The Privacy Rights of Employers and Employees (Part 2)

Cristina Portela Solomon and Stephen W. Schueler

Monitoring communications and workplace surveillance can be tricky. But they can also be good for both the employer and employees.

▲ ▲ ▲

PART 1 OF THIS ARTICLE explored some of the privacy concerns that employers are likely to have with respect to intellectual property. This Part will continue with an examination of how to protect trade secrets, website privacy issues, and two topics of special concern to employees: how and when the employer can monitor employee communications and surveillance of the workplace.

Cristina Portela Solomon and **Stephen W. Schueler** are partners with Winstead Sechrest & Minick P.C., in Houston. This article is based on a paper the authors prepared for a seminar sponsored by the ABA's Section of Labor and Employment Law.

MONITORING EMPLOYEE COMMUNICATIONS IN THE WORKPLACE • Can an employer lawfully "spy" on its employees? The phenomenal growth and influence of the Internet has created new issues and concerns for employers everywhere. Employers want to take advantage of the convenience and connectivity offered by the Internet, but along with these advantages come a myriad of potential legal problems. For example, employees sometimes make inappropriate use of the Internet, which, at a minimum, wastes productive employee working time, and, at worst, can lead to costly and time-consuming litigation. Email is particularly troubling, as employees often incorrectly believe that email is a secure system, and do not realize that a message, joke, or anecdote sent to coworkers could reappear years later, particularly as smoking gun evidence in an employment discrimination case.

The stakes are high for employers: litigation centering around evidence harvested from company email systems is multiplying, and the growth of email-related claims is particularly evident in employment litigation, in which an off-color joke or a sexually provocative email may be the primary evidence in a discrimination claim.

Corporations across America are addressing this issue. A recent survey of workplace monitoring and surveillance of employee activity reveals that nearly three out of four major U.S. companies monitor employee conduct on the job, and more than half of major U.S. companies monitor Internet connections. The reasons these companies give for monitoring include productivity, the need to protect against legal liability and the need to monitor the performance of their employees. Additionally, one out of five companies has disciplined an employee for inappropriately using the Internet, according to *PC World* magazine.

Stories of Internet-related terminations and discipline are becoming increasingly common. For example, the *New York Times* terminated 20 employees for sending "inappropriate and offensive email," and Xerox terminated 40 employees for failing to heed Xerox's computer policy. In nearby Freeport, Dow Chemical fired 24 employees and reprimanded 235 employees for misusing email by sending sexually explicit and violent images.

To combat this problem, many employers are rushing to purchase tracking devices and software to monitor employee behavior, but what companies truly need to easily and effectively protect themselves is a simple privacy policy. This privacy policy, which should make clear that an employee has no reasonable expectation of privacy when using employer-owned computers and software, can go a long way to protecting both the employer and the employee from lawsuits and embarrassment.

Electronic Communications In The Workplace

Employers must increasingly consider the expanding rights of employees in all facets of their work. As technology usage continues to expand, employers must consider a wide array of monitoring methodologies, some of which include electronic surveillance. Additionally, employers who do monitor and gather employee information, in some instances, find themselves subject to certain affirmative duties to disclose the information obtained to employees.

An employer's ability to monitor employee behavior is limited by the U.S. and state constitutions, assorted federal and state statutes, and privacy law developed through common law. Nevertheless, employers risk liability for conduct or communications that are conveyed by electronic means. Severe and pervasive conduct may occur in the form of voicemail messages and untoward email messages. Similarly, open

displays of objectionable Internet sites or postings are akin to displays of nude photographs and calendars.

Can Employers Monitor Employees' Computer Use And Telephone Calls?

The Federal Wiretapping Act, as amended by the Electronic Communications Privacy Act of 1986 (the "Act"), 18 U.S.C. §§2510-2521, generally prohibits the interception, disclosure, and intentional use of wire, oral, and electronic communications. Anyone who has had a communication improperly intercepted may bring a civil action against the violator for actual and punitive damages, as well as attorneys' fees. Violators of the Act are also subject to fines or imprisonment.

A detailed discussion of the provisions of the Act is beyond the scope of this article. However, there are two exceptions for employers that clearly apply to employer monitoring of employee communications:

- First, the Act does not apply if the communication is monitored with the consent of one party to the communication;
- Second, the provider of the means of communication, a telephone company or an employer who provides telecommunications equipment, may monitor communications to check service.

The consent and business necessity exceptions to the Act may be express (obtained in a signed authorization) or implied (from the distribution of the organization's email policy or employee handbook).

Finally, the Act allows the providers of email service to monitor communication made by the employee through the provided service if the monitoring is "incident to the rendition of his or her service or to the protection of the rights or property of the provider of that service." Whether or not an employer is a "service provider" can be a difficult issue to resolve. However, even if the employer is a provider, it should exercise caution to ensure that only authorized individuals are permitted to monitor the email transmissions of employees. Generally, an organization's systems administrator and a manager or investigator are the only individuals who should be permitted to access email transmissions. Similarly, to the extent the monitoring of an employee's Web usage consists of an after-the-fact tracing of the employee's Internet usage, such a practice does not appear to violate the Act, but an argument can be made that it constitutes "accessing" a communication in violation of the Act. All things taken together, the employer's best approach is to obtain explicit consent to monitoring.

Monitoring Carefully: Employees' Communications May Become Harassment

Electronic harassment poses a special problem for employers because it can be perpetrated privately, thereby reducing the likelihood of early detection. For this reason, employers are often advised to implement and disseminate policies regarding the use and monitoring of communications. Before developing and implementing such policies, it is imperative to understand the legal ramifications of such actions.

Protecting your organization and employees requires you to be able to take action when necessary. In some instances, that means ensuring you've reserved the right to act in a certain manner. Employers are recognizing the importance of being able to access employee communications quickly and without added liability. After all, being able to review employee email and voicemail communications should help you avoid liability, not open the door to claims from your employees and those with whom they communicate.

How To Manage Privacy Concerns

Whenever employee communications are at issue, you need to balance the employee's reasonable expectation of privacy against the organization's need to access information. Recent court cases have illustrated the importance of balancing these concerns.

The single best method for avoiding privacy claims is to make everyone who uses and receives company email and voicemail messages aware that there may be monitoring of the system and that privacy should not be expected. Some organizations have gone as far as setting up company email "stationery" that includes a disclaimer at the bottom of every message that reminds the employees of the limits of their privacy in the workplace. At a minimum:

- Put your organization's privacy policy in writing, making a clear statement that employees should not expect their computer usage to be private. Make it clear to employees that they should not expect any privacy in the email or telephone system, and that their use is subject to monitoring. However, an employer should have a legitimate business reason for monitoring—it is unwise to engage in excessive or unwarranted monitoring of employee activity. To this end, state in the policy the reason why the monitoring is taking place. If the company must monitor in order to comply with Texas regulations, simply say so in the policy. This will help foster employee understanding of and compliance with the monitoring;
- Include a clear statement in the policy that computer and Internet access are provided to employees to facilitate the performance of official work duties;
- Be specific about what is and is not allowed. The policy should state that all technology and equipment is property of the company and intended for business use only. The policy also should make clear that inappropriate communications, such as sexist, racist, or obscene material, will not be tolerated. Consider including a statement of how confidential information should be handled by employees, if appropriate to the company;
- Include in the policy a simple explanation that monitoring may occur without prior notice;
- Widely distribute the policy and obtain a signed acknowledgment from employees;
- Provide at least basic training to all employees on how to properly use email and voicemail systems. Explain basic facts about email and the Internet. Too often, employees are not aware that deleted email can be easily "undeleted" and read, and that user passwords do not exclude the employer from the employee's data. This basic knowledge can help to prevent many problems;
- Limit surveillance efforts to those instances supported by specific facts. For example, if an employer is concerned about an employee spending an excessive amount of time on the Internet, the employer can obtain sufficient information for disciplinary purposes by monitoring the employee's use and need not investigate every website visited. On the other hand, if the employer is concerned about an employee visiting pornographic websites and the implication raised because other employees can see the computer images, monitoring the websites visited by the employee becomes more relevant;
- Conduct random checks so that employees realize the employer is serious about enforcing the policy. Conduct these tests often enough that employees are on notice of the company's monitoring of email. If a violation is found, enforce the policy uniformly and consistently.

If an employer drafts its own privacy policy, it may wish to consider having an attorney review the policy for content.

The Danger Of Random Monitoring

It is important that employers be aware that random surveillance of an employee's use of

electronic media, that is unsupported by a reasonable suspicion, may face the same challenges as those that have been mounted against random drug testing. Of course, employers must be mindful that their monitoring practices are legal and do not contravene federal wiretapping or similar laws.

Discoverability Of Communications

Remember, also, that your organization should not expect its electronic communications to be confidential in the event of an inquiry or legal dispute. Messages that have been deleted from individual inboxes can often be retrieved from backup files. In the event of a lawsuit, attempting to block another party from obtaining access to your email and voicemail records is likely to be unavailing.

SURVEILLANCE OR SEARCH OF WORK AREAS • Many employees believe that employers cannot conduct searches of desks, lockers, and similar company property. When such searches are conducted, and the employee is terminated as a result, the employee often brings an invasion of privacy claim against the employer. These claims usually are unsuccessful, but one older case shows how an employer can be found liable for invasion of privacy.

In *K-Mart Corp. v. Trotti*, 677 S.W.2d 632 (Tex.App. 1984), *writ ref'd n.r.e.* 686 S.W. 2d 593 (Tex. 1985), the court considered the privacy interest of an employee in a locker provided by the employer to store personal effects during work hours. The court began its analysis by recognizing that the locker was the employer's property and, when unlocked, was subject to legitimate, reasonable searches by the employer. The court further reasoned:

"This would also be true where the employee used a lock provided by [the employer], because in retaining the lock's combination or master key, it could be inferred that [the employer] manifested an interest both in maintaining control over the locker and in conducting legitimate, reasonable searches."

Id. at 637. But the court concluded that when, as in *Trotti*, an employee buys and uses his own lock on the locker, with the employer's knowledge, a jury is justified in concluding that the "employee manifested, and the employer recognized, an expectation that the locker and its contents would be free from intrusion and interference." *Id.* The court affirmed a punitive damage award of $100,000 against K-Mart.

Consent Defense

Consent is an absolute defense to the tort of invasion of privacy. Accordingly, to protect against such claims, employers should take the following steps:

- Obtain an acknowledgment from employees recognizing that all offices, lockers, furnishings, computers, hard drives, and office equipment are the property of the company and are intended to be used for company business. The acknowledgment should further state that there should be no expectation of privacy anywhere within the confines of the company's premises (irrespective of whether the locker or furniture assigned to any employee is under lock and key);
- Do not permit employees to place locks on desks, lockers, and so on, or place passwords on computers.

PROTECTING TRADE SECRETS DURING THE EMPLOYMENT RELATIONSHIP • The best way to protect your trade secrets and confidential information is to make sure that the information remains secret and confidential:

- Have employees sign employment contracts that include an agreement to protect the employer's trade secrets;

- Require employees to participate in a confidential information education program. If the employee does not know that the employer desires secrecy, the employee may not be held to have a confidential relationship with the employer, and the information may not be protected;
- Have the employee assign to the employer any inventions and ideas, including trade secrets or confidential information, which were created by the employee in the course of employment. Otherwise, the employee may claim an interest in the trade secret or confidential information;
- Compose and circulate trade secret and confidential information policies and procedures manuals to employees, and require employees to certify that they have read and that they understand the company's trade secret policies and procedures;
- Periodically remind the employees of the policies and procedures in place to protect the company's trade secrets;
- Limit access to trade secrets to only those employees who "need to know" the trade secrets, and maintain detailed records of who has access to the trade secrets and when they have access to such information;
- Physically lock the areas in the company where trade secrets reside;
- Have systems in place to retain control over documents that contain trade secret information;
- Keep document control logs to protect sensitive documents;
- When there are multiple copies of a document that contains trade secrets, number the copies and prohibit any further copying of the document.

WEBSITE PRIVACY POLICIES • Many companies include privacy policies on their websites. Generally, a privacy policy is not a required part of a website. However, each website needs to be reviewed to understand what types of information are being collected and then whether the website owner has any responsibility with respect to that information.

Policies For Collection Of Personal Information

In the case of an e-commerce website, a stated website policy would probably be needed if the site will collect personal information (names, addresses, SSN, password) or financial information (usually credit cards). In these cases a privacy policy is needed because the website owner is soliciting and accepting personal or financial information. In other websites, the website functionality dealing with information from a web visitor is nothing more than the use of cookies or the invitation to contact using email, which is no more private than someone making a telephone call to the website owner. In these cases, a website owner does not solicit personal or financial information, and a detailed privacy statement may not be needed.

A second consideration is the effect of the information provided by a website visitor. In some cases, it may be wise for the website owner to make it clear that there is no obligation of confidentiality with respect to information being submitted by a website visitor. For example, if a website visitor gave information on a sales lead, or a lead for an office lease, or an idea for a new product, the website owner would not want to be the subject of a claim that the visitor is entitled to a sales commission, a brokerage commission, or a license fee. However, if the information gathered through a website is in fact used by the website owner (sold to a list broker, compiled as click stream data, and the like) then the privacy policy should address these issues.

TERMINATION OF EMPLOYMENT • By its nature, termination of an employee tends to be a quick and sometimes emotional process. An employer, however, should be careful to slow down and take the time to end the employment relationship in a carefully thought out manner so as to protect the employer's intellectual capital. Here are some suggestions:

- Conduct an exit interview wherein all confidential materials are returned to the employer, and the employee acknowledges such return in writing;
- In the exit interview, discuss all restrictive covenants and importance of keeping trade secrets confidential. Provide copies of any agreements and be prepared to answer questions;
- Collect keys, laptops, calling cards, manuals, and all other items issued to the employee;
- Remove the employee from voice mail, email, and the company intranet;
- Ask about future employment to check on potential conflicts;
- Ask the employee to inform his or her new employer of existing confidentiality agreements or covenants not to compete;
- Contact the employee's new employer to give notice of the employee's restrictive covenants;
- After the employee leaves, review the departing employee's previous position, new position, and any restrictive covenants so as to evaluate the risk of losing intellectual assets;
- Make sure the departing employee feels he or she was treated fairly;
- Utilize consistent document control policies that consider which documents to retain and which documents to destroy;
- Clearly identify the company's trade secrets—stamp trade secret documents "confidential" or "trade secret";
- Visibly label areas of the workplace which contain trade secrets with signs or labels indicating the same;
- Institute security measures to protect trade secrets;
- Implement restrictive security codes and passwords;
- Limit remote access to information stored in computer files;
- Consider installing auto-callback functions;
- Maintain firewalls between the computer system and the Internet;
- Require third parties to execute confidentiality agreements before they receive confidential information.

CONCLUSION • The modern workplace, infused with litigation and new rights, presents a number of challenges to the employer. Ideally, the privacy rights of all individuals would be completely respected. Unfortunately, the risk of liability from what an employer doesn't know is so great that employers are almost required to make some intrusion into their employees' lives, and employees, in turn, must accept their employer's oversight. Nevertheless, given clearly defined guidelines about when such intrusion will occur, and given due respect for the rights of the employees, an employer may safely toe the line between knowing too much and not knowing enough.

PRACTICE CHECKLIST

The Privacy Rights Of Employers And Employees (Part 2)

Can an employer lawfully "spy" on its employees? Whenever employee communications are at issue, you need to balance the employee's reasonable expectation of privacy against the organization's need to access information.

• The Federal Wiretapping Act, as amended by the Electronic Communications Privacy Act of 1986 (the "Act"), 18 U.S.C. §§2510-2521, generally prohibits the interception, disclosure, and intentional use of wire, oral, and electronic communications. However, there are two exceptions for employers that clearly apply to employer monitoring of employee communications:

__ First, the Act does not apply if the communication is monitored with the consent of one party to the communication;

__ Second, the provider of the means of communication, a telephone company or an employer who provides telecommunications equipment, may monitor communications to check service.

• The consent and business necessity exceptions to the Act may be express (obtained in a signed authorization) or implied (from the distribution of the organization's email policy or employee handbook). So the employer should implement and disseminate policies regarding the use and monitoring of communications:

__ The privacy policy should be in writing and state clearly that employees should not expect their computer, email, or telephone system usage to be private and that their use is subject to monitoring;

__ Include a clear statement in the policy that computer and Internet access are provided to employees to facilitate the performance of official work duties;

__ Be specific about what is and is not allowed. The policy also should make clear that inappropriate communications, such as sexist, racist, or obscene material, will not be tolerated;

__ State that monitoring may occur without prior notice;

__ Widely distribute the policy and obtain a signed acknowledgment from employees;

__ Provide at least basic training to all employees on how to properly use email and voicemail systems. Explain basic facts about email and the Internet;

__ Limit surveillance efforts to those instances supported by specific facts;

__ Conduct random checks so that employees realize the employer is serious about enforcing the policy. Conduct these tests often enough that employees are on notice of the company's monitoring of email. If a violation is found, enforce the policy uniformly and consistently.

• Likewise, any employer efforts with respect to worksite surveillance should be part of an overall policy and supported by employee consent.