



NATIONAL WORKRIGHTS INSTITUTE

Bringing Human Rights to the Workplace

Privacy Under Siege:

Electronic Monitoring in the Workplace

166 WALL STREET, PRINCETON N.J. 08540 • (609) 683-0313 • FAX (609) 683-1787
WWW.WORKRIGHTS.ORG

INTRODUCTION

Everyone in the office knew that Gail would change her clothes in her cubicle for the gym after the work day was done. When her employers installed a hidden camera to monitor the person in the neighboring cubicle's suspected illegal activities, her daily ritual was captured on film. The first few times could have been labeled as mistakes, but the filming of Gail changing her clothes over a five month period was inexcusable.¹

Electronic monitoring is a rapidly growing phenomenon in American businesses. Introduced in the early twentieth century for such limited uses as timing breaks and measuring hand-eye movements, systematic electronic monitoring has since grown into the very fabric of American business practice. As technologies become more powerful and easy and inexpensive to install and maintain, the rates of electronic monitoring in this country have skyrocketed. In 1999 the percentage of employers who electronically monitor their workers was 67%.² Just two years later, in the year 2001 this number had increased to 78%.³ By 2003, 92% of employers were conducting some form of workplace monitoring.⁴ This rapid growth in monitoring has virtually destroyed any sense of privacy as we know it in the American workplace. Employers now conduct video surveillance, listen in on employee telephone calls, review employee computer use such as e-mail and the Internet and monitor their every move using GPS. But as legitimate work product is being monitored, so are the personal habits and lives of employees. As technology has proliferated in the workplace, it has become ever more penetrating and intrusive. And yet there are few, if any, legal protections for employees. There has been no attempt to balance employer demands with legitimate employee privacy concerns. Collection and use of personal information is a rampant byproduct of workplace monitoring and threatens the very freedoms that we cherish as Americans. Legislation is necessary to govern the practice of electronic monitoring in the workplace, protect employee privacy and return a sense of fundamental fairness and dignity to the American workplace.

¹ Gail Nelson v. Salem State College Civil Action No. 98-1986C

² 1999 American Management Association Survey, "Workplace Monitoring and Surveillance"

³ 2001 American Management Association Survey, "Workplace Monitoring and Surveillance"

⁴ 2003 Center for Business Ethics at Bentley College, "Survey 'You've Got Mail...And the Boss Knows'"

PRIVACY AND INTRUSION ISSUES

While employers generally initiate electronic monitoring in response to legitimate business concerns, the results have been devastating to employee privacy. Virtually everything we do and say at work can be, and is, monitored by our employers. Our employers listen watch us on video cameras, read our e-mails, listen to our voice mail, review documents on our hard drives, and check every web site we visit.

This would be bad enough if it involved only work related behavior and communication, but it doesn't. The advent of cell phones, pagers, and home computers is rapidly erasing the traditional wall between the home and the workplace. People now regularly receive communications from their employer at home. Maggie Jackson, former workplace correspondent for the Associated Press, estimates that the average professional or managerial employee now receives over 20 electronic messages from work every week.⁵ This new flexibility also means that personal communication increasingly occurs in the workplace. An employee who spent much of the weekend on a cell phone with her boss will not (and should not) consider it inappropriate to make a personal call from the office.

This means that employer monitoring systems frequently record personal communications. Often, this communication is not sensitive. But sometimes the messages are very personal. An employee who sends their spouse a romantic e-mail while eating lunch at his or her desk can find that their love letter has been read by their boss. Or a note to a psychiatrist stored in an employee's hard drive is disclosed.

Internet monitoring can be extremely invasive. People today turn to the Internet as their primary source of information, including sensitive subjects they would be uncomfortable communicating about on their office telephone or e-mail. In part, this is because of the efficiency of internet research. Even an untrained person can find information on the web in minutes that would have taken hours or even days to find by traditional means (if they could find it at all). People also turn to the Internet for information because they can do so anonymously.

The result is that people turn to the Internet for information and help about the most sensitive subjects imaginable. Women who are victims of domestic abuse turn to the Internet for information about shelters and other forms of help. People also turn to the Web for information and help with drug and alcohol problems, financial difficulties, marital problems, and medical issues. Monitoring Web access gives an employer a picture window into employees' most sensitive personal problems.

Most invasive of all is video monitoring. Some cameras are appropriate. Security cameras in stairwells and parking garages make us all safer without intruding on privacy. But employers often install cameras in areas that are completely indefensible. Many

⁵ Conversation with Maggie Jackson, former workplace correspondent for the Associated Press, April 2002.

employers have installed hidden video cameras in locker rooms and bathrooms, sometimes inside the stalls. No one should be subjected to sexual voyeurism on the job.

Such problems are made worse by the manner in which monitoring is often conducted. Most employers make no effort to avoid monitoring personal communications. The majority of employers install systems that make no distinction between business and personal messages, even when more discriminating systems are available.

In addition to official monitoring, IT employees often monitor their fellow employees for personal reasons. Most employers give such employees carte blanche access to employee communications. While it is possible to set up technical barriers to ensure that monitoring is confined to official programs, few employers use them. Many employers do not even have policies directing IT employees to restrict their monitoring to official programs. Even employers with such policies rarely have procedures to enforce them. As a result, employees involved in monitoring often read the messages of fellow employees for their own amusement.

The final indignity is that employees don't even know when they are being watched. While a majority of employers provide employees what is described as notice, still many do not and the information currently provided is generally useless. The standard employer notice states only that the company reserves the right to monitor anything at any time. Employees do not know whether it is their e-mail, voice mail, Web access, or hard drive that is monitored. They do not know whether the monitoring is continuous, random, or as needed. They do not even know whether they are being monitored at all. Such notice is almost worse than no notice at all.

As bad as the situation is today, it is likely to be far worse in the future. Many people today do work for their employer on their home computers. The most direct example of this is telecommuting. Approximately 20 million employees and independent contractors now work at home at least one day per month,⁶ and this number is growing rapidly. Millions more have linked their home computer to their office network so they can work from home informally on evenings and weekends.

When this occurs, people's home computers are subject to monitoring by their employer. Workplace computer monitoring systems monitor the entire network, including a home computer that is temporarily part of the network. This means that personal communications in our home computers will be revealed to our employers. Personal e-mail sent from or received by our home computers will be disclosed to our employers, along with personal letters, financial records, and any other personal information in our home computers. Not only is this possible, it is highly likely. When asked if they would be interested in having personal information from employees' home computers, corporate attorneys responded positively.⁷

⁶ O'Brien, Kathleen. "Taking Advantage of the Mobil Office: Homeward Bound", *The New York Times*, April 5, 2000 Section G, p.1.

⁷ 1999 Midwinter Meeting of the Committee on Employee Rights and Responsibilities, American Bar Association Section on Labor and Employment Law, March 22-24 1999.

MONITORING AND PRODUCTIVITY

Employers generally conduct electronic monitoring in order to increase productivity. It is far from clear, however, that monitoring achieves this goal. In fact, too much monitoring can actually decrease productivity by increasing employee stress and decreasing morale.

In a study conducted for Bell Canada⁸, it was reported that 55% of all long distance and directory assistance operators experienced added stress due to some form of monitoring. Increased stress can often lead to physical symptoms. In a study by the Department of Industrial Engineering, University of Wisconsin-Madison, higher levels of stress in monitored employees resulted in an increase in somatic complaints, including a 27% increase in occurrences of pain or stiffness in shoulders, a 23% increase in occurrences of neck pressure and a 21% increase in back pain experienced by employees. Such stress and stress related symptoms can create medical expenses, lost time and absenteeism.

Studies have shown that the introduction of electronic monitoring into the workplace is likely to encourage employees to favor quantity of work produced over quality. Even employers who do not intend on placing production increases above quality may do so inadvertently, simply because quality is more difficult to monitor electronically. Pressure to increase productivity commonly has adverse effects on the quality of work produced. In two studies published in the *National Productivity Review*⁹ the authors found that “monitored employees were less willing to pursue complex customer inquiries than their unmonitored coworkers.” Similar results were found in other productivity studies.¹⁰

Trust between employee and employer is crucial to maintaining a high level of productivity and unnecessary and covert monitoring is harmful to this balance. A recent study conducted jointly by Microsoft and the London School of Economics found that “providing information in an environment of trust can greatly facilitate the coordination of work.” Indeed “Mutual trust is not an added bonus of the mobile organization, it is an absolute core principle... Mistrust results in the perceived need to engage in activities only serving the purpose of demonstrating ability internally and not generating business value.”¹¹

This does not mean that employers should never collect information about employees' work by electronic means. It does mean, however, that monitoring should not be

⁸ D. DiTecco, Senior Management Sciences Consulting, “Operator Stress and Monitoring Practices.”

⁹ Grant, Rebecca and Christopher Higgins. “Monitoring Service Workers via Computer: The Effect on Employees, Productivity and Service.” *National Productivity Review* Vol. 8 (2) (Spring)

¹⁰ Irving, R.H., C.A. Higgins and F.R. Safayeni. “Computerized Performance Monitoring Systems: Use and Abuse.” *Communications of the ACM* 29 (8)

Aiello, John R. and Kathryn J. Kolb. “Electronic Monitoring and Social Context: Impact on Productivity and Stress.” *Journal of Applied Psychology* 80 93)

Westin, A.F. “Two Key Factors that Belong in a Macroergonomic Analysis of Electronic Monitoring: Employee Perceptions of Fairness and the Climate of Trust.” *Applied Ergonomics* 23(1)

¹¹ Sorenson, Dr. Carsten. “The Future Role of Trust in Work-The Key Success Factor for Mobile Productivity.” <http://members.microsoft.com/advisor/trustinwork/default.msp> (November, 2004)

employed based on a general idea that it will increase productivity. Before initiating any program of monitoring, employers should carefully consider:

1. Why they believe this specific monitoring program will increase efficiency.
2. The effect of the monitoring program on employee stress.
3. The effect of the program upon employee morale.
4. Whether the value of the increased efficiency outweighs the cost of increased stress and decreased morale.

As with any other important decision, employers should attempt to quantify these factors and conduct a cost-benefit analysis.

MORE EFFECTIVE SOLUTIONS

Most employers are not voyeurs. More often than not, they would rather not know personal information about their employees that has no bearing on job performance. Yet there is rarely an attempt to be more discriminating in their practices or a balancing of employer needs with employee privacy concerns. There are a variety of ways that employers can address specific concerns without monitoring highly personal information. The following are a few suggestions.

- Businesses should properly train managers and supervisors to deal with employee issues and problems. Most businesses do not have managers that are properly trained to deal with sensitive employee subjects. These staffs need to be observant and reactive to employee needs. Properly trained managers are a company's best asset in terms of dealing directly with and correcting many of the concerns that prompt the adoption of electronic monitoring practices. Supervising staffs can set conduct guidelines, address concerns, mediate complaints, as well as monitor and deal individually with those employees that choose to abuse company resources.
- Businesses should always conduct an in-house assessment to identify whether electronic monitoring is even necessary. This seems like an obvious point, but many businesses adopt large scale monitoring programs on the assumption that they will add benefits to their workplace without identifying their own specific requirements and whether the adoption of an electronic monitoring program would meet those requirements.
- Before deciding to conduct monitoring, management should speak with employees about the productivity problem. Employees may suggest alternative ways of solving the problem. If monitoring is chosen, employees can participate in designing the monitoring program and its scope in a way that is acceptable to them.
- If monitoring is conducted, the scope should be as narrow as is consistent with achieving the desired objective. Employers should be especially careful to restrict the program to business related communications and avoid monitoring personal communications. Additionally they should utilize web access software that eliminates the need for monitoring each individual website an employee visits.

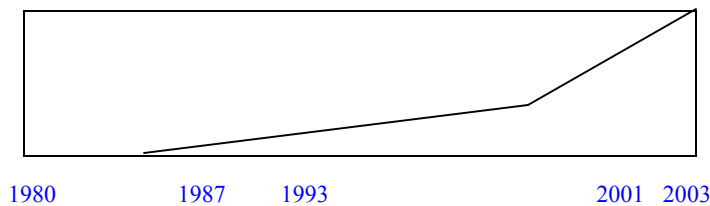
- Consider monitoring on an “event basis.” This involves conducting monitoring when it is known something inappropriate has occurred and confining the monitoring to dealing with that event.
- If a company does choose to adopt a program of electronic monitoring, proper notice should be given well in advance of any monitoring practices. This notice should explicitly state what would be monitored as well as when this monitoring would occur. The American Management Association has recommended that employer's give notice of electronic monitoring since 1997.

THE NUMBERS:

ELECTRONIC MONITORING HAS BECOME A COMMON PRACTICE

Electronic monitoring in the American workplace has seen dramatic growth in recent years. Prior to 1980, electronic monitoring was virtually unknown. When the Congressional Office of Technology Assessment studied its use in 1987, only 7% of employees were affected.¹² But in only 6 years, a MacWorld survey found that electronic monitoring had nearly tripled (to 20% of employees).¹³ In 2001, the American Management Association reported that the percentage of companies monitoring had risen to 78.4%.¹⁴ By 2003, 92% of employers were conducting workplace monitoring.¹⁵

Rate of Monitoring American Workers



Even more troubling are the ways employers monitor:

- 75% of employers that monitor do so without individualized cause¹⁶
- 50% of all employers that do have a monitoring policy do not train their employees about their monitoring policy¹⁷
- 20% of employers do not have a written monitoring policy¹⁸
- 25% of employers do not have in place any procedures or safeguards to ensure that the monitoring process is not abused¹⁹

While the national debate over privacy rages, the unregulated growth of electronic monitoring in the American workplace shows no signs of abating.

¹² "The Electronic Supervisor: New Technology, New Tensions," U.S. Congress, Office of Technology Assessment, OTA-CIT-333 (Washington, DC: U.S. Government Printing Office, September 1987).

¹³ Piller, Charles "Privacy in Peril," *MACWORLD*, July 1993. pp 124-130.

¹⁴ 2001 American Management Association Survey, "Workplace Monitoring and Surveillance"

¹⁵ 2003 Center for Business Ethics at Bentley College, "Survey 'You've Got Mail...And the Boss Knows'"

¹⁶ 2001 American Management Association Survey, "Workplace Monitoring and Surveillance"

¹⁷ 2004 American Management Association "Workplace Email and Instant Messaging Survey" and 2003 Center for Business Ethics at Bentley College, "Survey 'You've Got Mail...And the Boss Knows'"

¹⁸ 2004 American Management Association "Workplace Email and Instant Messaging Survey"

¹⁹ 2003 Center for Business Ethics at Bentley College, "Survey 'You've Got Mail...And the Boss Knows'"

EVERYDAY PEOPLE: STORIES OF WORKPLACE MONITORING ACROSS AMERICA

California:

At a Neiman-Marcus Store in Fashion Island Newport Beach , Kelly Pendleton, a two-time “employee of the year” discovered a hidden camera in the ceiling of the changing room used by female employees that was being monitored by male colleagues.

Employees of Consolidated Freightways were horrified to find that the company had installed hidden cameras in its restrooms- some cameras pointing directly at the urinals. Over a thousand hours of video records were made covering thousands of employees. "The guys were really shaken, and some of the women went home crying," says Joe Quilty, the dockworker who discovered the hidden cameras.

An AT&T employee received a formal reprimand for using the company e-mail system to send a love note to his wife, also an AT&T employee.

9th Circuit Court of Appeals Judges disabled computer monitoring software that had been installed by the Administrative Office of the U.S. Courts without notice or consent. Judge Alex Kozinski charged that the surveillance system was a needless invasion of privacy. Several members of Congress agreed, Rep. Howard Berman wrote “While it may be appropriate to monitor an employee’s Internet use or e-mail in certain circumstances, I do not believe indiscriminate, systematic monitoring is appropriate... Its is particularly inappropriate for the courts, which will inevitably be called on to rule in cases involving questions of employee privacy.”

Alana Shoars was in charge of the Epson Torrance, California plant e-mail system. Ms. Shoars assured Epson Employees that their e-mail was private. She discovered later that her supervisor was reading all employee e-mail in the Torrance plant.

Florida:

An employee of Walt Disney World videotaped female employees in bathrooms and locker rooms. 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 hours in the dressing room area.

The general manager of the Apalachicola Times newspaper installed a hidden video camera in the employee bathroom and made 29 videotapes worth of recordings. Barbara

Lynn Perry, one several women who was regularly videotaped remarked "No one had my permission as far as surveillance...I was never formally or informally asked for my permission. I had no idea there was a camera in the bathroom."

Georgia:

Air force machinist Donald Thompson is placed under investigation by the Office of Special Counsel for forwarding an e-mail lampooning the president's qualifications. "To me, sending it was just an electronic version of water cooler chit chat" he said.

Female employees at a local plant in Pendergrass run by Atlas Cold Storage were regularly videotaped in the bathroom without their knowledge or consent. According to employees, the plant manager would regularly remind them that "there's not anywhere you can go where I can't see you."

Hawaii:

Hawaiian airlines pilot Robert Konop sets up a personal, password protected website so that he and fellow pilots can have private discussions and freely criticize management. A Vice-President of the airline pressures a fellow pilot for the password and accesses the site.

Illinois:

A technology professional was terminated after his boss listened in on a phone conversation he was having with his girlfriend after his shift ended.

An employee quits after his boss announces to the entire office the content of a personal e-mail that had been retrieved from the monitoring system.

Maryland:

A 17 year old woman, Jennifer Smith, testified before the Judiciary Committee of the Maryland House of Representatives that in her job as a lifeguard, she was videotaped changing into her bathing suit by her supervisor at the county swimming pool.

Massachusetts:

At the Sheraton Boston Hotel hidden cameras were discovered in the employee changing room. Hours of tape of employees in different stages of undress were logged. One of the Sheraton workers, Jean L. Clement, stated that: "Learning about the secret videotaping

made me very scared at work because I feel as though I'm being watched wherever I go, which is how I felt when I lived in Haiti."

Nebraska:

Melissa Haines of Broken Bow, an employee of Mid-Nebraska Individual Services, discovered hidden monitors the employer had installed to record personal as well work related conversations. "My job has been awful. Is there anything I can do? What I say to a friend should be confidential" she remarked.

New Jersey:

The City of Clinton Township, NJ installed GPS tracking devices behind the front grilles of patrol cars without notifying their officers.

A female employee logs onto an expectant mothers website at her job during working hours. Just looking for information, the employee tells no one of her possible condition. Soon after, her immediate supervisor congratulates her on her pregnancy.

Heidi Arace and Norma Yetsko, two employees of the PNC Bank were terminated after forwarding jokes on their company's e-mail. Such letters had been regularly sent in the past by fellow employees with the attention of the employer and they had previously never enforced any monitoring policies. As Arace puts it, "I was cold. I was frozen. It was like I lost everything in my life. You get a simple e-mail like this, you read it; you chuckle; forward it on, click. Done deal...everyone was doing it."

New York:

Howard Boyle, president of a fire sprinkler installation company in Woodside, N.Y., presented his employees with cell phones to use without informing them that they were equipped with GPS. Mr. Boyle can find out where they are at all times including during breaks and while they are off duty. "They don't need to know," said Mr. Boyle. "I can call them and say, 'Where are you now?' while I'm looking at the screen and knowing exactly where they are."

Lourdes Rachel Arias and Louis J. Albero discovered that their employer, Mutual Central Alarm Service, was monitoring and recording all incoming and outgoing telephone calls including personal and private conversations without notice or consent.

Pennsylvania:

Despite assurances from his employer that e-mail was confidential, that it would not be intercepted, and that it would not be used for the basis for discipline or discharge, Michael Smyth is terminated for sending an unprofessional message from his home over the company e-mail.

Tennessee:

Joyce Carr and Bernice Christianson discovered that their employer, Northern Telecom, was secretly taping all incoming and outgoing private telephone conversations in a Nashville plant by means of hidden microphones. An investigation discovered systematic efforts by top management to wiretap public pay phones in the employee cafeteria and monitor conversations through microphones in the plant sprinkler system.

Texas:

Microsoft, which had no monitoring policy at the time, opens the personal folders of employee Bill McLaren's office computer even though they are password protected.

Washington:

At Washington's WJLA-TV station, tracking devices were installed in station vehicles supposedly to allow editors to know where the closest vehicle might be to a breaking story, but employees claimed that the devices had been used to monitor them. Employees recounted stories of managers phoning them to instruct them to drive slower or to question them about stopping at certain locations.

ELECTRONIC MONITORING OF EMPLOYEES A LACK OF LEGAL REGULATION

FEDERAL LAW:

The only relevant federal legislation to protect employee privacy is the Omnibus Crime Control and Safe Streets Act of 1968, as amended by the Electronic Communications Privacy Act of 1986. The ECPA, with certain exceptions, prohibits the interception, disclosure, or use of a wire, oral or electronic communication. This protection applies to all businesses involved in interstate commerce and has also been interpreted to extend to most intrastate phone communications. It also applies to conversations between employees that employers may overhear because the employees are wearing headsets. The Act creates both criminal and civil causes of action. Civil remedies may include compensatory and punitive damages, as well as attorney's fees and other litigation costs.

There are three exceptions to this blanket prohibition. One exception allows wire and communications service providers (common carriers) to intercept communications if done for quality of service purposes. Under this exception, a telephone company can monitor its employees to ensure adequate job performance and supervise customer contacts.

A second exception allows interception when there is consent. A party to the communication may intercept the communication, or prior consent may be given by one of the parties to the communication. Generally, courts will not find implied consent. For instance, knowledge of the capability of monitoring alone will not substitute for actual consent. See *Watkins v. L.M. Berry & Co.*, 704 F. 2d 577 (11th Cir. 1983). Consent will be implied where the employee is aware of a general monitoring program and uses a business-only phone to make a personal call when other phones are provided for that purpose. See *Simmons v. Southwestern Bell Tel. Co.*, 452 F. Supp. 392 (W.D. Okla. 1978), *aff'd.*, 611 F 2d 342 (10th Cir. 1979).

The third and primary exception allows for wire eavesdropping when done in the "ordinary course of business": context and content. Under a context analysis, emphasis is placed on the importance of the business policy served by the monitoring and extent to which the monitoring furthers that policy without unnecessarily interfering with employee privacy. Business units whose primary function involves customer contact via telephone have the strongest argument for the legitimacy of monitoring. The "unnecessary interference" element includes considerations of whether the monitoring was announced or covert and whether separate telephones were provided for personal calls. A content analysis focuses on whether the monitored call was personal or business in nature. Regardless of their chosen approach, the courts have consistently held that an employer violates the act when it continues to monitor a purely personal phone call after learning of its personal nature. See *U.S. v. Harpel*, 493 F. 2d 346 (10th Cir. 1974) and

U.S. v. Axselle, 604 F. 2d 414 (5th Cir. 1980). The employer may be limited to a "reasonable" length of time to make this determination. Courts which have considered this question have defined "reasonable" as anywhere from 10 seconds to 5 minutes (See Watkins and Axselle).

ECPA does prohibit access to stored communications (Stored Communications Act) but this prohibition is also subject to severely weakening exceptions. There remain access exemptions for the person or entity providing a wire or electronic communications service and for the user of that service with respect to a communication of or intended for that user. Employers are likely to fall under one or both of such exceptions.

What limited protections ECPA does provide to employees have been greatly weakened because the statute has quickly become outdated. The ECPA does not apply to most common forms of monitoring technologies such as electronic mail monitoring, Internet monitoring and video surveillance. Since ECPA requires an "interception" of a communication, communications in a stored state are exempt. Additionally, as in the case of electronic mail, courts have so far found that company owned proprietary systems are exempt. See Shoars v. Epsom, 90 SWC 112749 and 90 BC 7036 (Superior Court, Los Angeles County). Assurances by employers that monitored and stored employee e-mails are not reviewed by management is no guarantee that employers will not reprimand or terminate employees for the content of their e-mail messages. See Smyth v. Pillsbury & Co. 914 F. Supp. 97, 101 (E.D. Pa. 1996).

Additionally the ECPA does not require an employer to give notice of electronic monitoring practices, nor is there any other statute that requires an employer to give notice of monitoring practices, no matter how invasive the monitoring may be.

STATE LAW:

In addition to federal statute, employees sometimes also receive some privacy protection from various state constitutional, common law and statutory sources. Most states have a constitutional provision that reflects the proscriptions in the Fourth amendment regarding search and seizure. Some states have specific constitutional guarantees of privacy that extend beyond the Federal Constitution's privacy rights. Only California courts, however, have held that the state constitutional right of privacy applies with respect to both public and private employers. See Porten v. University of San Francisco, 134 Cal. Rptr. 839 (Cal Ct. App. 1976) In all other states, employees have successfully invoked the state constitutional right of privacy only after establishing the government as the employer. Some state courts, such as New Jersey and Alaska, have nevertheless determined that their state constitutions can form a basis for creating public policy arguments in favor of a private sector employee's right to privacy.

A majority of states do have statutes restricting the interception of wire communications by private individuals. These states, however, generally mirror the ECPA, and contain similar exceptions and exemptions. Although some states have shown a willingness to legislate in the employee privacy area, the efforts have only been piecemeal. Within the past year California has added a section to its Labor Code that prohibits an employer from monitoring, without a court order, employees in restrooms, locker rooms or other places designated by the employer for changing clothes. Labor Code, Sec 435 (a) to (c). Additionally, Connecticut added a section to its labor code requiring employers to give employees written notice of the types of monitoring which may occur. Conn. Gen. Stat. Sec 31-48d. Nevertheless, state governments have not addressed the issue comprehensively or uniformly, and in most cases have not addressed it at all.

Finally, some limited protections exist in the common law of torts. The tort that most plaintiffs use to challenge employer monitoring and surveillance is the intrusion-on-seclusion tort. The classic conception of this tort, recognized in every state, is that it is used to punish highly offensive privacy invasions. There has been an attempt to apply the tort in the employment context to challenge workplace monitoring abuses. Under present law, however, formidable obstacles face the employee who wishes to bring such a privacy claim.

First, the intrusion-on-seclusion tort requires the employee to establish that the monitoring conduct is highly objectionable to a reasonable person. Because routine monitoring can appear harmless from some perspectives (especially that of a third party), and because the negative effects of such monitoring are often gradual and incremental, this standard frequently forecloses an employee claim. In particular, when the monitoring complained of has been arguably linked to work-related activities, those challenges have been unsuccessful. See *Barksdale v. IBM* 620 F. Supp. 1380 (W.D.N.C. 1985). Additionally, courts have not been receptive to employee claims that their work environments contain sufficiently private spaces for an invasion of privacy to occur. See *Ulrich v. K-Mart Corp.*, 858 F. Supp. 1087 (D. Kan. 1994). For example, an employee's office, desk or locker may be held to be the employer's property, and therefore not private. The combination of these elements typically defeats an employee's tort claim in all but the most egregious of circumstances, which usually involve monitoring in areas such as bathrooms or locker rooms. Even in such highly private areas, state court decisions are mixed. See, for example, *Speer v. Department of Rehabilitation & Correction*, 646 N. E. 2d 273 (Ohio Ct. Cl. 1994).

QUESTIONS AND ANSWERS

IS THERE A NEED FOR WORKPLACE PRIVACY LEGISLATION?

Yes. The explosion of workplace surveillance in recent years has stripped Americans of virtually all their privacy on the job. Nearly 80% of employers now use electronic surveillance. Soon it will be universal. Employer monitoring practices often go well beyond specific and even legitimate management concerns. They are rarely tailored to meet individual employer demands or balanced with employee privacy concerns. Current laws are outdated, vague or more often silent on this issue. A balance between the legitimate concerns of business and employee privacy must be created.

SHOULD EMPLOYERS GIVE NOTICE OF MONITORING?

Yes. Employers may need to conduct monitoring for quality control and other business reasons, but they do not need to do it in secret. Indeed, the American Management Association and most corporate counsels recommend that employers provide notice of monitoring programs. Legitimate monitoring programs do not need to be carried out behind employees' backs. Secret monitoring is not only unnecessary, it is counter-productive. The purpose of monitoring is to ensure that employees are following company policy regarding the use of electronic communications technology. If employees know that the company monitors e-mail or Internet access, they will be more careful to follow the rules. Most important, secret monitoring is ethically wrong. People have a right to know when they are being watched. Reading someone else's messages without telling them is both deceptive and a profound violation of their privacy.

IN WHAT SITUATIONS SHOULD MONITORING BE LIMITED?

Employers have legitimate reasons for many monitoring programs. Company e-mail systems have sometimes been used to send inappropriate material that contributes to a hostile environment. The seemingly endless level of information on the Internet has led some employees to spend excessive time at work web surfing. Employers need to respond to these concerns. But, without limitation, employers' efforts to prevent abuse can often lead to serious invasions of privacy. People are not robots. They discuss the weather, sports, their families, and many other matters unrelated to their jobs while at work. While many of these non-work related conversations are innocuous, some are highly personal. An employee might tell her best friend about problems with her husband or share concerns about family financial problems, or their fear that their child may have a drug problem. Most employers are not voyeurs. More often than not, they would rather not know personal information about their employees that has no bearing on job performance. Yet there is rarely an attempt to separate personal from business related

communications. An employer is well equipped to run an efficient and productive business without monitoring the content of personal communications.

Clearly the most invasive workplace monitoring practice; video surveillance of highly private areas such as bathrooms and locker rooms is never conducted in the ordinary course of business and is ripe for abuse. Employees have a heightened expectation of privacy and personal autonomy in such areas. Such monitoring destroys the very essence of human dignity, is highly degrading and such activity disproportionately involves the secret photography of women. The decision to breach such highly sensitive areas and to what degree, is a decision better suited to the reasoned judgment of a court of law.

WHY SHOULD THE GOVERNMENT BE ENTITLED TO DICTATE HOW PRIVATE MANAGEMENT CAN RUN THEIR BUSINESSES?

The government at times must act to ensure that management treats its workers fairly and justly. In the past, Congress has passed numerous laws placing restrictions on private business activities. Such laws include actions prohibiting private businesses from hiring children, discriminating against women and minorities, and paying sub-minimum wages. In addition, legislation has been enacted to ensure employees' rights to organize unions, and to receive prior notice of expected plant closings. Today, in order to protect employees' right to privacy and dignity, restrictions on electronic monitoring by employers must be enacted.

FEDERAL LEGISLATIVE HISTORY

Congress has introduced two notable bills in the past fifteen years to protect employee privacy. These bills were endorsed by a variety of civil rights and labor organizations.

The Privacy for Consumers and Workers Act

On February 27, 1991, the late Senator Paul Simon and Representative Pat Williams introduced the PCWA. The bill would have required employers to clearly define their privacy policies and notify prospective employees of those practices that would affect them. It would have required that surveillance be limited to job related functions and would have prohibited such surveillance of personal communications. It would have prohibited video surveillance in highly personal places such as bathrooms (unless there was suspicion of illegal conduct) and would have required notification when telephone monitoring was taking place. Additionally, it would give employees access to records collected as a result of surveillance.

The Notice of Electronic Monitoring Act

A more limited version of PCWA was introduced by Senator Schumer on July 20, 2000. NEMA would have subjected an employer to liability for intentionally monitoring an employee without first having given the employee substantive notice that the employer was engaged in such a monitoring program. Notice fulfilling the requirements of the Act would include the type of monitoring taking place, the means, the type of information that would be gathered including non-work related information, the frequency of monitoring and how the information would be used. An exception to such notice was made if the employer had reasonable grounds to believe the employee was engaged in illegal conduct and surveillance would produce evidence of such. NEMA put no actual restrictions on an employer's ability to monitor as long as they complied with the notice provisions.

WORKPLACE PRIVACY ACT

A BILL

To amend title 18, United States Code, to authorize electronic monitoring conducted in the ordinary course of business, provide for the disclosure of electronic monitoring of employee communications and computer usage in the workplace and limit electronic monitoring in highly sensitive areas of the workplace.

Section 1. Short Title

This Act may be cited as the ‘ Workplace Privacy Act’

Section 2. Electronic Monitoring in the Workplace

(a) IN GENERAL- (1) Except as otherwise specifically provided in this section, an employer may, by any electronic means, read, listen to, or otherwise monitor any wire communication, oral communication, or electronic communication of an employee of the employer, or otherwise monitor the computer usage of an employee of the employer if the monitoring meets the requirements of sections (b) and (e) and-

(A) The monitoring is conducted at the employer’s premises and

(B) The monitoring is conducted in the normal course of employment while the employee is engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the employer.

(2) An employer who conducts monitoring in violation of this section shall be liable to the employee for relief as provided in subsection (f).

(b) IN GENERAL- (1) Except as provided in subsection (d), an employer who intentionally, by any electronic means, reads, listens to, or otherwise monitors any wire communication, oral communication, or electronic communication of an employee of the employer, or otherwise monitors the computer usage of an employee of the employer, without first having provided the employee notice meeting the requirements of subsection (b) shall be liable to the employee for relief as provided in subsection (f).

(2) Not later than one year after first providing notice of electronic monitoring under paragraph (1), and annually thereafter, an employer shall provide notice meeting the requirements of subsection (b) to all employees of the employer who are subject to such electronic monitoring.

(3) Before implementing a material change in an electronic monitoring practice described in paragraph (1), an employer shall provide notice meeting the

requirements of subsection (b) to all employees of the employer who are subject to electronic monitoring covered by that paragraph as a result of the change.

(c) NOTICE- A notice meeting the requirements of this subsection is a clear and conspicuous notice, in a manner reasonably calculated to provide actual notice, describing--

- (1) the form of communication or computer usage that will be monitored;
- (2) the means by which such monitoring will be accomplished and the kinds of information that will be obtained through such monitoring, including whether communications or computer usage not related to the employer's business are likely to be monitored;
- (3) the frequency of such monitoring; and
- (4) how information obtained by such monitoring will be stored, used, or disclosed.

(d) EXCEPTION- An employer may conduct electronic monitoring described in subsection (a) without the notice required by subsection (b) if the employer has reasonable grounds to believe that--

- (1) a particular employee of the employer is engaged in conduct that--
 - (A) violates the legal rights of the employer or another person; and
 - (B) involves significant harm to the employer or such other person;and
- (2) the electronic monitoring will produce evidence of such conduct.

(e) IN GENERAL- (1) No employer or agent of an employer may engage in video or audio monitoring of an employee in bathrooms, dressing rooms, locker rooms, or other areas where employees change clothing unless--

(A) Such monitoring is authorized by court order.

(2) An employer who conducts monitoring in violation of this section shall be liable to the employee for relief as provided in subsection (f).

(f) CIVIL ACTION- (1) Any person aggrieved by any act in violation of this section may bring an action in a United States district court.

(2) a court in an action under this section may award--

- (A) actual damages, but not less than liquidated damages in the amount of \$5,000;
- (B) punitive damages;
- (C) reasonable attorneys' fees and other litigation costs reasonably incurred; and
- (D) such other preliminary and equitable relief as the court determines to be appropriate.

(g) ENFORCEMENT ACTION BY SECRETARY-

(1) In General- Any employer who violates this section shall be liable to the United States for a civil money penalty in an amount not to exceed \$10,000 for

each violation, except that, if the violation is knowing, the penalty for the violation may be up to \$25,000.

(b) Written Notice and Opportunity for Hearing- The Secretary of Labor shall assess a civil penalty under subsection (a) by an order made on the record after opportunity for a hearing provided in accordance with section 554 of title 5, United States Code. In connection with the hearing, the Secretary may issue subpoenas requiring the attendance and testimony of witnesses and the production of evidence that relates to the subject matter of the hearing.

(c) Determination of Amount of Civil Money Penalty- In determining the amount of a civil money penalty under subsection (a), the Secretary shall take into account--

(1) the nature, circumstances, extent, and gravity of the violation or violations; and

(2) with respect to the violator, the ability to pay, effect on ability to continue to do business, any history of prior violations, the degree of culpability, and such other matters as justice may require.

(h) WAIVER OF RIGHTS- (1) The rights provided by this Act may not be waived by contract or otherwise, unless such waiver is part of a written settlement to a pending action or complaint.

(i) PREEMPTION- (1) Nothing in this Act shall be construed to preempt, modify, or amend any State, county, or local law, ordinance, or regulation providing greater protection to the privacy of employees.

