Denver Law Review

Volume 79
Issue 4 *Symposium - Privacy*

Article 11

January 2002

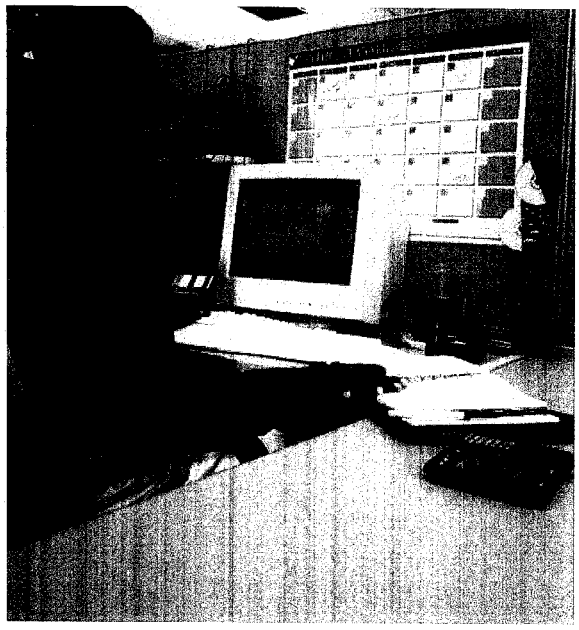
I'm Watching You

Leslie E. Nunn

Dane Patridge

Brian McGuire

I'm Watching You



I'M WATCHING YOU

BY LESLIE E. NUNN, J.D., DANE PATRIDGE, PH.D., & BRIAN MCGUIRE, PH.D.

Over the last several years, an issue has emerged that has challenged employers: whether and how to monitor employee electronic communications, in particular, employee use of e-mail and the Internet. Employers have undertaken such monitoring in an effort to reduce the amount of productivity lost to non-work related activities and to guard against employees accessing inappropriate websites or sending inappropriate e-mails.[1] Employer concern with potential sexual or racial harassment has also motivated many to take action.[2] Major employers, such as The New York Times, Dow Chemical, and Xerox, have recently terminated employees for inappropriate e-mail and Internet use.[3] In addition, the American Management Association reports that over eighty percent of surveyed companies engage in electronic monitoring and/or surveillance of their employees.[4] These employers monitor employee use of the Internet, e-mail, and computer files, as well as video recording employee performance and reviewing employee telephone conversations and voice mail messages.[5] Furthermore, nearly ten percent of companies in the United States have been subpoenaed for employee e-mail in pending cases.[6] There have also been cases where employers have obtained court orders allowing them to search the home computer hard drives of employees.[7]

One consequence of the actions that employers have taken in this area is concern regarding the rights of employees.[8] To what extent, if any, are there limits on the employer's right to monitor employee use of e-mail and the Internet? Most companies have policies concerning e-mail and Internet use, a somewhat smaller percentage provide notification to employees of the monitoring, and relatively few provide training regarding such policies.[9]

In an ironic twist, the United States Court of Appeals for the Ninth Circuit ordered staff members to disable the

software that had been monitoring the e-mail and Internet use of the judges.[10] The United States Judicial Conference's Committee on Automation and Technology, however, was of the opinion that "federal employees - including judges - should continue to be monitored for Internet misuse and should be blocked from such activities as downloading music."[11]

This paper will address the monitoring of employee electronic communication. The following sections will examine the law concerning searches, the issue of employee notice, and recommend policies in this area that would be prudent for employers to adopt.

BACKGROUND: SEARCHES AND THE FOURTH AMENDMENT

Fourth Amendment

The first ten amendments to the Constitution of the United States are referred to as the "Bill of Rights" and are generally understood to codify the most basic of rights that we enjoy as citizens and residents of this country.[12] The right to be free of unreasonable searches is one of the most carefully guarded rights, and is treated in the Fourth Amendment to the Constitution.[13] The Fourth Amendment reads as follows:

The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[14]

What is a "Search"?

The Supreme Court has construed the constitutional protection against unreasonable searches and seizures embodied in the Fourth Amendment "as proscribing only governmental action; it is wholly inapplicable 'to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the government or with the participation or knowledge of any governmental official.'"[15] Within the meaning of the Fourth Amendment, "a 'search' occurs when an expectation of privacy that society is prepared to consider reasonable is infringed."[16] In determining whether a claimed expectation of privacy is proper, the courts apply a two-part test.[17] First, did the individual demonstrate by his conduct that he had an "actual (subjective) expectation of privacy?"[18] Secondly, if so, was that subjective expectation something that society at large would "recognize as reasonable?"[19]

However, this is not to say that the individual's subjective expectation of privacy is dispositive of the issue.[20] The totality of the circumstances must be considered to determine whether an individual has a legitimate expectation of privacy.[21] For example, what can be observed or heard, without the aid of technical enhancement, when the observer is legally present in a place where he has a right to be is not considered an illegal search.[22]

Searches can be performed visually[23] or by more advanced technology, such as through the use of electronic listening devices[24] or thermal imaging devices.[25] It is not the same as a seizure.[26] The term "seizure" describes the actual taking of an item or items found during a search.[27]

Plain View

The law is well settled in that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[28] "The rationale of the plain-view doctrine is that if contraband is left in open view and is observed by a police officer from a lawful vantage point, there has been no invasion of a legitimate expectation of privacy and thus no 'search' within the meaning of the Fourth Amendment . . . ."[29]

Administrative/Regulatory Inspections

As with searches that occur in the criminal context, Fourth Amendment protections also apply "with respect to administrative inspections designed to enforce regulatory schemes."[30] "In closely regulated industries, however, an exception to the warrant requirement has been carved out for searches of premises pursuant to an administrative inspection scheme."[31] For an

administrative or regulatory inspection to be conducted constitutionally without a warrant, three criteria must be met: (1) "there must be a substantial government interest in the regulatory scheme under which the inspection is conducted;"[32] (2) "the warrantless search must be necessary to further the regulatory scheme;"[33] and (3) "in terms of certainty and regularity of its application, the inspection must provide a constitutionally adequate substitute for a warrant."[34] These three requirements combined present a formidable chasm to cross. These requirements for warrantless inspections are normally met only in a few industries; i.e., the liquor,[35] gambling,[36] tavern,[37] meatpacking,[38] wastewater treatment,[39] auto-body repair,[40] and toxin-producing industries.[41]

Search Warrant

The police must have a search warrant before they conduct a search, except in rare and specific situations.[42] As the Fourth Amendment specifically states, a search warrant should be issued only upon a finding of "probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[43] The property to be searched must be described in writing and in specific detail.[44] Likewise, the items being looked for must be described in specific detail in the search warrant.[45]

Exceptions to Warrant Requirement

Normally, searches without a warrant are presumed to be unreasonable.[46] Among the situations where a warrant is not necessary, other than for administrative or regulatory searches of closely regulated industries, are situations where time is clearly of the essence.[47] A warrant is also not necessary when: (a) the person to be searched gives free and voluntary consent to be searched;[48] (b) entry of the subject property is necessary to save a person's life;[49] (c) a search is necessary to prevent the immediate loss or destruction of evidence of a crime;[50] (d) the items are in plain view, as described above;[51] (e) a search is necessary to protect the safety of the law enforcement officer, such as looking for weapons in the driver's area of a car that is stopped because of a traffic violation;[52] and (f) a search occurs incident to arrest.[53]

SEARCHES CONDUCTED BY AN EMPLOYER

Private employers are normally not subject to the same restrictions as law enforcement officers because the Fourth Amendment applies to governmental actors and not private individuals.[54] In a purely commercial setting an employer has a business and monetary interest in what her employees are doing while on the job and while on the business premises. Under general employment law, every employee owes a duty of loyalty to his employer.[55] This duty gives the employer a vital, as well as legal, interest in what is going on in and about her premises.[56] Since the employer is not a criminal investigator, she is given wider latitude in conducting searches of her own business areas.[57]

Employer as an Agent of the Police

When the police conduct a criminal investigation, they cannot coerce or too strongly encourage an employer to search her employee's work place without a search warrant.[58] If the employer does so, she is acting as an agent of the police and the constitutional restrictions are the same as if the police themselves conducted the search.[59] A search warrant is required unless the search fits one of the above referenced exceptions.[60]

A two-part test is used to determine if the employer's actions are subject to constitutional strictures. The first inquiry is whether the law enforcement agency initiated, "'knew of[,]' or 'acquiesced in' the intrusive conduct."[61] The second inquiry is whether the employer who performed the search intended to assist law enforcement efforts, or was merely trying to further her own ends.[62]

That is not the case, however, when the employer conducts a private search of the employee's work area, on her own, and without any contact with the police.[63] In that case, whatever the employer finds is usually held to be admissible in a criminal prosecution of the employee.[64]

Invasion of Privacy

When an employer suspects an employee of misconduct, the employer usually simply fires the employee.[65] If, however, the employer is not trying to assist law enforcement and has as her main purpose the furtherance of her own business ends, the employer is usually permitted to conduct her own search of the employee's work area located on the employer's property.[66] However, this general rule has limitations, one of which is the common law tort of invasion of privacy.[67]

The tort of invasion of privacy has come to symbolize several different causes of action.[68] However, for purposes of this article, we will concentrate on the cause of action entitled "intrusion upon seclusion, which focuses on the manner in which information that a person has kept private has been obtained."[69]

...is usually held to be admissible in a criminal prosecution of the employee.

continued on page 576

continued from page 552
Just as the Fourth Amendment protects peoples' reasonable expectations of privacy from governmental intrusion, so to does this common law tort protect the private individual from the prying eyes, ears, and senses of others, both public and private.

In order to "prevail on a claim of intrusion of seclusion as a violation of one's privacy, a plaintiff must show that another has intentionally intruded, physically or otherwise, upon the plaintiff's seclusion or solitude, and that such intrusion would be considered offensive by a reasonable person."[70] In the employer/employee context, the protection afforded an employee from intrusion by his employer is determined by balancing the employee's reasonable expectation of privacy in the area against the reasonableness of that expectation.[71]

Searching a Terminated Employee's Work Area

When an employee's working relationship with the employer is terminated, either voluntarily or involuntarily, the employer has a major business interest at stake. Is the employee wrongfully taking some of the employer's property with them as they leave (such as customer and supplier lists, equipment, trade secrets, supplies, etc.)? This is particularly alarming to the company owner when the employee's parting has been a less than happy scene. Therefore, the employer's interest in what is in the terminated employee's workspace is a legitimate one.[72]

Other People Having Access to the Employee's Office

When others have access to the office of the employee being searched, it would be difficult for that employee to restrict access by other people to his work area. If the employee cannot keep others out of his area, he cannot reasonably expect to have privacy in his work area.[73] This issue was, perhaps, carried to extended lengths when, in 1992, a Florida federal court in *Pottinger v. City of Miami*,[74] held that a homeless person had a subjective expectation of privacy regarding their property, including their bedroll and other personal belongings, when they slept in public areas.[75] However, the court did deny that there was an expectation of privacy to sleep and eat in public, and, therefore, the city may arrest them for these activities without violating their privacy rights.[76] Accordingly, others having access to an area greatly diminishes the ability of anyone working in that area to claim a valid privacy interest.[77] If there is no reasonable expectation of privacy, then without any other prohibition, the search can validly take place.[78]

Shared Offices With Other Workers

New Jersey considered the issue of workers sharing a common work space and found that, from an objective viewpoint, a worker sharing locked work space cannot reasonably have an expectation of privacy where other workmen have access to the same work space.[79]

This view is shared by most state and federal courts, which have addressed the issue in the Fourth Amendment context.[80] In fact, the United States Supreme Court says that, "what a person knowingly exposes to the public" is not subject to constitutional protection.[81] Again, as stated above, what can be perceived with ones own unaided senses, when lawfully in a place where they have a right to be present, is not an illegal search.[82]

In the employer/employee context, if an employee is insensitive to his surroundings and who might be present to observe or overhear, that employee should not be able to later claim that it was improper for someone to see or overhear what he did or said. Accordingly, even if the employee had a subjective expectation of privacy in his office space, the employee's expectation would not be reasonably grounded.

Locked Desk or Computer

If an employee has the only key to his desk and keeps it locked, that situation is essentially the same as where the employee has the only password to the company provided computer, which he uses. Again, we must look to the circumstances of the work environment. In *United States v. Speights*,[83] the court reviewed a case involving a police officer that kept an illegal sawed-off shotgun in his personally assigned locked locker in the police station dressing room.[84] In this case, the court noted that the police department did not have any regulation or notice that the police lockers were subject to unannounced searches at any time.[85] While the lockers were infrequently checked for cleanliness, these checks had occurred only three or four times in the preceding twelve years.[86] The police officers were permitted to keep personal items in their lockers and were allowed to use their own personal padlock to secure the contents of their assigned locker.[87] There was no requirement that an extra key to that padlock be given to the police chief or any other supervisor.[88] Under these specific circumstances, the court held that the officer did have a reasonable expectation of privacy and the warrantless search was violative of his constitutional rights.[89]

The same logic incorporated by the court in *Speights* would apply in a non-governmental situation. For example, in *K-Mart Corp. Store No. 7441 v. Trotti*,[90] the court stated that where "the employee purchases and uses his own lock on the lockers, with the employer's knowledge, the [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."[91]

On the other hand, a warrantless search of a deputy sheriff's locker was upheld where the locks given the deputies had both keys and combinations, but the commander kept a master key and the combinations to all locks.[92] While the deputies could change the keys and combinations at will, copies of the new keys and new combinations had to be given to the commander.[93]

Would the approach adopted in the

above-cited cases also apply to a computer? If the employee is permitted to have his own password, and that password is not required to be given to his supervisor, then the employee could reasonably expect privacy as to what he kept on the company owned computer that he was using (assuming this employee is the only person assigned to use that computer).

Sending the Computer Out for Repair

What protection would an employee have when he sends out his company-owned computer to be repaired? What if management temporarily took the computer to install new software or modify the configuration? What expectation of privacy would the employee have at that time?

The Supreme Court of Kentucky, in *Deemer v. Commonwealth*,[94] addressed an analogous situation. Film was taken to a commercial developer to be processed.[95] As the processing company developed the film, the photos clearly depicted a crime taking place.[96] Police were notified and the culprit was prosecuted.[97] The defendant filed a motion to suppress the photos because he had been taking film to that location for five years and never experienced interference before.[98] Apparently, he argued that the processing company acted as his agent in the developing process.[99] The court, noting that the defendant lost any expectation of privacy when he delivered the film for processing, rejected this argument.[100] The rolls of film here were delivered to a commercial entity whose responsibility was to visually examine the prints in the development process.[101] The defendant, the court stated, knew or should have known this.[102]

In like circumstances, an employee could not reasonably complain that a computer technician observed improper materials on his company-owned computer when the technician was updating, reconfiguring, or otherwise working on the computer. While it might be said that in *Deemer*, the employee initiated the action that led to the viewing of the photos,[103] this would not be true when a company technician comes to the employee's computer (if the work was done at the behest of the employer and not the employee). Nevertheless, the employee should reasonably anticipate that the employer could, at any time, install improvements to the company-owned computer.

Employers Following the Electronic Trail

Unlike many other forms of communication, it is difficult, if not impossible, to totally erase from a computer hard drive the communications sent out from that computer.[104] Recently, software has been developed which enables an employer to see what has been done on a computer in the past.[105] Software, like *Investigator*, is now commercially available to read a hard drive, thereby telling of the nefarious deeds done by the employee.[106] The computer itself incriminates the worker.[107]

That an employer may, from time-to-time, conduct a random search of an employee's possessions on the job, could arguably give the employer the right to review e-mails from one employee to another or otherwise see what an employee has done on the company-owned computer in the ordinary course of business.[108] For instance, if an employee is not at work due to illness, it may be necessary for the employer to review what messages were sent by that employee (to ensure the continuity of workflow until the worker is able to return to the job). While federal law might not prohibit this action, some state laws may nevertheless still consider this as offensive and illegal.[109] Part of the issue may be the manner in which the employer views employee's thoughts and actions. Viewing what went out electronically in e-mail or hearing voice-mail messages left for the employee can sometimes be treated differently than monitoring a telephonic (or actual) conversation between workers.

For example, Wal-Mart Stores learned this in *Desilets v. Wal-Mart Stores, Inc.*,[110] when the company was held liable for eavesdropping on employees in violation of the Omnibus Crime Control and Safe Streets Act of 1968.[111] Title III of this act prohibits interception, disclosure, and intentional use of private conversations,[112] and Wal-Mart recorded conversations between its workers.[113]

EMPLOYEE MALFEASANCES AND EMPLOYER RESPONSES

Harassment, Discrimination, and other "No-No's"

Employees' use of the Internet or company intranet to send harassing, sexually suggestive, or racially motivated messages can be very costly for a company that does not prevent or stop it.[114] For example, Chevron paid out $2.2 million dollars to settle claims for failing to prevent the circulation of an e-mail message describing 25 reasons why beer is better than women.[115] Accordingly, companies have a duty to stop and also prevent improper messaging because failing to do so can result in hefty penalties for the company.[116]

Employers Terminating Employees

Recently, there have been a number of employers disciplining and terminating employees for improper use of the Internet.[117] For example, the New York Times fired over twenty employees and Xerox Corporation fired forty for unauthorized use of the Internet.[118] These employees were terminated for sending offensive e-mail messages and/or viewing Internet pornographic materials at work.[119]

Lawsuits by Employees

Where employees have brought lawsuits against their employers or former employers, the legal foundations have been based on the following theories: the tort of invasion of privacy, discrimination statutes, Fourth Amendment protections regarding search and seizure, First Amendment guarantee

The damage to the company is obvious.

Necessary work is not getting done, yet the employee is still being compensated.

of freedom of speech, Electronic Communications Privacy Act of 1986, Omnibus Crime Control and Safe Streets Act of 1968, and familiar torts such as defamation, negligence, and intentional infliction of emotional distress.[120] The success that these employees meet in the judicial system is varied. Perhaps most importantly, the policy of the employer (in effect at the time of the communication) prohibiting such conduct was a major factor on the outcome of the cases.[121] Other important factors are circumstances of the communication, the intent and attempt of the employee to keep the communication privileged and away from the employer's knowledge, and the means used for the communication itself (telephone or email).

Theft of Time

A safer course of action for the company to take when discharging employees for unauthorized use of the internet, telephone, and other communications means is to discharge the employee for not working during the time she was improperly using the Internet, telephone, or other communication.

The damage to the company is obvious. Necessary work is not getting done, yet the employee is still being compensated. Furthermore, useless e-mails sent to a large number of employees can overtax the company servers, thereby causing a meltdown of the internal communications system.[122] The company may have to pay overtime in order for the employee to accomplish what he should have been doing during regular work hours. The list could go on, but these grounds would be considered sufficient for a court to uphold a firing of an employee for improper usage of the Internet or intranet.

Employers' Policies

One hurdle that a company must overcome to have its "monitoring of employee's conduct" held proper is the various federal and state statutes requiring a person's consent before his conversations can be monitored or recorded.[123] The employer should give advance notice to all employees that conversations, e-mails, and use of the Internet will be monitored. In order to better protect itself, the company should have each employee sign a consent form allowing the company to monitor the employee's use of the Internet, telephone, and other company assets. "Notification and consent negate an expectation of privacy and usually protects companies from liability under such federal statutes as Title III of the Omnibus Crime Control and Safe Streets Act of 1968 and the Federal Electronic Communications Privacy Act of 1986, governing interstate communications, as well as common law invasion of privacy charges."[124]

Union Organizing Activities

One exception to the right of an employer to prohibit employees' use of the Internet for other than company purposes is the right of a union to use the company's Internet.[125] Federal labor laws (National Labor Relations Act, and others) protect the union and its members' right to use certain company facilities to discuss matters considered within the union's purview.[126]

CONCLUSION

As held by the United States Supreme Court in *O'Conner v. Ortega*,[127] "employees' expectations of privacy in their offices, desks, and file cabinets... may be reduced by virtue of actual office practices and procedures, or by legitimate regulation."[128] The Court went on to state that, "offices may be so open to fellow employees or the public that no expectation of privacy is reasonable. Given the great variety of work environments . . . the question whether an employee has a reasonable expectation of privacy must be addressed on a case-by-case basis."[129]

While it is hoped that employers will always make the correct decisions regarding the monitoring of employees, the complexity of laws related to protecting the privacy of individuals often causes confusion on behalf of companies conducting employee searches. This study examined some of the complexities involved and some possible alternatives in addressing those complexities.