

## **THE COMMENTATORS**

### **How to Manage Employee Blogging and Other Cyber Issues**

**By Megan M. Belcher, Esq., SPHR and Tracy Gullickson, Esq.**

Technological advances — blogging, e-mail, fax machines, voice mail, and closed-circuit television — offer employers previously unprecedented opportunities to carefully monitor and gauge employee production, performance, behavior, and compliance. Today's employees are exposed to many types of privacy-invasive monitoring including: closed-circuit video monitoring, Internet monitoring and filtering, e-mail monitoring, instant message monitoring, phone monitoring, location monitoring, and keystroke logging. Technological advances allow employers to determine:

- whether an employee is blogging at work;
- whether an employee's email content is pertinent to work related issues;
- when an employee's machine or computer is running;
- the time it takes to perform certain job functions or tasks;
- an employee's error rate or correction percentage;
- how many data entries are made per minute;
- how many mistakes are made within that minute;
- how many customers are served within a given amount of time;
- how many breaks are taken within a given amount of time; and
- the numbers called from telephone extensions and the length of such calls.

Employers have legitimate interests in ensuring that their employees are not engaging in activities that may interfere with the productivity of the entire company—or potentially damaging public communications—costing an employer significantly in lost production. Employers will most likely want to ensure that:

- employees are using work time for the benefit of their employers;
- employee's on-duty telephone calls are in fact business-related;
- employee's use of company time, equipment and supplies furthers business objectives;
- employees are not stealing products or information;

- employees are not engaging in illegal activity at the workplace; and
- employees are not incurring viruses that could sabotage business equipment via internet usage; and
- employees are not subjecting their employers to liability for: sexual harassment, hostile work environment, or wrongful termination.

To prevent litigation costs, employers **must** understand the legal restrictions of employee monitoring and investigation to maximize technological advances and minimize legal liabilities. An employer should establish written policies, purchase requisite software tools, educate employees on its policies, and have employees acknowledge and agree to its policies.

## **I. LEGAL RECOMMENDATIONS FOR MONITORING AND INVESTIGATING EMPLOYEES**

When considering the appropriateness of employer monitoring and investigations, courts use a balancing test to evaluate the reasonableness of the means utilized by employers versus the cause and purpose of such monitoring. Because challenges to employer monitoring or investigation are based primarily on privacy grounds, employers can improve their positions by putting employees on notice of possible investigations and workplace monitoring. Employers can achieve this goal by adopting and publishing specific monitoring policies. Employees who have notice of their employer's policies generally cannot demonstrate any reasonable expectation of privacy in the observed or investigated activity.

For example, where the employer intends to monitor telephone calls, examine computer files, or scrutinize e-mail messages and voice mail messages, the employer should adopt a policy alerting employees to that possibility. Not only does this decrease an employee's argument that he or she reasonably expected the information to remain private and confidential, but also, publication of such a policy should result in deterring those problems that the monitoring seeks to uncover.

As with so many other areas of employment law, the best defense to a legal challenge is to ensure that any information gathered regarding an employee is legitimately job-related. Training supervisors in proper monitoring methods, as well as appropriate counseling, disciplining, and termination of employees who violate legitimate work rules and expectations, will help employers avoid legal liability. In any event, a legal opinion as to the lawfulness of an intended monitoring device is advisable.

Employers also should adopt appropriate document retention – and purging – procedures. Employers should control what goes into business computers and adopt policies regarding appropriate use of inter-office communication. These policies will help to prevent an employer's e-mail and voice-mail systems from becoming the conduit of inappropriate and unprofessional humor or commentary.

Further, employers should periodically review the need for routine investigations. Information should not be gathered when there is no need and employers should limit their

surveillance activities to public places where no reasonable expectation of privacy exists. Employers should confirm, when possible, the accuracy of any data obtained via employee monitoring. To the extent possible, employers also should keep all information obtained in an investigation strictly confidential.

## II. GENERAL LEGAL FRAMEWORK

Three primary sources could potentially regulate or curtail employer monitoring: constitutional protections, common law or tort claims, and statutory protections.

### A. Constitutional

In most states, including in Missouri, non-governmental, private sector employers are outside the purview of constitutional protections afforded to governmental employees. Federal courts have consistently refused to extend the Fourth Amendment right against unreasonable search and seizure to private employers, though some courts applying state invasion of privacy laws have permitted actions for violation of privacy rights.<sup>1</sup> Therefore, the primary source of legal protection for private, non-unionized employees, and thus the primary source risk of legal liability for alleged violations of an employee's privacy, is tort law.

### B. Common Law or Tort

Generally, employee monitoring and searching that is uniformly and openly applied will not give rise to wrongful discharge liability, absent a collective bargaining agreement or other employment agreement of a definite duration.<sup>2</sup> In the absence of a cause of action for wrongful discharge, the remaining tort actions available to non-union, private employees to challenge employer monitoring activities are derivatives of the tort of outrage. Such torts include invasion of privacy and intentional infliction of emotional distress, sharing a common requisite element: that the employer's behavior be egregious, extreme, and outrageous. For example, in *Bodwig v. K-Mart, Inc.*, 635 P.2d 657 (Or. Ct. App. 1981), a female cashier employed by K-Mart was accused by a female customer of taking the customer's four five-dollar bills. After searching the cashier's pockets, work area, and register to no avail, K-Mart's female assistant manager conducted a strip search of the female cashier in the customer's presence. The bills were not located and, not surprisingly, the cashier sued K-Mart for outrageous conduct. The Oregon Court of Appeals held that a jury should be allowed to determine whether K-Mart's conduct of subjecting its employee to a strip search in the presence of a customer was "beyond the limits of social toleration and reckless of the conduct's predictable effects on plaintiff." *Id.* at 661.<sup>3</sup>

---

<sup>1</sup> See *Webster v. Motorola Corp.*, 418 Mass. 425 (1994) (private employer's urinalysis drug testing of all employees without regard to job duties violated the state privacy law).

<sup>2</sup> See *Borse v. Piece Goods Shop, Inc.*, 963 F.2d 611 (3d Cir. 1992) (the First and Fourteenth Amendments do not create the mandated public policy necessary to support private employee's claimed wrongful discharge and violation of public policy).

<sup>3</sup> See also *Massey v. Victor L. Phillips Co.*, 827 F. Supp. 597 (W.D. Mo. 1993) (claims for intentional infliction of emotional distress brought by defendant's sole female employee based on existence of "peep hole" between only bathroom available for her use and the male supervisory employees' bathroom was dismissed on procedural grounds).

### C. Statutory Regulation

Besides tort law remedies available to private, non-union employees and, perhaps, because the standard of outrageousness necessary to impose tort liability is so high, statutory regulation of employer monitoring continues to increase. For example, 18 U.S.C. §§ 2510-2521, generally prohibits the use of any mechanical or electronic device to monitor, intercept, or record telephone conversations of other persons without consent. Violators of this federal statute face substantial civil and criminal penalties, including fines of up to \$10,000 and imprisonment for up to five years.

Under what has become known as the **business extension exception**, however, an employer may monitor an employee's telephone conversations at the workplace for legitimate business reasons, including, for example, evaluating the employee's customer relations skills. 18 U.S.C. §§ 2510(4), 2510(5)(a)(i). Two essential elements must be proven before the employer is entitled to the business extension exception, however: (1) the intercepting equipment must be furnished to the user by the phone company or connected to the phone line; and (2) the intercepting equipment must be used in the ordinary course of business. This provision has been consistently interpreted to require that the employer monitor only long enough to determine whether the call is a legitimate business-related call or whether it is of a personal nature. Monitoring beyond that threshold determination can exceed the exception and expose the employer to liability.<sup>4</sup>

In addition to the federal statute, Missouri has a similar provision and exemption. *See* MO. REV. STAT. § 542.402. Under § 542.402, it is permissible under Missouri's wiretapping provisions:

for a person not acting under law to intercept a wire communication where such person is a party to the communications or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act.<sup>5</sup>

### III. MONITORING EMPLOYEE PERFORMANCE AND CONDUCT

Advances in technology greatly enhance the means and manner for employers to monitor employees and investigate suspected misconduct. However, technological advances may threaten legitimate privacy interests. Accordingly, employers should understand the lawful

---

<sup>4</sup> *See, e.g., MGM Inc. v. Liberty Mut. Ins. Co.*, 855 P.2d 77 (Kan. 1993) (even if employer's contention that employees were aware of existence of concealed recording devices installed in employer's ceiling to monitor unauthorized long distance calls were true, such knowledge would not constitute "consent" and therefore could not be a defense to prohibited monitoring); *see also Deal v. Spears*, 980 F.2d 1153 (8th Cir. 1992) (monitoring device purchased by defendant employer at Radio Shack was neither furnished by phone company nor connected to phone line; furthermore, defendants' recording and listening to entirety of 22 hours of calls went beyond the legitimate determination of whether phone calls were personal and in violation of company policy and therefore went "**well beyond the boundaries of the ordinary course of business.**").

<sup>5</sup> *See also State v. King*, 873 S.W.2d 905, 909-910 (Mo. Ct. App. 1994).

methods and permitted scope for monitoring and investigating employee behavior, performance, and misconduct.

## A. Surveillance

Technological advances have greatly enhanced the means and manner of employee surveillance, which has become quite routine. As a result, advances in technology and increases in employee surveillance may threaten legitimate privacy interests. Accordingly, employers must recognize and understand that lawful surveillance depends on its nature and its purpose. The key factor in determining whether surveillance is lawful is whether the employee's reasonable expectation of privacy was violated.

### 1. Visual Surveillance

To investigate employee behavior, allegations, and/or suspicions of misconduct, employers may conduct surveillance simply by observing employee activities, photographing<sup>6</sup> employees who are in plain view at work stations during regular working hours,<sup>7</sup> or researching employee compliance with company orders.<sup>8</sup> Also, often times employers can lawfully videotape employees and photograph employees in the workplace.<sup>9</sup>

Employers additionally can use surveillance to investigate employee workers' compensation claims when an employer observes the employee outside of his or her home and in a location observable to the public.<sup>10</sup> Courts find that employee claims for workers' compensation provide notice for and furnish awareness of a possible investigation.<sup>11</sup> Generally,

---

<sup>6</sup> However, in the absence of some special justification or circumstance, the National Labor Relations Board ("NLRB") specifically prohibits videotaping or photographing employees engaged in any statutorily protected activity. *Waco, Inc.*, 273 NLRB 746 (1984); *Hoschton Garment Co.*, 279 NLRB 565 (1986) (Mere observation of union activity or employee protest in a public area does not automatically create impermissible surveillance).

<sup>7</sup> See *Munson v. Milwaukee Bd. of School Directors*, 969 F.2d 266 (7th Cir. 1992) (finding employer's surveillance of public school principal formed no invasion of privacy claim where surveillance determined principal's residence conformed with school board policy and observation took place from public streets and highways); *Smith v. Colorado Interstate Gas Co.*, 777 F. Supp. 854 (D. Colo. 1991) (finding that an employee under close observation at her desk did not form any invasion of privacy); *Thomas v. General Elec. Co.*, 207 F. Supp. 792 (W.D. Ky. 1962) (noting that videotapes were an efficient, effective, and economical means of studying and establishing safe and effective procedures).

<sup>8</sup> *Schibursky v. International Business Machines Corp.*, 820 F. Supp. 1169 (D. Minn. 1993) (finding no cause of action for infliction of emotional distress although employer used managers, co-workers, and security personnel to monitor the employee's behavior and even authorized the use of the company's computer system in violation of standard policy because the employee repeatedly was warned to decrease her hours of overtime).

<sup>9</sup> *Barksdale v. International Business Machines Corp.*, 620 F. Supp. 1380 (W.D. N.C. 1985) (Observing and recording the performance of temporary employees during a study of computer equipment did not intrude on employees' seclusion and in most instances would be found lawful).

<sup>10</sup> See *Johnson v. Corporate Special Serv., Inc.*, 602 So.2d 385, 387 (Ala. 1992).

<sup>11</sup> See *McLain v. Boise Cascade Corp.*, 533 P.2d 343, 346 (Or. 1975); *Warren v. Signal Delivery Service*, 1997 WL 18225, 2-3 (Mo. Ct. App. 1997); *Turner v. General Adjustment Bureau, Inc.*, 932 P.2d 62 (Utah Ct. App. 1992); *Seldana v. Kelsey-Hayes Co.*, 443 N.W.2d 382 (Mich. Ct. App. 1989).

unless the form of surveillance is “conduct utterly intolerable in a civilized society,” the employer’s behavior is lawful. *Schibursky v. International Business Machines Corp.*, 820 F. Supp. 1183 (D. Minn. 1993).

However, surveillance of employees can form impermissible invasions of privacy if the observation takes place in a non-public area where the employee has a reasonable expectation of privacy. In *Speer v. Ohio Dept. of Rehab. & Corr.*, an Ohio court found an employer’s surveillance unlawful and exceeding all reasonable boundaries where the employer placed an employee’s supervisor in the ceiling of a bathroom for more than seven hours to investigate the alleged wrongdoing. *Speer*, 624 N.E.2d 251, 253-54 (Ohio Ct. App. 1993).

Similarly, in *Doe by Doe v. B.P.S. Guard Services, Inc*, the Eighth Circuit found that a cause of action for invasion of privacy exists so long as “there was an objectionable intrusion into the plaintiffs’ enjoyment of an area that the plaintiffs had a right and expectation of privacy.” *Doe by Doe v. B.P.S. Guard Services, Inc*, .945 F.2d 1422, 1427 (8th Cir. 1991). A company hired a guard service for security at a fashion show and then the service rigged a video camera to view and record the models as they undressed. The Eighth Circuit rejected the employer’s claims that no models were viewed or recorded undressing and found a valid cause of action.<sup>12</sup>

Further, surveillance of employees who are off the job presents different issues and is more likely to be interpreted as unlawful behavior. Since employees have greater expectations of privacy outside the workplace, surveillance creates a greater liability risk.

## **B. Electronic Interception And Non-Electronic Eavesdropping**

### *1. Federal Regulation*

New technology has meant new and expanded means of surveillance. Congress enacted the Electronic Communications Privacy Act of 1986 (ECPA), which amended the Omnibus Crime Control Act of 1968, to respond to technological developments and to protect the privacy of “wire communications.” 18 U.S.C. §§ 2510-2521.

The Act prohibits the “intentional” interception<sup>13</sup> of “any wire, oral, or electronic communication,” the use of an electronic service to effect that end by means of transmission, and the intentional disclosure of the content of such communications “knowing or having reason

---

<sup>12</sup> An independent contractor’s privacy was not infringed by video taping of the entrance to the women’s locker room. The camera was installed inside the locker room, but pointed only to the door and away from the interior of the room. This was done to catch a male supervisor suspected of sneaking into the locker room with a female subordinate. *Brazinski v. Amoco Petroleum Additives Company*, 6 F.3d 1176 (7<sup>th</sup> Cir. 1993).

<sup>13</sup> “Interception” is defined as the “acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.” 18 U.S.C. § 2510(4).

to know that the information was obtained” through an interception in violation of the Act. 18 USC at § 2511.<sup>14</sup>

The Electronic Communications Privacy Act also addresses electronic mail (e-mail) and other computerized message systems.<sup>15</sup> These prohibitions on interception and disclosure of the contents of an “electronic communication” apply to computerized mail and message systems if the “system” is one that “affects” interstate or foreign commerce.<sup>16</sup>

However, the Act exempts the interception of an electronic communication system that is configured such that the electronic communication is readily accessible to the general public. 18 U.S.C. § 2511(2)(g)(i). Interestingly, one court also has indicated that an unauthorized interception of e-mail messages would violate the ECPA only where the e-mail message is “intercepted” (and not simply read after it has been delivered) by a non-intended recipient. *See Steve Jackson Games, Inc. v. U.S. Secret Service*, 36 F.3d 457 (5th Cir. 1994). Additionally, § 2511(1)(b) prohibits the use of, or the procurement to use, a device to intercept any oral communication<sup>17</sup> when the use takes place on the premises of or concerns any business.

However, these broad and sweeping prohibitions contain several exemptions that have particular relevance or application in the employment arena and to today’s employers. First, the Act does not prohibit an employer from intercepting or accessing an electronic communication made through a speaker that makes the communication readily accessible to the general public. 18 U.S.C. at § 2511(2)(g)(i). Second, the Act does not prohibit an employer from using a “pen register or trace device” as defined under the federal Act at § 2511(2)(h)(i). Third, interception excludes:

any telephone or telegraph instrument, equipment or facility, or any combination thereof, (i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business. . .”

---

<sup>14</sup> The term “wire communication” was expanded to include digital voice transmissions and voice transmissions by radio or fiber optic cable, and the term “electronic communications was added to include electronic mail, digitized transmissions, and video teleconferences.

<sup>15</sup> 18 U.S.C. §§ 2510-2521 (1993).

<sup>16</sup> 18 U.S.C. § 2570(12).

<sup>17</sup> An “oral communication” is defined as one uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication. 18 U.S.C. at § 2510(a).

18 U.S.C. at § 2510(5)(a). Finally, the Act does not prohibit an employer from intercepting a wire, oral, or other electronic communication “where one of the parties to the communication has given prior consent<sup>18</sup> to such interception.”<sup>19</sup> 18 U.S.C. at § 2511(2)(d).

## 2. State Law

The federal statutes do not preempt greater privacy protections given by state law. Accordingly, employers must recognize that although federal law allows interception and no violation occurs with at least the consent of one party to the conversation, several states require the consent of both parties in order to lawfully intercept.<sup>20</sup> However, Missouri has a statute similar to the federal provisions which does not require both parties’ consent. See MO. REV. STAT. § 542.402. Additionally, besides state statutory protection, telephonic interception may violate a state’s common law of privacy.<sup>21</sup> Even in states with common law privacy rights, if an employer informs employees of the monitoring, then generally the employees have no reasonable expectation of privacy and no unreasonable intrusion can occur. *Jackson v. Nationwide Credit, Inc.*, 426 S.E.2d 630 (Ga. Ct. App. 1992).

## C. Searches

### 1. Public/Governmental Employers: Fourth Amendment

Governmental employees have Fourth Amendment<sup>22</sup> constitutional protections against unreasonable searches and seizures by their employers.<sup>23</sup> To be unlawful, a governmental

---

<sup>18</sup> Consent to an interception may be express or implied, but it may not be implied “cavalierly” – knowledge of the “capability of monitoring alone cannot be considered implied consent.” *Watkins v. L.M. Berry & Co*, 704 F.2d 577, 581 (11th Cir. 1983).

<sup>19</sup> This exemption does not allow an employer to intercept for the purpose of committing a crime or tort.

<sup>20</sup> See CAL. PENAL CODE §§ 631-632; DEL. CODE ANN. tit. 11, § 1336(b); FLA. STAT. § 934.03(2)(d) (1985); GA. CODE ANN. § 16-11-66 (1990); ILL. ANN. STAT., ch. 38, § 14-2 (Smith-Hurd) (1979); MD. CODE ANN. CTS. & JUD. PROC. § 10-402(c)(3) (1989); MASS. GEN. LAWS ANN. ch. 272, § 99(B)(4) (Michie/Law. Co-op 1992); MICH. COMP. LAWS § 750.539c; MONT. CODE ANN. § 45-8-213(c) (1993); N.H. REV. STAT. ANN. § 570-A:2 (1986); PA. CONS. STAT. tit. 18, §§ 5703-5704 (1983); WASH. REV. CODE § 9.73.030 (1988).

<sup>21</sup> *Binkley v. Loughran*, 714 F. Supp. 776 (M.D. N.C. 1989); *Awbrey v. Great Atlantic & Pac. Tea Co., Inc.*, 505 F. Supp. 605 (N.D. Ga. 1980); *Oliver v. Pacific Northwest Bell Telephone Co.*, 632 P.2d 1295 (Or. App.) (reviewing authority), *review denied*, 642 P.2d 310 (Or. Ct. 1981).

<sup>22</sup> The Fourth Amendment states that, in part, “the right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures, shall not be violated.”

<sup>23</sup> The following cases involve Fourth Amendment violations.

- Public employer violated the Fourth Amendment by requiring mandatory AIDS and Hepatitis B testing for health services employees where any risk of disease transmission was minuscule. *Glover v. Eastern Nebraska Community Office of Retardation*, 867 F.2d 461 (8th Cir. 1989).
- Public employer violated the Fourth Amendment by searching all cars leaving the parking lot where employer could not offer any reason for conducting the search. *McGann v. Northeast Illinois Regional Commuter R.R. Corp.*, 8 F.3d 1174 (7th Cir. 1993).
- Public employer violated the Fourth Amendment by subjecting employees to routine strip and body cavity

employer search must infringe on a reasonable expectation of privacy. In *O’Conner v. Ortega*, the United States Supreme Court distinguished between areas and items that are work-related and personal belongings that fall within the realm of privacy. *O’Conner*, 480 U.S. 709 (1987). In *O’Conner*, while a state hospital physician was on administrative leave, his office was searched and the hospital seized his personal items, including a photograph, a valentine’s card, and a book of poetry. The Supreme Court discussed that the physician had a reasonable expectation of privacy in his desk and file cabinets, remanding the case to determine if the search was reasonable. The Supreme Court found that searches investigating worker misconduct or searches for even non-investigative reasons (retrieving business files or documents) are presumptively lawful. The Supreme Court also noted that an employee’s expectation of privacy “may be reduced by a virtue of actual office practices and procedures, or by a legitimate regulation.” Accordingly, to decrease employees’ reasonable expectations of privacy, employers should increase their access to employees’ work space.<sup>24</sup> Obtaining an employee’s prior consent also would likely preclude any challenge to an employer’s search.<sup>25</sup>

## 2. *Private Employers*

Although constitutional protections only apply to governmental employees and the Fourth Amendment does not bind private employers unless the employer acts under the auspices of the government, employees of private entities still may challenge an inappropriate search or seizure on other legal grounds. However, since the Fourth Amendment does not extend the right against unreasonable searches and seizures to private employers, challenges to searches conducted by private employers are rare and seldom successful.<sup>26</sup>

Generally, employers may search employees’ offices, desks, credenzas, and filing cabinets to locate particular items during an employee’s absence or to investigate allegations of

---

searches where no legitimate reason for searches was found. *Security and Law Enforcement Employees, Dist. Council*, 737 F.2d 187 (2d Cir. 1984).

- Public employer violated the Fourth Amendment by subjecting police officers to random urinalysis testing where nothing revealed an existing drug problem or public perception of problems from drug use. *Guiney v. Police Com’r of Boston*, 411 Mass. 328 (Mass. 1991).

<sup>24</sup> See *Williams v. Philadelphia Housing Authority*, 826 F. Supp. 952 (E.D. Pa. 1993) (the court found that a search of an employee’s desk while the employee was on medical leave was proper because the search was not associated with an attempt to discover employee misconduct but instead to locate documents).

<sup>25</sup> See *American Postal Workers Union v. U.S. Postal*, 871 F.2d 556 (6th Cir. 1989) (postal workers who accepted lockers knowing the lockers were subject to inspection at any time waived any Constitutional claim for privacy); *Bateman v. State*, 513 So.2d 1101 (Fla. Ct. App. 1987) (acceptance of government employment does not eliminate Constitutional claim for invasion of privacy or alone form consent to lawful searches without violating Fourth Amendment protections).

<sup>26</sup> But, private employers who are acting on behalf of government are subject to Fourth Amendment limitations against unreasonable searches or seizures.

misconduct.<sup>27</sup> Employers also may inspect employees' lockers, handbags, vehicles, and parcels if the employee is exiting the premises.<sup>28</sup>

However, if an employee can lock his or her locker, desk, credenza, etc., then the employer's search of employees' personal belongings may form an invasion of privacy and may create a question of fact for the jury.<sup>29</sup> Employers also may violate public policy by terminating employees who refuse to submit to searches of their personal property.<sup>30</sup>

Accordingly, to protect against the possibility of unreasonable searches or seizures, private employers should: (1) follow an established policy authorizing searches and stating the circumstances and manner; (2) obtain consent from the employee; and (3) conduct the search in a responsible, non-discriminatory manner. Reasonable searches that are a part of an employer's legitimate work-related investigation or part of an unannounced policy generally are lawful and do not create any invasion of privacy.

For example, in *Doe v. Kohn, Nast & Graf, P.C.*, the employer searched an employee's unlocked desk and credenza for sales records. The court found that the employee had no reasonable expectation that his employer would not search his desk for company documents. *Doe*, 862 F. Supp. 1310 (E.D. Pa. 1994). Under the analysis used in that ruling, employers must show no reasonable expectation of privacy was encroached by their behavior.

#### **IV. EMPLOYEES' USE OF TECHNOLOGICAL ADVANCES**

Although the focus of this discussion is generally monitoring and investigating by employers of employee activity, it is noteworthy that these technological advances can be, and frequently are, used by employees. For example, many employers are surprised to learn that their conversations with current employees, or terminated employees, may be surreptitiously recorded by the employee or former employee who obviously knows and consents to the recording. This is a frequent tactic used by such employees or former employees to entrap employers in the hopes of advancing potential or existing litigation. Similarly, what your employees — supervisory and non-supervisory — “say” to one another on e-mail or voice-mail is discoverable and can be used, for example, as evidence of a racially or sexually hostile environment.

---

<sup>27</sup> *O'Donnell v. CBS, Inc.* 782 F.2d 1414 (7th Cir. 1986) (finding no invasion of privacy where executive's secretary unlocked his credenza and removed incriminating papers after executive provided her with the key, implicitly consenting).

<sup>28</sup> *Gretencord v. Ford Motor Co.*, 538 F. Supp. 331 (D. Kan. 1982); *Rebel v. Unemployment Compensation Board of Review*, 450 A.2d 305 (Pa. Comm. Ct. 1982).

<sup>29</sup> For example, an employer's search of an employee's hotel room was found to violate the employee's privacy interests, and an employer's opening of an employee's personal mail was an invasion of privacy. *Sowards v. Norbar*, 605 N.E.2d 468 (Ohio Ct. App. 1992); *Vernars v. Young*, 539 F.2d 966 (3d Cir. 1976); *K-mart v Troin*, 677 S.W.2d 632 (Tex. Ct. App. 1984).

<sup>30</sup> *Borse v. Piece Goods Shop, Inc.*, 963 F.2d 611 (3d Cir. 1992).

## A. Harassment and Discrimination

In recent years, a number of lawsuits alleging harassment and discrimination have included allegations of harassment or discrimination by e-mail. In one recent decision, a Pennsylvania district court referred to such messages as “e-harassment” where a new attorney’s supervisor harassed her by sending sexually explicit and graphic e-mail messages.<sup>31</sup> Additionally, provision of Internet access gives employees the capability to access and download sexually explicit or racially derogatory material right at their workstations. Such capability raises questions and concerns of liability when employees bring such material to the office from the outside, along with the additional wrinkle that the employee has now accessed such material through a company system.

This is troubling for employers for numerous reasons. Computer investigation companies are now able to search company computers and, in some instances, even rebuild hard drives to locate messages containing objectionable content. Even where companies do not know that such information is transmitting through their systems, employees may allege that the employer was negligent because it allowed harassing or discriminatory material to be transmitted on the company system. If an employer has not taken measures to prohibit or prevent the transmission, or has failed to respond adequately when it becomes aware of such transmission, the employer may be liable for negligence as well as the harassment that occurred.

In one high-profile lawsuit, two African-American employees of Morgan Stanley & Co. filed a \$60 million lawsuit in 1996 against the investment banking firm claiming that they were professionally isolated and denied advancement after they complained about an e-mail containing racist jokes.<sup>32</sup> The e-mail had been disseminated on the firm’s computer system. The same employees responsible for circulating the e-mail message through the company’s e-mail system were also responsible for reviewing one of the employee’s work performance. The lawsuit was settled in a confidential agreement for an undisclosed sum of money.

In another lawsuit, this one filed against Microsoft Corporation, a district court found that the plaintiff presented sufficient evidence, including inappropriate remarks and harassing e-mail messages, for a jury to conclude that Microsoft’s business reason for failing to promote a female employee was pretextual and that Microsoft failed to promote the female as a result of gender discrimination.<sup>33</sup>

In Texas, two employees sued Worldcom Corporation on grounds of race discrimination and negligence for allowing the company e-mail system to be used for transmission of racially derogatory jokes.<sup>34</sup> The e-mail messages were sent by non-managerial employees at Worldcom. After employees brought the e-mails to the attention of Worldcom supervisors, the supervisors organized two meetings to discuss proper use of the e-mail system and reprimanded the

---

<sup>31</sup> *Rudas v. Nationwide Mut. Ins. Co.*, No. 96-5987, 1997 WL 11302 (E.D. Pa. Jan. 10, 1997).

<sup>32</sup> *Owens v. Morgan Stanley & Co.*, No. 96 CIV.9747(DLC), 1997 WL 793004 (S.D.N.Y. Dec. 24, 1997).

<sup>33</sup> *Strauss v. Microsoft Corp.*, 856 F. Supp. 821 (S.D.N.Y. 1994)

<sup>34</sup> *Daniels v. Worldcom Corp. Worldcom Comms., Inc.*, No. CIV.A.3:97-CV-0721 P., 1998 WL 91261 (N.D. Tex. Feb. 23, 1998).

employee who sent the message. Additionally the Company had an established policy regarding the use of e-mail. Based on the company's established e-mail policy and actions taken after the employer found out about the e-mail message, the court held that the evidence showed that the employer acted reasonably and plaintiff's claim for negligence therefore failed as a matter of law.

Lawsuits involving inappropriate e-mail communications and access of sexually explicit or racially derogatory material on the Internet are certain to increase with the rapid expansion of employee access to e-mail and the Internet in the workplace. Employers must also be on the lookout for inappropriate use of camera phones by their employees. Employers should address these issues by establishing acceptable use systems policies, as well as anti-discrimination and anti-harassment policies, before such problems arise.

### **B. Preventing Theft of Confidential Information**

In addition, one of the major concerns with the emergence of camera phones on the market is the potential that such small, inconspicuous devices could be used as a device to steal trade secrets and other confidential information. The prospect camera phones might be used for such a purpose is all the more disconcerting to employers given that pictures taken via camera phones can be transmitted instantaneously over the internet to individuals who may not have the company's best interests in mind. Moreover, the fact such pictures may have been taken is not easily traceable when taken with a personal camera phone, as opposed to removing and copying actual paper files or copying files from the company's computer systems. This is enough of a fear that several large corporations with significant interest in their trade secrets and proprietary information, including DaimlerChrysler, BMW, and Samsung (ironically, the largest manufacturer of camera phones), have banned them entirely from some of their sites. Other companies like Texas Instruments allow employees to bring their camera phones into work, but prohibit them from taking any pictures with them. Still other companies post signs prohibiting the possession of camera phones in certain areas containing trade secrets or other proprietary information. In lieu of those more drastic measures, companies can also consider revising their trade secret policies to clarify that confidential documents and/or trade secrets can neither be "copied" or "photographed."

### **V. FORMULATING CORPORATE SYSTEMS POLICIES (i.e., Computer, E-mail, Internet, and Voicemail)**

Established, written policies regarding employee use of e-mail, internet, and other corporate systems can reduce employer liability in several ways. First, such policies can successfully deter undesired use of company systems. Employees who are aware that their communications can be monitored by their employer are likely to think twice before transmitting inappropriate or unprofessional material via the company e-mail system. Likewise, an employee who understands that the employer may obtain a list of Internet sites accessed by each employee is less likely to spend his time at work accessing X-rated sites. Second, courts may be less likely to hold an employer liable for certain activities, including harassment and discrimination, where the employer can produce an established policy prohibiting such uses. Third, employees will not be able to successfully argue that they had a reasonable expectation of privacy where company

policies clearly state that information transmitted and accessed on company systems is not private or confidential.

Establishing policies regarding use of camera phones in the workplace poses a different issue since most, if not all, camera phones are personally owned by the employee, not provided by the employer. As discussed above, however, some employers may want to consider a complete or partial ban in the workplace, revise their anti-discrimination and anti-harassment policies to prohibit inappropriate use of camera phones, establish a code of conduct to protect employee privacy, and revise their trade secret policies to prohibit photographing confidential documents.

When formulating corporate systems policies, employers must draft provisions specific to their company networks, industries and uses. However, there are several areas of concern that every employer should evaluate and use as guidelines when creating systems policies.

**A. Employees Do Not Have An Expectation of Privacy in Information Transmitted or Accessed on Company Systems**

Employers should have written policies with respect to each system -- computer use, e-mail, voice-mail and the Internet -- clearly stating that the system is provided for business use only and notifying employees that they have no expectation or guarantee of privacy with regard to information transmitted or accessed through each system. A copy of each policy should be distributed to each employee. A signed acknowledgment of receipt of each policy kept in the employee's personnel file. Additionally, employers should periodically remind employees by written memorandum, e-mail, or periodic flash-ups on each employee's computer screen that the information is not private, may be monitored, and use is governed by written corporate policy.

The policy should further require employees to provide the employer with all log-ons and passwords used by the employee. Use of passwords and log-ons unknown to the employer should be prohibited. These measures further reduce employees' expectation of confidentiality and privacy.

**B. Set Forth Employer's Business Reasons for Monitoring and Accessing Use of Its Systems**

Policies should clearly state that the employer's systems are provided by the company and are to be used for work-related purposes only, and that all information transmitted on the system is the property of the Company. Make it clear that Internet transactions and other communications transmitted from the Company network could be perceived as activities authorized by the Company. Consequently, all users must follow applicable laws, regulations and policies when accessing the Internet or transmitting information on the Company's system.

**C. Outline Acceptable and Unacceptable Uses of Company Systems**

It is not necessary for employers to create an exhaustive list of acceptable and unacceptable uses of company systems. However, it is helpful for employers to include a list of particular areas of concern to the employer. For example, the policy might specifically state that users may not attempt to gain unauthorized access to the Company's system or to access another

employee's account. Additionally, the policy might specifically prohibit acts that could disrupt company systems - such as spreading computer viruses or downloading large files without permission from the system administrator.

The policy should clearly state that any listing of unacceptable uses is not all-inclusive of the prohibited uses of the system.

**D. Warn Employees of Disciplinary Consequences for Violating the Policy and Employer Will Report and Prosecute Illegal Activities**

It is not necessary for the policy to set forth specific disciplinary consequences corresponding with the various violations of the policy. Rather, the employer may state that it retains discretion to determine discipline for violations of the policy, up to and including termination.

Additionally, the policy may state that any uses of the system in violation of the law will be reported and prosecuted.

**E. Amend Existing Anti-Harassment and Discrimination Policies to Clearly Prohibit the Transmission and Access of Inappropriate Material Via E-Mail, Voice-Mail and Internet**

In addition to formulating policies governing acceptable uses of Company e-mail, voice-mail, and Internet systems, employers should review and revise current policies governing workplace behavior. Employers should amend anti-harassment and discrimination policies to clearly state that the transmission and access of harassing and discriminatory material via company systems are prohibited under such policies.

**F. Formulating Camera Phone Policies**

Establishing policies regarding use of camera phones in the workplace poses a different issue since most, if not all, camera phones are personally owned by the employee, not provided by the employer. However, some employers may want to consider a complete or partial ban in the workplace, revise their anti-discrimination and anti-harassment policies to prohibit inappropriate use of camera phones, establish a code of conduct to protect employee privacy, and revise their trade secret policies to prohibit photographing confidential documents.

**VI. CONCLUSION**

Employers should give employee monitoring and investigations thoughtful consideration. Companies should weigh the potential benefits of employee monitoring and investigating against the potential legal risks and impact on employee morale. The interests of employers and employees are not always at odds. Both groups are often concerned about the quality of the work environment. Respect for employee privacy is important, and is one factor people consider when deciding whether to apply for a job, take a job, or keep a job. Consistent with employers' goal of maintaining a productive workforce is their goal of attracting good employees and keeping them happy. However, the line separating a reasonable intrusion on employee privacy

from one that is unreasonable is often neither clear nor bright, and courts are routinely asked to draw the line for labor and management as a whole.

Different technologies and techniques obviously carry different risks and benefits. Whatever method an employer may choose, implementing workplace policies, conducting appropriate investigations, informing employees of possible monitoring, and enacting training programs are the best sources of protection against legal challenge.

The following list provides general areas of consideration to properly investigate and monitor employees and to protect the employer's interest and minimize legal liability.

- Understand that most communication media in the workplace are not generally protected under the law and security/confidentiality measures are the burden of the employer.
- Inform employees what aspects of the workplace should not create an expectation of privacy — i.e., monitored phone calls, lockers, desks, workplace items.
- Train supervisors to conduct appropriate monitoring and lawful searches.

Inform employees of what is and is not considered confidential or privileged in the workplace — i.e., personnel information, computer data, files, e-mail and voice mail.

- Document that employees have been educated and notified regarding the company policy and that they have given consent to the monitoring of interactions transmitted over business-owned equipment.
- Monitor and enforce the company policies with regularity, avoiding focus on select individuals.
- Become generally familiar with the Wiretapping laws to know when it is improper to intercept wire and cable communications.
- Put securities measures in place to avoid retrieval of stored information – computer access codes, locked files.
- Be aware that employees can legally tape record conversations with supervisors.