

## MONITORING THE ELECTRONIC WORKPLACE

*Jonathan Topazian*

### **A. Introduction**

Forty years ago, well before the advent of the electronic workplace, the Maryland Court of Appeals first recognized that individuals have a legal right to a certain degree of privacy in their personal affairs. See Carr v. Watkins, 227 Md. 578 (1962). The essence of the right to privacy is the right to be left alone. See Household Finance Corporation v. Bridge, 252 Md. 531, 537 (1969).

“However, it is exceedingly difficult to apply privacy rights in the context of employee relations because the very nature of the employment relationship is antithetical to the right to be let alone.” S. Mazaroff, Maryland Employment Law, § 5.04 (2d Ed. 2001). This is because an employer has a legitimate interest in all aspects of the background and conduct of an applicant or employee insofar as that background and conduct could impact on experience, qualifications and performance on the job. After all, the employment relationship is a voluntary one, and by entering into that relationship, the employee agrees to give up certain aspects of his or her privacy that pertain to the employment relationship. In other words, the employees may be said to have checked their privacy rights at the door as a condition of their employment, at least when it comes to the everyday events occurring in the workplace.

Beginning in 1970, the Maryland General Assembly has passed a variety of legislation that carves out certain areas in which an individual enjoys privacy rights even in the context of the employment relationship. For example, employers which reject applicants on the basis of a negative credit report are required, among other things, to inform the applicant of the fact that they were rejected on the basis of the credit report and the identify of the individual or entity who provided the report. Md. Commercial Law Article, § 14-1204. Employers in Maryland cannot require applicants or employees to take polygraph exams (lie detector tests) as a condition of employment. Md. Labor & Employment Article, § 3-702. Maryland employers are prohibited from inquiring into an applicant's physical or mental disabilities, as well as treatment for such conditions, absent a direct relationship to the applicant's ability to perform the job; they may not force an applicant or employee to disclose criminal charges that have been expunged; and they may not ask an applicant or employee about the use of legally prescribed drugs or other substances that are not prohibited by Maryland law. Md. Labor & Employment Article, § 3-710; Md. Annotated Code Article 27, § 740; Md. Health-General Article, § 17-214.1(h).

Although the General Assembly has set forth by statute certain areas of private affairs which cannot be transgressed even in the context of the employment relationship, the advent of the electronic workplace has raised a veritable host of issues touching upon the realm of private affairs not addressed directly by legislation. This paper examines employee privacy rights with respect to employer monitoring of computer, e-mail and Internet, monitoring of telephone and voice mail, as well as video and other surveillance of employees in the workplace.

**B. Employers Have Legitimate Business Reasons To Monitor The Electronic Workplace**

Many employers monitor or contemplate monitoring employee phone calls, e-mail transmissions and Internet usage. For example, more than two thirds of employers engage in some monitoring of employees, and e-mail monitoring doubled between 1997 and 1999. Lavelle, Survey Shows Increase In Firms That Monitor Employee Communications Knight-Rider Trib. Bus. News (4/16/99) (reporting American Management Association survey of over 1000 member companies). Furthermore, video-taping of employees has dramatically increased and new surveillance techniques have been developed, including tracking systems, such as those utilized by the trucking industry, that inform employers where their employees are and for how long.

There are many legitimate reasons for such monitoring. Employers may be liable for sexual and other forms of workplace harassment based upon the transmission of inappropriate electronic messages and materials within the workplace. See Autoli ASP, Inc. v. Dep't of Workforce Services, 29 P.3d 7 (“e-mail transmission of sexually explicit and offensive material such as jokes, pictures, and videos exposes the employer to sexual harassment and sex discrimination lawsuits”); Harley v. McCoach, 928 F. Supp. 533 (E.D. Pa. 1996) (African-American employee received e-mail addressing her as “Dear Brown Sugar.”)

Additionally, employers have a legitimate expectation that working hours be spent on the business of the employer rather than personal, non-employment related conduct via phone lines, e-mail transmissions, and Internet or web surfing. Similarly, many employers have legitimate reasons to engage in video surveillance of employees, not only to ensure productivity, but also to prevent employee misconduct such as harassment, violence, theft and vandalism.

However, under certain circumstances, employers may be found liable under an invasion of privacy theory in monitoring their employees. In 1999, for example, four employees of Wal-Mart were awarded \$20 million for, among other things, invasion of privacy. The company

covertly videotaped them eating snacks from damaged containers and fired them under the company's anti-pilferage policy. See Richman, Restoring the Balance: Employer Liability and Employee Privacy, 86 Iowa Law Review 1337 (2001) (discussing Stringer v. Wal-Mart Stores, Inc., (Ky. Ct. App. 1999).

## **C. The Federal And State Wiretapping And Electronic Communications Acts**

### **1. Monitoring Communications After Transmission**

One of the most frequently asked questions is whether electronic surveillance and monitoring of Internet, e-mail and telephone usage violates the federal Electronic Communications Privacy Act (ECPA) and/or the Maryland Wiretapping and Electronic Surveillance Control Act. See 18 U.S.C. 2510, et seq.; Md. Code Ann., Courts and Judicial Proceedings Article, 10-401, et seq. Most courts have held that the federal and analogous state statutes do not apply to monitoring of electronic communications (i.e., e-mail) when access occurs **after** the transmission has been completed.

This is because the federal and state statutes require "interception" of an electronic communication and once the communication has reached its intended recipient and is in electronic storage, the communication can no longer be intercepted within the meaning of the Act. See, e.g., Steve Jackson Games, Inc. v. United States Secret Service, 36 F.3d 457 (5<sup>th</sup> Cir. 1994); Eagle Investment Systems Corp. v. Tamm, 146 F. Supp. 2d 105 (D. Mass. 2001); Fraser v. Nationwide Mutual Insurance Co., 135 F. Supp. 2d 623 (E.D. Pa. 2001); Wesley College v. Pitts, 974 F. Supp. 375 (D. Del. 1997).

In this regard, a recent Virginia case held that searching an employee's computer hard drive for evidence of e-mail communication records is not an interception of electronic communications within the meaning of the ECPA. United States v. Simmons, 92 F. Supp. 324

(E.D. Va. 1998). There, the employer did not copy the employee's e-mail while it was being sent or received by the employee. Instead, the employer copied the employee's pornographic e-mails that had previously been stored on his hard drive. Therefore, there was no interception.

On the other hand, in Sanders v. Robert Bausch Corp., 38 F.3d 736 (4<sup>th</sup> Cir. 1994), the employer installed a "voice logger," which recorded all telephone conversations, 24 hours a day, 7 days a week, on certain phone lines. The Court found that this monitoring violated the ECPA because plainly there was an interception of telephonic (wire) communications while they were taking place.

## **2. Interception of Electronic Communications**

Maryland's statute, like the federal ECPA, also is limited to interception of wire and electronic communications. However, where communications **are intercepted** during the transmission, Maryland law provides more protection than its federal counterpart because consent (which can be obtained from the employee by a well-drafted computer and telephone use policy, as discussed below) must be obtained from **all parties**, rather than just one party as required under the federal ECPA. See 18 U.S.C. 2511(2)(d) (permitting interception of electronic communications where one party has given prior consent to interception).

### **C. The Tort Of Invasion Of Privacy**

Putting aside the ECPA and its state counterpart, the common law of most states, including Maryland, recognizes a variety of claims for invasion of privacy, including the tort of unreasonable intrusion upon the seclusion or private affairs of another. In Pemberton v. Bethlehem Steel Corporation, 66 Md. App. 133 (1986), the Court held that the plaintiff must show that there was an intentional intrusion upon seclusion and that the intrusion would be highly offensive to a reasonable person. To determine whether there is an intrusion upon

seclusion, it must be determined whether there is a reasonable expectation of privacy in the zone or area in which the intrusion occurs. Ferman v. Sheppard, 130 Md. App. 67 (1998).

### **1. E-Mail And Internet Monitoring**

Although monitoring e-mail and Internet usage does not violate the ECPA, provided that there is no interception, employees plainly may have invasion of privacy claims if they can show a reasonable expectation of privacy in their stored electronic communications. In this regard, employers may overcome individual employee's expectations of privacy by carefully drafting and disseminating an electronic communications policy. First, the policy should plainly state that electronic communications are to be used solely for company business, and that the company reserves the right to monitor or access all employee Internet or e-mail usage. The company further should emphasize that it will keep copies of Internet or e-mail passwords, and that the existence of such passwords is not an assurance of the confidentiality of electronic communications. The policy also should include a prohibition against the transmission of any discriminatory, offensive or unprofessional messages, and should inform employees that access to Internet web sites that are obscene, offensive or discriminatory is strictly prohibited. Furthermore, the policy should state that no employee is permitted to post personal opinions or messages on the Internet using the company's access, particularly if the opinion or message is discriminatory or offensive.

### **2. Interception Of Telephonic Communications**

Absent consent of one or all parties to the interception of telephone calls, such practices absent consent of the participants to the communication may violate the Federal ECPA (at least one party must consent) and the Maryland counterpart (all parties must consent). In Simmons v. Southwestern Bell Co., 452 F. Supp. 392 (W.D. Ok. 1978), the Court concluded that implied

consent existed where the employer had a well known telephone monitoring policy and prohibition against using company phones for personal calls. On the other hand, in Watkins v. L.M. Berry & Co., 704 F.2d 577 (11<sup>th</sup> Cir. 1983), the employer notified its employees that it would monitor their phone calls, and that their personal calls would be monitored, but only to determine if their calls were personal in nature, rather than business-related. The Court held that this notification was sufficient to imply consent to the monitoring of business phone calls, but not the monitoring of personal phone calls.

As with Internet and e-mail, a well-defined telephone policy that limits or precludes personal phone calls should be implemented by employers to avoid creating any expectation of privacy among employees, thus foreclosing invasion of privacy claims. Furthermore, employers who decide to electronically monitor employee telephone calls are well-advised to have in place a voice greeting that informs incoming callers that their calls may be monitored for quality control or other internal purposes, as well as the well-defined telephone usage policy that informs employees that their calls, whether personal or business-related, may be monitored in conjunction with the policy.

### **3. Video Surveillance And Monitoring**

The ECPA and its state counterpart do not apply to video surveillance and monitoring of employees because the statutes apply only to the interception of oral and wire communications. See Ricks v. State, 312 Md. 11 (1998). However, where video surveillance is conducted in an offensive and intrusive manner, employer may create invasion of privacy claims in their employees. The question is really one of degree. Liberti v. Walt Disney World, 912 F. Supp. 1424 (1995), provides an example of how not to conduct video surveillance. There, a Disney employee, who worked as a costume designer, was also a voyeur. The female plaintiffs were

performers for Disney's King of the Kingdom show, and were provided female-only dressing rooms. The voyeur employee made holes in the dressing rooms so that he could see into them while the performers were undressing and using the bathroom. He did not stop there, however. He set up a video apparatus and filmed the female employees on multiple occasions in various stages of undress and while using the bathroom. After several months, Disney security became aware of these activities, but did nothing to correct the situation for many months. Finally, Disney decided to conduct a sting operation by setting up its own video surveillance system. None of the female employees were informed so they could take measures to protect themselves and both the employees and the voyeur were video taped for over an hour in the dressing room area. Under these circumstances, the plaintiffs prevailed on their invasion of privacy claims.

#### **D. Conclusion**

The Maryland Courts have yet to decide a case where employees have asserted claims for invasion of privacy in the context of monitoring employee electronic or wire communications. However, Faulkner v. State, 317 Md. 441 (1989) provides useful guidance in this respect. There, the employer provided a locker to each of its employees which remained the property of the employer. Lockers were used by employees both to keep personal items and to store company equipment. Under the rules of the workplace, the employer reserved the right to search lockers upon reasonable suspicion of improper use. As a result of wide-spread complaints of illegal drug use by its employees, management conducted an investigation, broke into the plaintiff's locker, and found illegal drugs.

The Court of Appeals in Faulkner found that, under these circumstances, management retained the prerogative to engage in the search, that the employee had, at best, only a minimal expectation of privacy, and thus the search was not unreasonable. The court's reasoning in

Faulkner supports the conclusion that employees do not have a reasonable expectation of privacy with regard to contents of their stored wire and electronic communications when they have been placed on notice that the employer fully reserves the right to access and monitor their communications for reasonable business-related purposes.