ontario satisfied both conditions and was a reasonable, lawful search under the Fourth Amendment.

The Supreme Court concluded that conducting a search to determine whether the character limit on messages was sufficient to meet the needs of employees and the City was a "legitimate, work-related rationale." In particular, the City had a legitimate interest in ensuring that employees were not paying overages fees for work-related messages and that the City was not paying for excessive personal communications by its employees.

Finding the search was justified by a work-related purpose, the Court next considered whether the scope of the search was reasonable in light of the circumstances. The Court concluded that "[a]s for the scope of the search, reviewing the transcripts was reasonable because it was an efficient and expedient way to determine whether Quon's overages were the result of work-related messaging or personal use."

Moreover, the Court noted that even if Quon had a reasonable expectation of privacy, it would not be reasonable for him to expect that all of his messages were immune from auditing or review because the pager had been issued by his employer, it was issued for a work-related purpose, and recovery of electronic communications might be necessary for certain work-related functions. All nine Justices concluded that because the City of Ontario's "search was motivated by a legitimate work-related purpose, and because it was not excessive in scope, the search was reasonable" and lawful.

E. Learning from Quon

Many employers, like the City of Ontario, have written policies that restrict employees' email and internet use; state that employees should limit their use of their work computers, email and devices for personal purposes; and warn that employees' activity and communications will be monitored. Many policies, however, have not been updated to reflect all of the mainstream forms of electronic communications.

Any internet or email policy should be updated to specifically address text messaging, the use of Company issued electronic devices, and the use of social-networking sites both during work hours and while off-duty. A policy should specifically state that employees' messaging and communications on electronic devices issued by an employer are subject to monitoring and that employees have no expectation of privacy in the use of such devices. The purpose for such policies is to dispel employees' expectations of privacy.

The Supreme Court's decision expressly noted that the City of Ontario's policy made clear that employees had no expectation of privacy. The Court declined to determine whether a supervisor's oral statements could override an official policy, so that is still an open question. Therefore, employers should not simply rely on the written policies to set employees' expectations of privacy in electronic communications.



Rather, you should audit their practices to ensure that neither your practices nor any “informal” policies are inconsistent with the written policy. Supervisors and managers should be reminded to never assure employees that their messages and online activity will not be monitored.

Finally, the law regarding expectations of privacy in electronic communications is more settled for private employers. Generally, employees of private companies lack an expectation of privacy when using their employer’s network or equipment. However, all employers should exercise caution when conducting a search of an employees’ electronic communications. Searches should only be conducted by employees who have been trained on an employer’s policies, including, but not limited to policies on electronic communications, harassment, and confidentiality.

Prior to conducting the search, an employer should be able to articulate a legitimate, work-related reason for auditing or searching communications, such as determining whether an employee is using work-time appropriately or whether an employee’s communications with a co-worker violated the employer’s harassment policy. Any search should be narrowly tailored to serve the purpose for which it is being conducted and the results of a search or audit should be communicated only to those employees who have a legitimate reason to know the content of the communications.

APPENDIX

Policy Recommendations for Social-Networking and Weblog Policies

In addition to information covered in this paper, employers should also consider the following issues when preparing their social-networking policies.

1. Define the conduct being regulated. Is the company only attempting to address email communications, or does the policy also address social-networking sites and blogs?
2. For any policy of this type, notify employees that any communications are subject to all of the company’s policies and procedures, including those on confidentiality, discrimination, harassment, and the company’s policy on the use of its electronic systems.
3. If the employer permits social networking for business purposes, this normally requires rules that are different than those established for personal social networking.
4. The limitations established on what type of communications are proper need to be carefully considered, especially in light of the NLRA concerns addressed earlier in this paper.
5. The company needs to determine whether employees are prohibited from listing company email addresses and company cell phone or office phone numbers in social-networking profiles, blogs, etc.
6. The company needs to decide whether it will prohibit personal activities involving Internet blogging, social networking, and other online activities while on company time, property, or business. Due to the impracticalities of a complete ban, a limited use policy may be worth considering.
7. The company may wish to limit or prohibit the use of the company’s logo and trademarks.
8. The company should prohibit the use of a picture or likeness of any supervisor, manager, employee, customer, etc. without their express written permission. Many companies prohibit the use of photographic or video equipment within their premises. If so, this policy should be cross-referenced.
9. For personal social networking, the company should decide whether it wants employees to post a disclaimer when discussing work-related matters, making it clear that these are their own opinions, and that they are not approved by the company and do not represent the views or opinions of the company.



10. Policies of this type should warn employees that they have no expectation of privacy when using the company's electronic communications and Internet service.

11. The policy should explain that employees are personally responsible for all commentary they express and material they post on the Internet.

12. The policy should make it clear that the company owns its computer system and information stored on it. As a result, the company may access any and all information on its computer system (subject to privacy issues discussed elsewhere in this paper).

13. The company should ensure that employees are educated on the policies and expectations. To accomplish this, companies should consider having a notice pop up on the computer screen on a regular basis, as well as hard copy signed acknowledgments of the policy through the company handbook or otherwise. Additionally, this policy should be reviewed during orientation and other employee training.

If your company engages in other types of electronic monitoring of employees, such as GPS, telephone recording, videotaping, etc., you should draft separate policies addressing the monitoring, notifying employees that it is taking place, and taking steps to ensure that the legal issues outlined in this white paper are properly addressed.

The law governing the electronic workplace is in the development stage. For this reason, it's a good idea to consult employment counsel when drafting policies of this type. Additionally, these policies should be reviewed annually to ensure that they are updated to reflect the latest legal trends.

The foregoing provides an overview of certain legal issues. It is not intended, and cannot be construed, as legal advice for any purpose. For more information contact an attorney in Fisher & Phillips' Louisville, Kentucky office (502-561-3990).

