CORNELL HR REVIEW

THE BENEFIT OF ADOPTING COMPREHENSIVE STANDARDS OF MONITORING EMPLOYEE TECHNOLOGY USE IN THE WORKPLACE

Karin Mika

With the explosion of technology has come the opportunity for nearly all aspects of everyone's life to be monitored. A phone GPS can detect a person's whereabouts at any time; keystroke monitors can record anything a person types on a keyboard; cameras can, and do, monitor movements in schools, stores, parking lots, homes, and many other places; software can capture real-time chats, email can be accessed by the provider of the service, and internet access points can be pinpointed, even if a person is not using his/her own computer. None of these technologies even consider the voluntary nature of disclosed personal activities – Facebook, internet blogs, listserv discussions, twitter posts, and even forwarded emails. For all intents and purposes our lives are open books, even if we take great strides to limit our disclosures.

One area where this becomes especially problematic is in the workplace. Although most people would agree that employers have many rights when it comes to scrutinizing arguably "personal" activities (for instance, sending threatening or harassing communications to co-workers, using work time to engage in personal social networking, or disclosing company secrets), many employees have run into situations where employers have arguably crossed the line when disciplining or discharging an employee for personal activities that seem unrelated to what an employer should be able to scrutinize. These activities include those that occur outside of working time, such as posting comments on a personal (or even anonymous public) blog, or posting pictures and/or comments on a quasi-private Facebook page. The activities may also include those that occur during working time, such as forwarding a seemingly innocuous email, or making a personal comment in an email when there is no general prohibition on this activity.

In most instances neither the employer nor the employee is truly certain of what his/her rights or obligations are. However, in most cases, it is usually the employee who suffers the consequences when the employer decides that an activity discovered through electronic monitoring is something that should be subject to discipline or discharge.

This article will examine issues as they relate to the privacy of employees' lives given that nearly everything can be discovered by some form of electronic monitoring. It will posit that most laws as they exist today do little to apprise either the employer or the employee as to what type of electronic monitoring of personal communications is

acceptable. It will further propose that most employer policies related to scrutinizing employee electronic communications are vague and unsuitable. The article will conclude that, given the leeway employers tend to be given (often justifiably so) in monitoring employees there is little chance that we will soon see any standardization of laws regarding what can be done with electronically obtained information. Because of this, the author asserts that, given the vague state of the law, employers need to devise effective monitoring policies in order to strike a balance between their interests and the privacy interests of their employees.

EXACTLY WHAT CAN AN EMPLOYER MONITOR AND WHAT CAN BE DONE WITH IT?

What is allowed to be monitored and what can be done with the monitoring seems to be the main question both employers and employees ask. The answer seems to be that an employer can monitor virtually everything and almost anything can be done with it. Limitations are few and far between, especially if the employer has a posted a policy regarding the types of monitoring that go on. Additionally, employees are rarely successful when they decide to challenge the legality of the discipline or termination they received as a result from employer monitoring. Overall, courts have displayed a willingness to uphold disciplines and discharges as long as the action resulted from the discovery of an activity that had some relationship to work duties.

In terms of employee monitoring, there are often not too many surprises as far as whether an employee can expect discipline and discharge for a particular offense. Most situations are just a matter of common sense and have nothing to do with whether the information was discovered by electronic means or not. For instance, if a camera would capture an employee selling drugs on company property, that employee should expect to be discharged. If an employee works for a company where the employee's job is to communicate with customers online, that employee should reasonably expect to be disciplined if monitoring discovers that the employee was surfing the internet rather than dealing with customers. Additionally, an employee who sends threatening or sexually harassing emails through the company computer system should also expect to be disciplined.

In each of these cases, most reasonable people would agree that the employer was well within their rights to both monitor these activities things electronically and carry out discipline should the monitoring disclose inappropriate work conduct. Issues arise, however, in a few major instances:

1. When the action of the employee does not occur during working hours (such as maintaining a personal blog or sending email while at home).
2. When the employer does not have a policy that prohibits using company equipment for personal use (such as when an employer allows an email account to be used to send and receive personal communications).
3. When the employer acquires the information through indirect means (such as when an email is forwarded or a co-worker "captures" otherwise private information and brings it to the attention of the employer).

4. When the employer acquires information (in a way which was not at all related to their job duties) that was originally private, happened at some point in the past, but somehow still can be gleaned through an internet search engine (such as when an employer is still able to discover a lewd photo from an employee's college days).

Most employees would not think their jobs could be at stake on the basis of having done something regrettable during a college spring break trip, or by griping to a friend on Facebook about a bad day at work; however, that is exactly what can occur.

THE LAWS AS THEY NOW STAND

While technological devices like cell phones and computers made their way into the workplace years ago, the law is far from settled with regard to *how* and *how much* employers can monitor their employees' use of technology. This is largely due to the fact that the laws regarding the "interception" and use of electronic "communications" remains a hodgepodge of federal and state rules. Some were enacted at a time when the internet did not even exist, while others were enacted without foresight as to how they might be employed in the workplace. The application of these laws to discharge situations made for the proverbial "attempting to put a square peg in a round hole." While lawmakers may have envisioned situations where employers would monitor employees only to discover illegal behavior—such as whether secrets were being disclosed, or if employees were meeting productivity goals—the monitoring of employees has extended far beyond these reasons, and also extends to monitoring beyond the regular workday.

While the law remains unsettled as to how much an employer can legally monitor, there are certain federal statutes that are integral to the discussion of whether employees retain any protection over their privacy interests. The primary federal statutes that cover acquiring electronic information are part of what was originally called the Omnibus Crime Control and Safe Streets Act. This Act, often called the Wiretap Act, was focused on preventing the government from recording and listening to the conversations of private citizens. The Act made the Fourth Amendment warrant requirement more stringent when law officers sought to "eavesdrop" on certain conversations. The Wiretap Act was enacted in 1968. A second component of the Wiretap Act is the 1986 amendment introduced as the Electronic Communications Privacy Act. This amendment focused on making it illegal for private citizens (including employers) to listen to and record conversations. Both of these laws were enacted at a time when the internet did not exist and when telephones and tape recorders were regarded as state-of-the-art technology.

According to the collective components of the Wiretap Act, it is unlawful for an individual to "intercept or endeavor to intercept, any wire, oral, or electronic communication." A few exceptions were made for providers of the service, employers, and when there was consent for the interception. The interpretation of just what is an interception has been one of the many ambiguities that made it difficult to apply this statute to electronic communications that are "acquired" by an employer. Originally, an interception was defined as requiring that the interception be while a communication was

in transit prior to its arriving at its destination (such as listening in on a phone conversation). This definition became a hurdle for courts when dealing with the advent of email communications and voicemail.

Also at issue, at least in terms of the employer and employee relationship, was whether an interception, if it occurred in a legal sense, fell within one of the statutory exceptions. The two primary exceptions to the statute are related to whether the interception occurs within the ordinary course of business, and whether the employee has consented to the monitoring. As previously indicated, one of the major issues related to consent was whether the monitoring went beyond the scope of consent given by the employee.

The Stored Electronic Communications Act, which is part of Title II of the ECPA prohibits the unauthorized "retrieval" of electronic communications and was enacted to close some of the loopholes related to email and other types of stored electronic communication. With respect to employers, courts have interpreted the statute to mean that similar exceptions that apply to intercepted communications apply to stored communications. Thus, if a retrieval is done in the ordinary course of business, many courts have found that the statute has not been violated. Moreover, if an employee consents to the monitoring of retrieved information, courts have also found that there has been no violation of the statute. Both of these interpretations are often predicated on what has been obtained by the employer and what was the scope of consent; however, most courts have interpreted the provisions of the ECPA broadly in favor of employers.

EMPLOYER INTERESTS V. EMPLOYEE PRIVACY

While the Electronic Communications Privacy Act and the Stored Communications Act have guided courts in dealing with workplace privacy issues, there is still no clear answer to the question of what employers are legally allowed to do with electronically obtained information. However, as previously indicated, there are a great many "retrievals" and "interceptions" that one should not expect an employee to object to. If working for a package delivery company, an employee might expect an employer to object if GPS monitoring demonstrated that the employee made numerous personal detours during the work day. If working for a company that issued a cellphone, an employee might expect an employer to object if scrutinizing cellphone usage revealed that the employee was making personal calls that were charged to the company. If working for a company that was a customer service firm, an employee might expect an employer to object if screen captures demonstrated that the employee was doing other things on the internet instead of dealing with customers. Quite often, employees will acknowledge an employer's right to do such monitoring when accepting an offer of employment.

But in terms of what might be monitored on the job, employers have other concerns that go beyond productivity and profitability. Employers are obligated to provide a safe and non-threatening environment for employees and often have policies regarding safety, and proscribing threatening behavior (both sexually threatening/harassing and physically threatening). Employers can easily be held liable if inappropriate behavior occurs in the workplace and the employer "should have known about it." Moreover, employers can be held liable for harm employees might cause to

members of the general public if there was a means to discover that the employee was inappropriately dealing with members of the public.

Few people would disagree that it is both the right and responsibility of an employer to have the means to prevent sexual harassment, threats of violence, disclosure of company secrets, or committing crimes on the job. However, few people agree as to what the boundaries of the employer should be in terms of how to accomplish this goal.

It is rare that any straightforward prerogative of a responsible employer becomes subject to litigation (e.g., checking whether an employee has threatened another employee by using company email). What tends to be litigated, however, are situations when the employer is perceived to have overstepped its bounds. For instance, if an employer, rather than merely monitoring internet usage for efficiency purposes, uses something personal for disciplinary purposes. Or if an employer, rather than monitoring whether a phone is being used mostly for work, listens in on conversations to see who is being called and for what. Or when an employer, rather than determining whether an employee has sent emails to particular people, also reads the content of those emails.

Those become difficult matters for courts, especially if an employee has given an employer carte blanche authority to monitor internet usage, phone usage, and email. In those situations, courts tend to look at matters on a case-by-case basis and assess what was an individual's expectation of privacy, and whether an employer may have overstepped the bounds of its consent to monitor.

However, many alleged invasions of privacy in the workplace have nothing at all to do with either monitoring or retrieval. Consider the matter of the forwarded email that a co-worker regards as sexually harassing, or even the forwarded email that expresses personal sentiments that were intended to be private. Consider also a situation where browsing the internet yields a discovery of information about an employee that an employer believes reflects badly on the employer. In none of these cases would the electronic information have been retrieved from an employee's work files or equipment, nor could the information be considered intercepted. Yet an employee might still be subject to discipline or discharge depending on existing work rules (e.g., "an employee may be discharged for engaging in any activity that in any way reflects badly on the employer or is disparaging of the employer."), or even mere whim of the employer in the absence of any work rules, such as in an at-will employment situation.

And perhaps the question that many might ask is, is this fair, especially if it is not the employee who has made the information available to the employer, but rather a third party?

Certainly an employee who is complaining to a friend about a bad day at work (whether the communication happens through a company email or during an after hours Facebook chat), would neither expect the conversation to get back to her employer, nor expect to be disciplined for it, but it does happen. From an employer's perspective, if the information can be discovered by one person, it can be discovered by a multitude of people. From an employer's viewpoint, if the information disparages the reputation of the employer or puts the employer in jeopardy of liability, then the employer should be able to discipline or discharge the employee. Thus, absent clear policies about what can be used for disciplinary purposes, chances are that anything discoverable on the internet is fair game for use as a basis for discipline or discharge.

Although it would be ideal to suggest that federal and state laws should be modified to compel employers to write policies that explain what electronic information could be used and how, this is an unrealistic goal. Given that the majority of employees are at-will, it is unlikely that there would be any real motivation for employers to explain what will not be used. Rather, it might be in the best interests of the employer to keep any policies it has as broad as possible in order to cover situations that are not necessarily foreseeable.

That said, this might not be the best tactic to take when formulating work rules or even unwritten policies. It is generally agreed that employees have the right to engage in discussions about "conditions in the workplace." Criticizing management is sometimes considered to be part of discussing conditions of the workplace, and various courts as well as the National Labor Relations Board have upheld an employee's right to engage in dialogue critical of management without fear of reprisal. But there is a question as to when critical statements aimed at perhaps improving a work situation become disparaging, derogatory, or nonproductive. At what point does an employee lose his/her right to vent on, for example, a public internet forum? Also, does it matter what line of work that employee is in? Where the lines are should be more specifically spelled out in order to benefit both employers and employees.

CONCLUSION

Legislation relating to employee monitoring is a hodgepodge of statutes that do not directly apply to the technologically advanced way that communications can be made. In addition, statutes, where they exist, do not address situations related to the scrutinizing of communications that an employee might regard as personal (such as posting on a blog or on Facebook), nor when the employee communicates on his/her own personal device during non-working hours. Because many employees now work on the go on either employer-issued equipment or on personal equipment, the lines between non-working hours and working hours have become blurred as have become the lines between work and non-work related. Employees have a right to know what behaviors are considered impermissible. Moreover, it is to the benefit of employers to have clear, enforceable policies that set the guidelines for what is expected from employees.

It is this author's position that although a federal statute could provide some of the guidelines necessary for a 21st century workforce, passing an all-encompassing statute that covers various unique workplace situations will be difficult. Moreover, although various proposed statutes deal with restrictions on monitoring, they do not necessarily encompass situations where disciplines from communications are made known to an employer although not "monitored" in the traditional sense. The author believes that it would be beneficial to both employers and employees to define what communications thought to be "personal" may result in workplace discipline. Whether this begins with union negotiation or a collaboration of human resources personnel and attorneys, employers need to devise effective monitoring policies. Only then can employer interests and employee privacy begin to reach a balance. א

Karin Mika (J.D.) presents nationally on topics related to integrating technology and multimedia into classroom teaching, and has judged at numerous moot court competitions. Prof. Mika's areas of scholarly research are varied and she has published in the areas of Native American Law, Employment Law, Learning Theories, and Health Care. Recently, Professor Mika was named National Publicity Director for the William C. Burton Awards, a yearly event that honors excellence in Legal Writing.