United States. Congress. Senate

S. HRG. 102-482

PRIVACY FOR CONSUMERS AND WORKERS ACT

D435
16

HEARING

BEFORE THE

SUBCOMMITTEE ON EMPLOYMENT AND PRODUCTIVITY

OF THE

COMMITTEE ON LABOR AND HUMAN RESOURCES UNITED STATES SENATE

ONE HUNDRED SECOND CONGRESS

FIRST SESSION

ON

S. 516

TO PREVENT POTENTIAL ABUSES OF ELECTRONIC MONITORING IN THE WORKPLACE

SEPTEMBER 24, 1991

Printed for the use of the Committee on Labor and Human Resources

U.S. GOVERNMENT PRINTING OFFICE

52-658 ⇆ WASHINGTON : 1992

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402
ISBN 0-16-037658-0

COMMITTEE ON LABOR AND HUMAN RESOURCES

EDWARD M. KENNEDY, Massachusetts, *Chairman*

CLAIBORNE PELL, Rhode Island
HOWARD M. METZENBAUM, Ohio
CHRISTOPHER J. DODD, Connecticut
PAUL SIMON, Illinois
TOM HARKIN, Iowa
BROCK ADAMS, Washington
BARBARA A. MIKULSKI, Maryland
JEFF BINGAMAN, New Mexico
PAUL D. WELLSTONE, Minnesota
ORRIN G. HATCH, Utah
NANCY LANDON KASSEBAUM, Kansas
JAMES M. JEFFORDS, Vermont
DAN COATS, Indiana
STROM THURMOND, South Carolina
DAVE DURENBERGER, Minnesota
THAD COCHRAN, Mississippi

NICK LITTLEFIELD, *Staff Director and Chief Counsel*
KRISTINE A. IVERSON, *Minority Staff Director*

SUBCOMMITTEE ON EMPLOYMENT AND PRODUCTIVITY

PAUL SIMON, Illinois, *Chairman*

TOM HARKIN, Iowa
BROCK ADAMS, Washington
BARBARA A. MIKULSKI, Maryland
JEFF BINGAMAN, New Mexico
EDWARD M. KENNEDY, Massachusetts
(Ex Officio)
STROM THURMOND, South Carolina
DAVE DURENBERGER, Minnesota
NANCY LANDON KASSEBAUM, Kansas
DAN COATS, Indiana
ORRIN G. HATCH, Utah
(Ex Officio)

BRIAN KENNEDY, *Chief Counsel and Staff Director*
KENT DEAN TALBERT, *Minority Counsel*

92-191250

KF26
.L2737
1991

CONTENTS

STATEMENTS

SEPTEMBER 24, 1991

	Page
Simon, Hon. Paul, a U.S. Senator from the State of Illinois, prepared statement	2
Cameron, Cindia, field organizer, 9to5, National Working Women's Organization, Atlanta, GA; Carol Scott, consumer representative, New Jersey Central Power and Light, Asbury Park, NJ; and Renee Maurel, reservationist, Northwest Airlines, Seattle, WA	3
Prepared statement of:	
Ms. Cameron (with an attachment)	6
Bahr, Morton, president, Communication Workers of America, Washington, DC, accompanied by Lou Gerber, legislative representative; Gary T. Marx, sociology professor, Massachusetts Institute of Technology, Cambridge, MA; and Marc Rotenberg, Washington director, Computer Professionals for Social Responsibility, Washington, DC	15
Prepared statements of:	
Mr. Bahr (with attachments)	17
Mr. Marx (with attachments)	45
Mr. Rotenberg	69
Ruffolo, Vincent, president, Security Companies Organized for Legislative Action, Chicago, IL, accompanied by Larry Sabbath, Rowland and Sellery; Lawrence Fineran, assistant vice president of government regulation and competition, National Association of Manufacturers, Washington, DC; and Edward A. Merlis, vice president for policy and planning, Air Transport Association, Washington, DC	82
Prepared statements of:	
Mr. Ruffolo	84
Mr. Fineran	88
Mr. Merlis	92
Thurmond, Hon. Strom, a U.S. Senator from the State of South Carolina, prepared statement	98

ADDITIONAL MATERIAL

Articles, publications, letters, etc.	
Questions and Answers:	
Responses to Senator Thurmond's questions from Ms. Cameron	99
Responses to Senator Thurmond's questions from Ms. Maurel	100
Questions from Senator Thurmond for Mr. Rotenberg	101
Responses to Senator Thurmond's questions from Mr. Bahr	102
Responses to Senator Thurmond's questions from Mr. Marx	102
Responses to Senator Thurmond's questions from Mr. Ruffolo	103
Responses to Senator Thurmond's questions from Mr. Fineran	104
Responses to Senator Thurmond's questions from Mr. Merlis	105
Responses to Senator Kassebaum's questions from Mr. Merlis	105

KF26
.L2737
1991x

PRIVACY FOR CONSUMERS AND WORKERS ACT

TUESDAY, SEPTEMBER 24, 1991

U.S. SENATE,
SUBCOMMITTEE ON EMPLOYMENT AND PRODUCTIVITY, OF THE
COMMITTEE ON LABOR AND HUMAN RESOURCES,
Washington, DC.

The subcommittee convened, pursuant to notice, at 3:02 p.m., in room SD–430, Dirksen Senate Office Building, Senator Paul Simon (chairman of the subcommittee) presiding.

Present: Senators Simon and Metzenbaum.

OPENING STATEMENT OF SENATOR SIMON

Senator SIMON. The subcommittee will come to order.

I will enter my written statement into the record.

Today we are going to hear testimony on S. 516, the Privacy for Consumers and Workers Act. We face a world with increasing technology, and one of the questions that we face in Government fairly regularly is how do we balance our freedom with this technology. What we want in this legislation is to strike a balance.

This legislation does not outlaw monitoring, but it says you have to have certain restrictions. The FBI, interestingly, cannot, even in the case of suspected treason, just with impunity go and monitor telephone calls. We have laws that they have to follow before they can tap a phone.

The bill is not written in concrete, and I think we can work out sensible accommodations. I read the testimony of Mr. Ruffolo, and it seems to me that most of the concerns that he has can be resolved through amendments. And that may be true—I have not read the other testimony yet—of some others who have concerns about this.

We are not stopping monitoring; what we are saying is there ought to be notification.

There is no question that workplace monitoring causes stress. What stress causes in this country no one knows. My staff has a document here that says it costs $50 billion a year. I think that is taken out of thin air. I don't think anyone knows. But whether it is $5 billion or $10 billion or $20 billion or $50 billion, there is no question it is costly in our society.

And in a very real sense, this is a women's issue. Women are disproportionately impacted through this because they are employed more in the type of jobs that are monitored.

It is very interesting that in a country like Japan you have virtually none of the kind of monitoring that we are talking about here

today because the Japanese believe that it would harm labor-management relations.

Today's *Wall Street Journal* has an article on this issue and it says, "Now, however, Bell Canada has stopped gauging individual AWT's except for new employees. Instead, the company averages the scores for entire offices without any decline in efficiency. Others have begun similar policies."

I think we can find some sensible answers if we work at it. I might add this is a general subject that's not new to me. Way back when I was in State legislature, and my wife was also in the State legislature, and we introduced legislation which became law in Illinois which put restrictions on wiretaps that could be made by individuals or police organizations, and we have learned to live with these things.

The reality is we want to have a free society. The reality is also we have all kinds of new technology. How do we find a balance—that's what we hope to get from our witnesses here today.

[The prepared statement of Senator Simon follows:]

PREPARED STATEMENT OF SENATOR SIMON

Today we will hear testimony on S. 516, the Privacy for Consumer and Workers Act, which would prevent potential abuses of electronic monitoring in the workplace. I am proud to be joined by my colleague, Senator Paul Wellstone, in sponsoring this important legislation.

Significantly, S. 516 does not prohibit electronic monitoring; it is simply a notification bill. The legislation strikes a careful balance between the demands for technological change and the need for citizen protection. S. 516 preserves the fundamental right to privacy in an era of growing use of surveillance technologies in the workplace.

According to a 1987 Office of Technology Assessment report, a conservative estimate of 6 million employees were monitored at that time. This figure, however, does not include professional, technical, and managerial workers, which would add an additional one to two million monitored employees. Moreover, as the workplace becomes more computerized and service oriented, the number of those electronically monitored will increase.

S. 516 does not say that electronic monitoring should not be used. What it does say is that electronic monitoring should not be abused. Employees should not be forced to give up their freedom, dignity, or sacrifice their health when they go to work.

In many ways, monitoring acts as an electronic whip that drives the fast pace of today's workplace in the growing service industry. Monitored employees, whether in telephone conversations with the public or in producing work with computers, must carry out repetitive duties that require rigorous attention to detail, executed under the stress of constant supervision and the demand for faster output. Unrestrained surveillance of workers has turned many modern offices into electronic sweatshops.

The stress that these employees experience should not be overlooked. Workplace stress costs this country an estimated $50 billion per year. This is a cost we cannot afford.

In addition, the consumer shouldn't be forced to give up freedoms when calling a company or when being called by an organization. Countless consumers are not aware that the calls they think are private, are secretly listened to by an intruder.

Consumers are deprived of the right to make fundamental choices about what sensitive information they are willing to divulge. For example, a caller could be discussing an insurance claim for a sensitive medical condition, such as a case of AIDS. While the AIDS victim is on the line, he does not know that the claims specialist's supervisor is secretly monitoring the call.

It is a sad irony that while the Federal Bureau of Investigation is required by law to obtain a court order to wiretap a conversation, even in cases of national security, employers are permitted to spy at will on their employees and the public.

In addition, current monitoring practices operate as a form of de facto discrimination. Women are disproportionately employed in the types of jobs that are subject to monitoring, such as clerical workers, telephone operators, and customer service representatives. Indeed, we will hear from two witnesses today who represent women working in these fields.

The legislation I introduced is a step in the right direction toward protecting fundamental privacy rights.

I look forward to the testimony of all the witnesses, and extend a special welcome to Vincent Ruffolo from the great city of Chicago, and Renee Maurel, who was born and raised in Illinois.

Our first panel includes Renee Maurel, a reservationist with Northwest Airlines; Carol Scott, a consumer representative of New Jersey Central Power and Light, and Cindia Cameron, a field organizer with 9to5, National Working Women's Organization.

If the three of you will take your places at the witness table, we will follow the 5-minute rule and will enter formal statements in the record. If you wish to read your statements, you may, but we will cut you off at 5 minutes and then move into questioning.

Let me add that we have a number of meetings going on, and I know that some of my colleagues in the Senate are very interested in this legislation, and in the House there are a number of Congressmen. Representative Pat Williams has introduced companion legislation, and my understanding is with over 100 sponsors.

We'll start with Cindia Cameron, if we may.

STATEMENTS OF CINDIA CAMERON, FIELD ORGANIZER, 9TO5, NATIONAL WORKING WOMEN'S ORGANIZATION, ATLANTA, GA; CAROL SCOTT, CONSUMER REPRESENTATIVE, NEW JERSEY CENTRAL POWER AND LIGHT, ASBURY PARK, NJ; AND RENEE MAUREL, RESERVATIONIST, NORTHWEST AIRLINES, SEATTLE, WA

Ms. CAMERON. Thank you.

My name is Cindia Cameron. I am with 9to5, National Association of Working Women. Carol and Renee, who are with me today, are two of the hundreds of individuals who have called 9to5, looking for help to protect their dignity and privacy in monitored workplaces.

What I would like to do is share some of the experiences of many of those others who could not be here today and describe how the bill you have drafted would protect millions of American workers from abuses of electronic monitoring.

First, the notification of monitoring. The requirement that employers provide written notification of monitoring systems and visual or oral signals of telephone surveillance would prevent some of the worst abuses and invasions of privacy.

Imagine how you would feel if the way that you found out your employer had monitoring in the workplace was if a coworker told you that your boss had routinely been listening in on your conversations with your boyfriend. That's what happened to Sherry, a top-rated collections agent in Atlanta.

Loretta found out that her manager had the ability to listen in to phone calls when she was fired, because he had listened in on a phone conversation where she was setting up an interview for another job. Her manager went a step further—since he had heard the name of the company that she was calling, he called their office and lied about her work performance.

But it is not just isolated unethical bosses who snoop in at the electronic keyhole that we are worried about. Computer journals now advertise software for bosses to "look in on Sue's computer screen. You monitor her for a while; in fact, she doesn't even know that you are there."

Or, how about the "peek and spy" software, which allows you to look in on someone else's screen. If you let the person know you are there, you are "peeking;" if you access their work secretly, of course, you are "spying."

The second point is access to records. The section of this bill which would provide an employee access to data collected about their work would allow them to challenge unfair discipline and provide some basis for due process protection.

Becky, who works for an insurance company, told us that employees access the computer with an i.d. number when they log in. After Becky had filed a sex discrimination suit against her employer, her i.d. number was routinely assigned to temporary workers, who were often and almost always slower than experienced staff. When she complained about this procedure and asked to see her files and the statistics kept on her, the company refused. Then, after 5 years of above average evaluations, Becky was fired.

Lack of privacy is at the heart of many complaints that we hear about computer monitoring. The portion of this bill that would require that data collected about employees be relevant to job performance is extremely important.

Electronic monitoring goes beyond simply collecting data by computer about employee performance. Technology now allows employers to cross the line from monitoring the work to monitoring the worker.

Sandra, for example, works for an express mail company. Her employer not only counts the number and length of calls she handles, but also the length and frequency of her trips to the bathroom. She was called into her supervisor's office recently, and he explained to her that four trips to the bathroom per day was exces-

sive; she obviously had a medical problem, and he would like for her to see a doctor.

Several large railroad companies based in St. Louis use a system that records the location and length of time that employees spend in each area of the building. Workers flash their i.d. cards across an electronic sensor, and a computer records whether they were in the restroom, the pay phone area, the smoking lounge, or at a friend's work station. Employees have been disciplined based on these figures, which are totally irrelevant to the job performance.

The next area is disclosure limitations. Having a computer count your every move, your every keystroke and phone conversation is very difficult and stressful, but some employers go further and publicly post employees' work results. In a survey of 700 employees at 49 companies, carried out by the Massachusetts Coalition on New Office Technology, 23 percent of those surveyed said that their individual statistics were posted publicly. The result here is humiliation for many employees and unnecessary, unproductive distrust and competition.

Finally, the use of monitoring data. Most of us have had the experience of someone standing over our shoulder while we work. It is usually not when we give our best performance. But with electronic monitoring, the supervisor is in the machine, watching and counting every minute and every movement. This supervisor does not take into account that everyone can have a bad day, a slow start, or a tough afternoon.

The provision of your bill that monitoring data may not be used is the sole basis for evaluation will prevent a ruthless human supervisor from hiding behind the myth of the neutral, objective computer as a way of harassing workers.

Just last week Jean, a reservationist at TWA, told of handling a difficult customer, then getting off the line and cursing under her breath. No one heard the comment by Jean and her supervisor, who picked it up through a headset monitoring device. Jean was called into the office, berated for unprofessional conduct, and required to sign a letter which went into her file, documenting the incident.

But it is not just workers who suffer the effects of abuse computer monitoring. Ask yourself whether as a consumer you are comfortable with the fact that when you call an insurance company to discuss your personal medical records or an airline to ask for an emergency rate to visit a relative dying of AIDS, there may be several people listening in on their line. Ask your husband, your wife or your best friend if their employer uses electronic monitoring before you call them on their lunch hour at work to make a hot date or discuss your legal or financial matters.

Most enlightened employers will say that when electronic monitoring becomes abusive, it should be left to labor-management relations. The idea that people without unions—which most women who are monitored are—can do that on their own is completely unrealistic.

Thank you.

[The prepared statement of Ms. Cameron follows:]

PREPARED STATEMENT OF CINDIA CAMERON

Thank you for this opportunity to present testimony on behalf of 9to5, National Association of Working Women, in support of S. 516, the Privacy for Workers and Consumers Act. Our testimony is based on extensive research as well as personal accounts from hundreds of men and women across the country.

In response to calls from our members about increasing problems with computer monitoring, 9to5 opened a hotline in January of 1989 to collect stories of workplace monitoring. The results were published in a report entitled *Stories of Mistrust and Manipulation: The Electronic Monitoring of the American Workforce.*

Carol Scott and Renee Maurel, who have testified today, are two individuals who called 9to5, looking for help to protect their dignity and privacy in electronically monitored jobs. I will share the experiences of others who could not be here in person, and describe how this bill will protect the estimated 25 million workers who are monitoring on at work, and the approximately 10 million whose job evaluations are based on computer-generate results.

NOTIFICATION OF MONITORING METHODS

The requirement that employers provide written notification of monitoring systems and visual or aural signals of telephone surveillance will provide urgently needed protections from some of the most serious invasions of privacy.

Imagine how you would feel if the way you found out about your employer's monitoring practices was by having a co-worker tell you that your boss had been making a habit of listening in to your private conversations with a boyfriend. This is what happened to Sherry, a top-rated collections agent in Atlanta.

Loretta found out that her manager had the capability to listen in on telephone calls, when she was fired after he overheard her making an appointment to interview for another job. Since he had overheard the name of her perspective employer, he went a step further, calling the company and giving false information about her work record.

It is not just isolated, unethical bosses who snoop at the electronic keyhole that we are concerned about. Computer journals advertise software which allows a boss to "look in on Sue's computer screen. You monitor her for awhile, in fact, Sue doesn't even know you are there." A software program called "Peek and Spy" allows you to look in on someone else's screen. When you let the person know you are looking, you are "peeking;" when you access their work secretly of course, you are "spying."

ACCESS TO RECORDS

The section of this bill providing an employee access to data collected about their work, will allow them to challenge unfair disciplinary actions, and provide some for due process protection.

Susan, an airlines reservationist, who became involved in a union organizing drive, says that a computer was used to fire her. According to her account, her good results (called "runs") were deleted from her file, and other agents' poor statistics were added. After many years of outstanding performance, she was told her numbers were too low, and she was dismissed.

Becky, who worked for an insurance company, explained that at her office each employee uses a computer ID number to log into the system. After Becky filed a sex discrimination complaint against her employer, she found out that her ID number was routinely assigned to temporary replacement workers, who were always slower than experienced staff. When she complained about this procedure and asked to see her file and statistics, the company refused. Becky has since been fired, despite more than five years of above average evaluations.

PRIVACY PROTECTIONS

Lack of privacy is at the heart of many complaints about the new electronic workplace. Maxine, a customer service representative who quit her job as a result of a serious stress-related illness, described her feelings, and those of dozens of hotline callers this way:

"Monitoring makes you feel like less than a child, less than a thinking human being. It's a shame because they have a lot of intelligent people there. You have to stop and think that your ancestors did not cross the ocean in steerage and come through Ellis Island to be treated like this."

RELEVANCY TO WORK PERFORMANCE

Electronic monitoring now goes beyond simply using computers to collect data on employee performance. In many cases, the technology allows an employer to cross a line from monitoring work, to monitoring the worker. The provision of this bill requiring that personal data collected be relevant to job performance is key to reestablishing a degree of dignity and privacy for large numbers of workers.

Sandra works for an express mail company. Her employer collects data not only about the number and length of calls she handles, but also on the length and frequency of trips to the restroom. She was recently told by her supervisor that four trips to the bathroom per day was excessive that she obviously had a medical problem and needed to see a doctor.

Several large railroad companies in St. Louis use a system which records the location and length of time employees spend in any part of the building. Workers flash their ID cards through an electronic sensor in each doorway. A computer tracks how long the employee spent in the restroom, the payphone area, the smoking lounge or in at friend's work station. Employees have been disciplined based on these figures.

Kevin was a recruiter for an employment agency, which used a telephone call accounting system to track each outgoing phone call. Kevin's wife worked for the company, and they often consulted about work-related matters. Kevin's supervisor, using the daily telephone printout, regularly questioned Kevin about the number of calls made to his wife. Despite Kevin's protests that the calls were work-related, and actually improved his performance, the harassment continued. Kevin quit in frustration.

DISCLOSURE LIMITATIONS

Having a computer count your every move, every keystroke and phone call is difficult and stressful. But some employers go beyond the counting and tracking to public posting of employees1work results.

In a survey of 700 employees at 49 companies carried out by the Massachusetts Coalition on New Office Technology, 23 percent of respondents said their individual statistics were posted publicly. Hotline callers report seeing their work records posted in the workplace with large red circles around certain statistics and written comments from the supervisor. The result is humiliation for the employee, and unnecessary, unproductive distrust and competition for high averages.

USE OF MONITORING DATA

Most of us have had the experience of someone standing over our shoulder while we work. This is not usually when we give our best performance. With electronic monitoring, the supervisor is in the machine; watching and counting every minute. This supervisor does not take into account that anyone can have a bad day, a slow start, or a difficult afternoon. The provision of this bill that monitoring data may not be used as the sole basis for evaluation, will prevent ruthless human supervisors from hiding behind the myth of the "neutral, objective computer" as a way of harassing workers.

LIMITS ON DATA USED FOR EVALUATION

Just last week Jean, a reservationist at TWA, told of handling a difficult caller and getting off the line; then cursing under her breath, as many stressed-out agents do. No one heard the comment, but Jean—and her supervisor—who picked it up through her headset monitoring device. Jean was called into the office, berated for unprofessional conduct, and required to sign a letter documenting the incident which went into her personal file.

Another reservationist told us, "One day I had a cold and had to make myself unavailable between calls to cough and blow my nose. I was monitored that day and got a very bad work report."

Luckily that agent was not targeted for dismissal. Al, a reservationist in Miami, found out from a friend in management that the company monitored him constantly for six months, trying to find an incident with which to fire him. All they found was one 10-minute trip to the restroom.

LIMITS ON DATA USED FOR PRODUCTION QUOTAS

A major theme of complaints by monitored workers is that trying to meet numerical figures, over which they have no control and no input, sets up a conflict between giving quality service and "keeping the time down." In the Massachusetts survey mentioned earlier, 65 percent of respondents said they could not do a quality job because they had to work too fast.

I have attached a copy of a "timer," or computer generated work report, from airline reservation agent to illustrate the tyranny of computer monitoring. As you will see, these agents receive scores on five different statistics per day; the number of calls handled, average time per call, average time between calls, "unmanned time" (usually meaning trips to the bathroom), and overall average. Agents are expected to take 150–200 calls per day, with a 96 percent success rating. They may be disciplined for any of the following: Calls longer than three and one half minutes, more than 12 minutes per day of "unmanned time," or too long between calls. This agent was put on warning for spending a total 23 seconds—over a full eight hour shift—between calls.

Sylvia, a data entry operator in Maryland, desperately needs protection from the use of computer generated results as the sole basis for setting of work quotas. Her pay and evaluations are based on meeting the minimum requirement of 11,000 keystrokes per hour. Although she punches in and out of her worksite, she is paid only for the time logged on the computer. If, for example, she needs to go to the bathroom, she faces a quandary. If she turns her machine off, she is not paid for the time away from her desk. If she leaves her machine on, her keystrokes per hour will decline; she will get a lower rating and face a pay decrease.

CONCLUSION

It is not just workers who suffer the effects of abusive computer monitoring. Each of us has likely had the experience of being cut off mid-sentence by a telephone operator whose goal seems to be simply to get us off the line as fast as possible.

Ask yourself whether, as a consumer, you are comfortable with the fact that when you call your insurance company to discuss your personal medical records, or ask an airlines agent for emergency rates to visit a relative dying AIDS, there may be several people listening in on your conversation. You might also ask your wife, husband or best friend if their employer uses telephone monitoring, before you call them on their lunch hour at work to make a hot date, or discuss your legal or financial affairs.

The most enlightened employers will say that where monitoring becomes abusive, it should be left to labor-management relations, to solve the problem, that government regulations are an unnecessary intrusion. I leave it to you to tell Sylvia, Jean or Loretta, that government need not intrude on their behalf, that they should negotiate on their own behalf with management. The truth is that the vast majority of monitored workers do not have unions; and without that protection and collective voice in the workplace, the idea of labor-management negotiation is completely unrealistic.

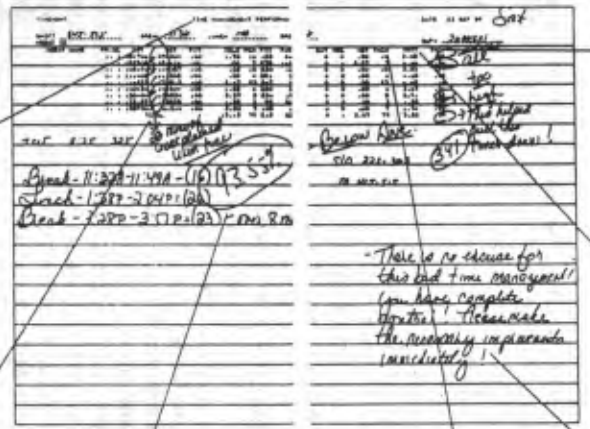
Workers, consumers, and citizens and all suffer from the increasing encroachment of electronic surveillance in the modern workplace. As Americans we believe strongly in the right to privacy. With this bill you have an opportunity to prevent serious erosions of this right in the workplace. I urge you to take the opportunity.

Thank you.

CRACKING THE ELECTRONIC WHIP

Meet the new boss: Computeri evaluation, *by Sharon Danann*

America's is a postindustrial service economy, runs the conventional wisdom—an economy wherein the product is information and work occurs in a clean, well-lighted place. It's the age of the telemarketer, the customer-service rep, and the flight reservationist—all of whom rely on computer technology to do their jobs. Abuse of workers in this new economy would seem unlikely, but it's here, with age-old cruelty. Twenty-six million employees nationwide, from telephone operators to elevator mechanics, have their work tracked electronically. For ten million of these men and women, computer-generated statistical evaluations, such as the one shown here, are used to judge job performance and, it is held, to increase productivity. But the computer can't measure the physical and mental toll exacted by the stress of second-by-second surveillance. This printout evaluation records the day's work of one of the 350 airline reservationists huddled over computer terminals in the vast 100-by-100-foot reservations center at TWA's Chicago office. (To protect her $5.67-an-hour job, the agent's name has been removed.) To judge from the supervisor's handwritten comments, the agent has had a bad day.



The supervisor has checked the gaps between SOT (sign-out time) and SIT (sign-in time). These gaps are known as UNM time, for unmanned time, a singularly inappropriate term. Most agents are women. "Unexplained" UNM time is almost always time spent in the bathroom. In this case, the reservationist's UNM time was unacceptably high because of an absence from 11:00 to 11:14—although we can all recall bathroom circumstances that required fourteen minutes or more, not to mention telephone calls to children sick at home. If the employee gets an urgent call from a babysitter or sick child, the message is relayed not to the employee but to the supervisor. To return urgent personal calls, employees must leave their work stations, thereby accruing UNM time, for even the most distraught mother dare not call home from her work phone, since the monitoring supervisor can listen to her call.

The supervisor has computed a "percent utilization" of 93.55 percent—an overall measure combining all the categories. It sounds like an exemplary level of productivity. But at this airline, rates below 96.5 percent trigger a series of disciplinary steps, such as a verbal or written warning ("a letter in your file") or even unpaid suspension if the number stays the same or falls lower in subsequent evaluations.

TNCH is the total number of calls handled. Between her morning break and lunch, this agent took twenty-three calls for information or reservations, and a total of seventy-nine for the day. That sounds impressive, but it's considered low by management, which expects agents to handle 150 to 200 calls a day. The reservationist will be pressured daily to raise this number. Raw totals, and not customer needs, are what management is concerned with.

The TACW, or total average after-call work—the paperwork for the tickets—has gotten this agent into extra trouble. Here she is being reprimanded for taking .39 minutes—about twenty-three seconds—to complete her paperwork for each call. The agent is damned if she does and damned if she doesn't; putting the customer on hold or engaging the customer in conversation in order to do paperwork will result in a higher TATT and can be observed by the eavesdropping supervisors.

TATT, or total average talk time, was three and a half minutes over the course of the day. The length of each call is closely scrutinized. Think about this the next time you ask for three comparison fares or provide the detailed information required to send an unaccompanied small child to see grandparents. Reservationists cannot try to save time on customer calls by dropping an unnecessary sales pitch without risking additional discipline. Supervisors, who randomly listen in on calls from a glass monitoring booth in the center of the reservations room, judge the calls strictly. If the supervisor challenges a particular call at the end of the day, the agent may be hard-pressed to remember it specifically. And she dare not commiserate with fellow workers—the supervisors can hear that, too.

On television commercials, airline reservationists and their equivalents in other jobs are smiling, friendly, and boundlessly gratified by serving you. In reality, the agent has nothing approaching "complete control." The control lies with management and the ensuing threat is not an idle one. If the agent continues to have days like this, with problems in any of the monitored categories, she will be fired. And if that happens, she will be forced to look for another job in the electronic mills of the new economy.

Sharon Danann is the former research director of 9to5, Working Women Education Fund, and author of the report "Stories of Mistrust and Manipulation: The Electronic Monitoring of the American Workforce."

Senator SIMON. Thank you very, very much.

Carol Scott.

Ms. SCOTT. My name is Carol Scott, and I am a customer service representative for JCP&L, an electric utility in New Jersey. My job is answering the 800 number for our company.

I was working on a holiday last February, and at some point during that day my supervisor approached me and asked me to come into his office, which of course, I did. He made mention to the fact that I received a couple of transferred phone calls, and I told him that those calls were customers calling back.

He then made a snide comment about the relationship that I must have with our customers because he heard one of them call me "babe." I asked him how he knew that, and he admitted that he had been listening in on my conversations. I then informed him that the call he listened in on was from a coworker and not one of the transferred calls in question.

Needless to say, I got very angry; we had a bit of an argument, and the incident ended there because I just simply walked away.

On a personal level, when that happened to me, I felt like I had just caught someone peeping in my bedroom window. My professional self then kicked in, and I felt totally disgusted. I was angry because the company was telling me, in essence, that they cannot trust what I say nor rely on my character to perform my job.

I filed a grievance, and at that time it became a labor issue.

Corporate's reasoning for this type of management is the need to know how their employees are doing and also the overall customer satisfaction.

Each month my company sends a survey-type letter to random customers who had recently contacted our customer service center. These surveys are computed, and we are given a rating each month. This is actual customer response on a monthly basis. Our customer satisfaction percentage is approximately 93 percent.

During a labor-management meeting, there was discussion regarding the fact that our customer service center received approximately 700,000 calls yearly, that there were approximately 20 customer complaints for the year, and out of those 20 complaints the representative was upheld approximately 85 percent of the time.

Add to all that the fact that all of our calls are recorded. Personally, I find it hard to accept the fact that the company needs all this information. I work with approximately 70 customer service reps whose average time on the job is 11 years and who have been at the top of their job level for at least 5 years.

Four supervisors each took 2-hour shifts every day just to listen to us. This has gone on for approximately 4 years. With all this monitoring going on, you would think that something positive would come out of all this. The truth is, it never did.

No one ever paid attention to the different aspects of the job that we could have been weak in, such as a more informed explanation of what degree-days are, or even a brush-up on how much usage is involved in central air conditioning.

Not even once did a supervisor come out and acknowledge a tough call, job well-done by one of the reps.

I am fortunate in the fact that I have a union to pursue this, and I also have the good fortune to have a corporate vice president with

high ethical standards. This combination enabled us to reach an agreement on this issue. My question to you is this: In the absence of these two very important factors, what is the American worker to do?

I have seriously wondered if the real reason for this type of management isn't to create and maintain feelings of inadequacy. It seems that big brother is seeping into our work force. Eighteen years ago this country was outraged when it was discovered that Richard Nixon was taping Oval Office conversations. The country was mortified, and the people were indignant. Yet, here I sit in a meeting of the U.S. Senate and have to argue for freedom, for privacy, and for the dignity of the American worker.

It makes me very sad to be here.

Senator SIMON. Thank you very much for your testimony.

Renee Maurel—and let me add Senator Adams from Washington hoped to be here to personally introduce you and welcome you, but unfortunately he is tied up in another meeting.

Ms. MAUREL. Thank you. Good afternoon.

My name is Renee Maurel, and I work for Northwest Airlines as a reservation sales agent, and I have been monitored in one form or another every working day for the last 27 years.

When I was hired by Northwest Airlines in 1964, I was told I would be monitored as part of my job. In the 1960's, there were no computers to do the monitoring; there was just a supervisor in a back room with a tape recorder. The telephone system, even though primitive, had a way to count the number of phone calls taken. I knew right from the beginning that I was being listened to and counted.

In time, with the advent of computers and the invention of monitoring equipment, monitoring became the job. How long I was on a phone call, how long between phone calls, how many minutes I was on a break or at my desk became the focus.

Not wanting to be the robot I was becoming, I had to create an alter ego—another person who did the work, did what the company demanded, sat there on the assembly line.

The company, delighted that we could be tracked so completely, took the monitoring capabilities to the most negative limit. I was disciplined or harassed on several occasions for nonbusiness-related conversations that took place between business calls. I was written up every time I was 2 or more minutes late from a break.

I have always felt that there was someone else in my headset, someone in my keyboard, waiting to punish me for the smallest infraction.

Stress and tension brought physical problems—eye, ear and neck strain among the most persistent. Because the statistics were so important, that is exactly what I passed along to the customers. I would unnecessarily keep them on the phone so I could finish my typing. I would cut them short if they became too chatty. I looked forward only to my 50 minutes of break time, and then worried that I might be late getting back to my desk.

Emphasis on statistics made me play games, try to outwit the monitoring devices. None of this did much to help the customer who, of course, was being monitored also. Speed counted as well as quality. The customer became a statistic.

At the 25-year mark, even my alter ego couldn't take it anymore. A quarter century of being monitored had taken its toll. I got to the point where I couldn't do my job effectively in any respect, and I thought of starting over somewhere else.

In an amazing turn of events at the exact same time, Northwest Airlines was purchased by a private company, Wings Holdings, Incorporated. One of the first things that the new management said to us was that in a customer service industry, employees are the most important asset. We could look forward to major changes in how the airline would be run.

In the 2 years since, almost everything in my work world has changed. In respect to monitoring, two very great changes have occurred. All reservation agents were given a survey to complete. We could say anything we wanted to say about our feelings on monitoring, and we did this anonymously. When the results were in, Northwest announced a self-monitoring program.

I am now advised in writing on the day I am taped. When called into the supervisor's office, we listen to the tape together, and we only listen to two potential sales calls. The new program is called "sales coaching" and is used to determine my selling technique—if I am truly selling the product. There is no grade, no judgment. And what an incredible new perspective—to do my work as an important, respected, knowledgeable, professional salesperson, no longer fearing and shrinking from the invisible listener.

I do my job in a happy, caring manner, no longer worrying how long it takes to satisfy a customer's needs.

The second change has been in the area of computer-printed statistics. These are still culled hourly, but the focus has shifted from counting bathroom breaks to totalling revenue generated by me—how much actual money I have made for the company. This is a much more interesting statistic and one that challenges me to improve.

The legislation before this committee will probably not affect the way Northwest monitors employees. If all companies were run by enlightened management, we wouldn't need laws to protect the worker from ruthless employers. The fact is American workers do need protection, and this legislation would provide basic minimum protection.

Northwest management has allowed me to see the light at the end of the tunnel. However, there are many American workers who are monitored daily and don't even know there is a light to reach for. They need this bill to be passed; they need to be respected so that they may pass that respect along to their customers.

I have been on a treadmill. I have not enjoyed it. I feel I was brainwashed and conditioned. Monitoring is intrusive, abusive, and can be debilitating depending on who has the information and how it is used. Even though things are changing for the better in my workplace, it will be a long time, if ever, before I will feel deprogrammed.

I certainly understand the need for statistics—how else can you run a company? But it can be terrible, and it doesn't have to be. It is common sense to respect the worker. We should have the right to know the specifics of our performance. The chain of respect con-

tinues to the customer, which makes for great service, satisfied callers, more business and larger profits, which is the bottom line.

The new monitoring system at Northwest Airlines is in its infancy, and I am looking forward to the many changes to come. There are others in this country who need to have some hope for their future. This bill is the answer.

Senator SIMON. Thank you very much.

The attitude that you express, is that shared by others?

Ms. MAUREL. It is brand new. It is happening. It is going to take a long time to evolve, but we all do see that things are changing and that maybe it's going to be a little bit better for us. The people who are told every day when it is their turn to be monitored do have that feeling, that part of it. I don't know if they can see the whole scope yet, but it is improving.

Senator SIMON. But the feeling of being uptight—if I may generalize—have other employees shared that same kind of feeling with you?

Ms. MAUREL. Oh, absolutely. There are also some that it doesn't bother at all; there is that type of person. But the ones who don't enjoy it express it, yes.

Senator SIMON. Ms. Cameron mentioned that the lack of privacy has a tie-in with job performance. Do you want to expand on that at all, Ms. Cameron, and I'd be interested, Ms. Scott and Ms. Maurel, if you want to comment on that as well.

Ms. CAMERON. I can talk from people who call us who say that there is this dynamic set up—as Renee said, if they are focused on meeting these numerical goals, and they know that someone else is listening besides them, it gives people a real hard time in conveying to the customer complete knowledge of what they are talking about and efficiency in doing their job. People are focused on getting that person off the line and going on to the next one.

People have told me about having their supervisors come in on the line while they are talking to someone and say, "Excuse me, that's not quite right. How about explaining it this way"—which I would think is a whole lot more disorienting to the consumer than the potential of having a "beep" on the line which lets them know that someone else may be listening.

Senator SIMON. And why do people call you?

Ms. CAMERON. People call us a lot because they are feeling extreme stress and extreme pressure. They want an outlet. They want to know if there is something that can be done.

The woman from the express mail company called and was crying when she said, "Is this normal? Am I over-reacting to the fact that my boss called me in and talked to me about do I have a medical problem?" A lot of people are just very frustrated, and they don't know where to turn. They feel like are they crazy, or is the company crazy.

Senator SIMON. And are these just isolated phone calls that you get, or is this pervasive?

Ms. CAMERON. We get hundreds of phone calls from a very wide variety of companies. Most of the complaints that people have are feeling that their dignity is being taken away. People will say, "I am a thinking adult. I had to pass a lot of tests to get this job. Why

do I get more grades in a week than my children at school get in a whole year? Why am I being treated this way?"

So it is both the dignity and the extreme stress. Renee mentioned the stress on her job. A lot of people who call us have stress-related diseases. They are on disability when they call us. It is when they get away from the job—they are on medical disability, and they call us and say, "I am not sure I can go back."

Senator SIMON. Ms. Scott, you talked about supervisors taking 2 hours a day to go through this. Do you feel that adds to the productivity of New Jersey Central Power and Light?

Ms. SCOTT. No. Totally from the workers' standpoint, I think it is very debilitating to them. You don't feel that you are being monitored in order to possibly help you do your job better. You get the feeling that you are being policed and that they are listening to you not to somewhere down the line help you with your job, either give you more training, brush up on something you may be a little weak in, but they are just trying to catch you talking to someone that you're not supposed to be talking to.

We had an incident where the phones were very quiet one afternoon, and one of the customer service reps in one aisle called a rep in another aisle just to say, "I'm a little bored right now." One of the reps was being monitored, and the supervisor came out and scolded her like a little kid who had just walked through a mud puddle. So it is not very respectful as far as I am concerned.

Senator SIMON. And Ms. Maurel said it would be interesting to have the bottom line, how much you bring in in income for, in this case, Northwest Airlines. It is more than interesting. That's a pretty basic statistic. But the example I cited of Canada Bell, where they don't say "We are going to monitor Ms. Cameron, Ms. Scott, and Ms. Maurel," but they take the overall office and compare it with other offices, and then they come and say—I assume come to some office and say "You can do a little better in this office"—that's a very different thing from the kind of private monitoring you are talking about, isn't it?

Ms. SCOTT. I think the capability to monitor—and I don't think any of us here today are against being monitored on the job; honestly, I don't know that I see the total need of it, but it is a new world, it is changing technology, and maybe it can be of some service to us—but I think what we're seeing is the way that it is actually used in reality on the job, and it is not being used in any positive manner.

Senator SIMON. We have been joined by Senator Metzenbaum.

Senator METZENBAUM. I am just here to listen, thank you. I may have some questions for Mr. Bahr when he testifies, but I just want to show that I am interested in the subject, and I left the Gates hearing to be with you.

Senator SIMON. We have just heard from three people who are telling what kind of problems we face. And again I would stress—and Ms. Scott, you mentioned you are not opposed to all monitoring—our bill doesn't knock out all monitoring. It simply puts some sensible restrictions there so that I think we can create a better labor-management climate, and I think we can create a climate that is more productive, as some companies are finding out—Northwest Airlines will benefit by their changes, I am reasonably

confident, just as Canada Bell has, and our friends in Japan apparently feel that their procedure is a much better procedure.

We thank all three of you very, very much for being here and testifying.

Our next witnesses are Morton Bahr, who is no stranger to this room, the president of the Communication Workers of America. We are happy to welcome him back once again. We welcome also Dr. Gary T. Marx, a sociology professor at Massachusetts Institute of Technology and Mark Rotenberg, the Washington director of Computer Professionals for Social Responsibility.

We are very pleased to have you here. Morton Bahr, you have another friend to your right who is also a long-time friend of this committee, and you may wish to identify him for the record.

Mr. BAHR. Lou Gerber, Senator, our legislative representative.

Senator SIMON. We'd be happy to hear from you at this time.

STATEMENTS OF MORTON BAHR, PRESIDENT, COMMUNICATION WORKERS OF AMERICA, WASHINGTON, DC, ACCOMPANIED BY LOU GERBER, LEGISLATIVE REPRESENTATIVE; GARY T. MARX, SOCIOLOGY PROFESSOR, MASSACHUSETTS INSTITUTE OF TECHNOLOGY, CAMBRIDGE, MA; AND MARC ROTENBERG, WASHINGTON DIRECTOR, COMPUTER PROFESSIONALS FOR SOCIAL RESPONSIBILITY, WASHINGTON, DC

Mr. BAHR. Thank you very much, Mr. Chairman, Senator Metzenbaum.

We do appreciate the opportunity to testify in support of legislation that would prevent secret electronic monitoring in the workplace.

In 1890, U.S. Supreme Court Justice Louis Brandeis referred to the right of privacy as "the right to be left alone, the most comprehensive of rights, the right most valued by civilized men."

But a century later, more than 10 million workers are subject to concealed electronic surveillance each work day at job sites across the Nation. Companies spy on as many as 400 million telephone calls a year between workers and the public. Managers covertly count the number of keystrokes workers produce every minute on video display terminals. Employers photograph wage earners who are honorably going about their jobs.

These misguided supervisory methods render privacy rights obsolete. Most disturbing, businesses are expanding the practice of monitoring their employees. The number of such surveillance systems sold to companies soared by nearly 200 percent between 1985 and 1988, and sales continued to rise.

To illustrate how secret electronic monitoring is running roughshod over the privacy rights of workers, I call your attention to 6 cases cited in the statement we have submitted for the permanent record.

This insidious practice not only tramples upon civil liberties, but also is taking a devastating toll on the occupational safety and health of workers.

Just 1 year ago, CWA and the University of Wisconsin announced the results of the first major study conducted in the United States to investigate a possible relationship between elec-

tronic monitoring and workers' negative health symptoms. This landmark research project revealed that telecommunications industry employees who were monitored suffered significantly higher levels of psychological and physical problems than the workers in the same industry who were not monitored.

One of the most alarming findings of the study was that 51 percent of monitored workers—and we are talking about secret monitoring—declared they were plagued by stiff or sore wrists, a rate 112½ percent higher than cited by nonmonitored workers.

Mr. Chairman, a serious problem with computer monitoring is that it puts a premium on measuring a worker's performance through arbitrary, quantitative standards, while it ignores the value of qualitative human judgments.

Computer monitoring can smother the ability of a worker to assist customers who have complex inquiries or to solve challenging problems.

To demonstrate the distorted priorities that emphasis on mindless quantitative standards can engender, I have included in my written testimony an account from a CWA member of an instance in which a telephone company manager willfully disconnected a call from a person who had dialed the company and was telling an operator he was considering committing suicide. After a conversation of about 15 minutes between the would-be suicide and the operator, a telephone company manager intentionally terminated the call because, as the manager claimed, the length of the call was ruining the average work time—as the AWTU suggested in *Bell of Canada*—on all customer calls of the operators under that manager's supervision as measured by the company's computer.

Telephone company operators are expected to complete calls from the public in about 20 seconds. In this case, the manager decided that conforming to the inanimate quantitative standard dictated by the computer was more important than saving the life of the would-be suicide caller.

Mr. Chairman, employers claim that they need to use secret monitoring to ensure quality service. But evidence demonstrates that the absence of monitoring may actually improve service. Ten years ago, legislation prohibiting secret telephone monitoring was signed into law in West Virginia by then Governor Rockefeller. Subsequent to passage of the law, C&P of West Virginia was ranked first in America among Bell System companies in six of 12 customer satisfaction categories, according to the company's official publication.

As you stated in your opening remarks, Mr. Chairman, many countries restrict monitoring by law. Without engaging in secret surveillance of their work forces, Japan and Germany, for example, America's two chief competitors in the global marketplace, have achieved robust economies, attained trade surpluses and won the praise of American business leaders for quality and productivity.

Industrial relations experts also agree that secret monitoring is a misguided practice. Professor Charles Hecksher of the Harvard School of Business has stated—and I quote—"Monitoring is a tool for bad managers. It is a crutch that allows bad managers to get away with a style we know does not work. The best way to get ef-

fective work out of people is to tell them what needs to be done and then get out of their way and let them do it."

S. 516 would provide employees with the right to know when and under what conditions monitoring will take place. It would allow workers to earn their living without being subjected to the environment of an electronic sweatshop.

In a report on electronic surveillance and civil liberties, the Office of Technology Assessment observed: "In the last 20 years, there has been a virtual revolution in the technology relevant to electronic equipment. The law has not kept up with the technical changes."

Mr. Chairman, the Privacy for Consumers and Workers Act would make a major contribution to closing the gaps cited in the OTA study between the growing use of electronic equipment for employee surveillance and governmental supervision of its use. Most important, approval of the legislation would strengthen the right to privacy at a time when the expanding use of surveillance technologies of the workplace has endangered this most fundamental of American values.

Thank you.

[The prepared statement of Mr. Bahr follows:]

PREPARED STATEMENT OF MR. BAHR

Good afternoon, Mr. Chairman and members of the subcommittee. I appreciate the opportunity to testify in support of legislation that would prevent secret electronic monitoring in the workplace.

The Communications Workers of America represents more than 600,000 workers employed in the telecommunications industry, public sector and printing and allied trades.

In 1890, Supreme Court Justice Louis Brandeis referred to the right of privacy as "the right to be left alone, the most comprehensive of rights, the right most valued by civilized men."

But a century later, in 1991, more than 10 million American employees are subjected to concealed electronic surveillance each workday at jobsites across our nation. Each year, employers spy on as many as 400 million telephone calls between wage earners and the public. They covertly count the number of keystrokes workers produce every minute on video display terminals. They even stealthily photograph employees who are honorably doing their jobs at offices and plants.

These distorted supervisory methods render privacy rights obsolete.

Most disturbing, private employers are expanding the practice of monitoring their employees. The number of monitoring systems sold to businesses soared by nearly 200 percent between 1985 and 1988. Since that time, sales have continued to rise.

To illustrate the dangerous implications of secret electronic surveillance, consider these recent true labor relations cases:

—An airline reservationist spoke with a co-worker between calls on a matter that had no bearing on her capacity to perform her job duties. The reservationist was unaware that the headset she wore contained a hidden device which communicated her comments to a supervisor. She was punished. Did the company have a right to penalize her for her private conversation?

—Northern Telecom Ltd. bugged various telephones at its plant in Nashville, Tennessee, including a telephone located in the employee cafeteria which was used by employees to make personal phone calls outside the plant. Hours and hours of workers' conversations totally unrelated to the company's business operations were recorded. In addition, this telephone equipment manufacturing company used microphones hidden in the plant's overhead sprinkler system and light fixtures to listen in on discussions between its wage earners.

The illegal wiretapping and use of concealed microphones went on for years before it was discovered. Management is believed to have engaged in electronic eavesdropping of its workforce to create a "hit list" of union supporters and to thwart CWA's effort to organize the facility. Were the Constitutional rights of the employees fulfilled?

—A computer operator discovered several months after she was hired that a computer was being used to keep track of her workday activities, including time in the bathroom. Didn't she have a "right to know" when she was hired that her employer monitored the workforce in this way?
—A telephone operator was suspended for cutting off a customer. However, disciplinary action wasn't taken until two months after the incident had been noted by the manager who had been secretly listening in on her calls. She couldn't remember what happened on that day well enough to defend herself. Was her right to due process respected?
—A newspaper kept a secret record of every time the telephone number of the union that represented its workers was dialed and from what extension. Were the employees' free speech rights recognized and honored?
—Nurses in a hospital discovered that management had installed a concealed camera in their locker room. The camera was monitored by male security guards. Should the nurses have been kept in the dark about this "Peeping Tom" invasion of their privacy?

These cases demonstrate that management's use of secret electronic surveillance goes far beyond monitoring of the work. It trespasses outrageously upon the privacy rights of the worker.

THE EFFECT OF ELECTRONIC MONITORING ON WORKERS' HEALTH

Secret electronic monitoring is taking a devastating toll on the occupational safety and health of workers.

Eight months ago, CWA and the University of Wisconsin announced the results of the first major study conducted in the United States to investigate a possible relationship between electronic monitoring and workers' negative health symptoms. This landmark research project revealed that monitored workers suffer significantly higher levels of psychological and physical problems than do workers in the telecommunications industry who are not subjected to electronic monitoring.

Telephone industry employees who were monitored experienced greater stress, more depression, higher levels of anger and more severe fatigue than did non-monitored workers in the same industry. Monitored employees also reported more musculoskeletal problems than did non-monitored workers.

More specifically, 81 percent of telephone industry employees who were monitored complained of depression as against 69 percent of those who were not monitored. In addition, 79 percent of monitored employees revealed that they suffered severe fatigue or exhaustion versus 63 percent of telephone industry workers not subject to electronic surveillance. Also, 83 percent of monitored employees reported problems with high tension as against 67 percent of non-monitored employees.

With regard to physical health, fully 51 percent of monitored workers declared that they were plagued by stiff or sore wrists, a rate 112.5 percent higher than cited by non-monitored telephone workers. Similarly, 81 percent of monitored employees mentioned problems with neck pressure versus 60 percent of non-monitored employees.

Attached to this testimony is the study referred to above, entitled "Electronic Performance Monitoring and Job Stress in Telecommunications Jobs," which I request to have included in the permanent hearing record.

MONITORING DEGRADES WORKERS

Unscrupulous employers are using secret electronic monitoring to transform the workplace of the near-21st century into an Orwellian version of 19th century factory labor relations.

Just as manufacturers in industrial plants accelerate the pace on assembly lines, similarly employers of office workers use computers to compress the time allowed to complete tasks, pushing employees to work at top speed. As a result, unwinking computers have become surrogate supervisors in today's high tech workplace.

Adding insult to injury, some employers post conspicuously the daily time records of employees, showing not only how long it takes for each worker to carry out his or her duties but also the time used for bathroom breaks.

A graphic example of the way in which computers are used to control work routines inhumanly is seen in the telephone industry. A typical operator handles more than 1,100 calls in a 7½ hour shift. The operator is required to complete each call in about 20 seconds.

He or she has absolutely no control over when the next call will be routed to the operator. A central computer determines if the operator receives three calls in a row or 300.

Aggravating the situation, the operator never knows when someone may be listening in, how long the surveillance lasts, what information will be collected or how the results of the monitoring will be used.

As a result of unrestricted secret monitoring, millions of employees endure, each workday, the humiliating experience of being "handcuffed" for 7½ hours to an electronic supervisor.

The degrading effect of secret electronic monitoring is described eloquently by a telephone operator who has been victimized by this misguided employment practice. Her account of her work atmosphere is as follows:

> "In our office, they turn on a blue light . . . that is only supposed to be on when someone is monitoring, but most days it is turned on at 8 a.m. and stays on all day. We did have three supervisors that do nothing but monitor on us all day. We now have a new supervisor in our department, and they have put her on monitoring also.
>
> "I have been with (Bell company) 29 years. (This) is the worst department I have been in all my years with the company.
>
> "They use monitoring to see if they can find something to charge against you. I find it to be dehumanizing, demeaning, unhealthy and disgusting.
>
> "Through the years I have been appraised as more than satisfactory and respected to do work without constant supervision.
>
> "All in our department feel as though we are in prison and we are regarded as nothing more than criminals that must be guarded and monitored on constantly as though we could not function on our own. We are all adults, but we are made to feel like naughty children.
>
> "I loved my job I had before. Now all I long for is the day I can retire and never have to set foot back in that horrible place.
>
> "I know this is rather lengthy, but I had to express my feelings about monitoring."

Another telephone company employee who was subjected to secret monitoring characterized the intimidating atmosphere as follows:

> "When I walk into the office, I can smell the odor of worker fear and stress."

To illustrate the distorted priorities that management's emphasis on mindless quantitative standards can engender, I am including an account from a CWA member of an instance in which a telephone company manager willfully disconnected a call from a person who had dialed the company and was telling an operator the caller was considering committing suicide. The manager disconnected the call after about 15 minutes because the manager claimed that the length of the call was "ruining" the average work time (AWT) of the operators under the manager's supervision.

As mentioned earlier, telephone company operators are expected to complete calls from the public in about 20 seconds. Operators and their supervisors are then evaluated by higher management as to whether they have complied with this lifeless statistic.

The account of this case in which a telephone company manager decided that curtailing the length of the call was more important than saving the life of the would-be suicide follows:

> Dear CWA, the article I just read on monitoring in the workplace touched my heart. The memories of my TSPS operator job, and of my slight business-office job; are not good ones.
>
> I see you know all about the operators AWT's, but you don't know how important that number is to the managers. The AWT is their rating, they will do anything to improve it. What sticks in my mind year after year (since 1982) is the time my supervisor cut-off a life and death situation from my TSPS position. I was doing my best with a very sad person thinking of committing suicide. This was around the holiday season 4 or 5 years ago. My service-assistant at the beginning of the call was advised by me (I slipped her a note, not giving myself away to the would-be-suicide) of the phone number and nature of the call within the first few minutes. I did my best to reason and talk with this person, while I hoped my supervisor was doing her job by getting police to that person's location. About 15 minutes later, while I was still talking with this person, and making progress, one of the managers came over, who was alerted to this long call I was on, and just disconnected the call. I was stunned, then a collect caller pops in on my position. I sat there dumb-founded for a few seconds, thinking what this poor suicide person did next. To this day, I never found out. The man-

ager said, and I quote "You're ruining my work-time." There is no need for me to say anymore.

Feel free to call me anytime. The TSPS world is a jungle. The managers have no dignity. I know, I had dozens of them in my 4+ years as an operator. Thank God, I'm away from that.

Sincerely,

MONITORING AND SERVICE QUALITY

Along a related line, employers claim that they need to use secret monitoring to ensure quality service, but evidence demonstrates that the absence of monitoring may actually improve service.

Ten years ago, legislation prohibiting secret telephone monitoring was signed into law in West Virginia by then Governor Jay Rockefeller. Despite the absence of such surveillance, C. & P. of West Virginia was ranked first in America among Bell System companies in 6 of 12 "customer satisfaction" categories, according to the company's official journal, C&P Mountain Lines. A company vice president was quoted in the publication as stating proudly, "Customers told us we do an outstanding job."

Of special interest, the Bell System transferred some of its directory assistance operations from Washington, D.C., where monitoring was permissible, to West Virginia after monitoring there was outlawed.

The West Virginia law was subsequently overturned during the tenure of Governor Rockefeller's successor. This occurred in part because—at a time when West Virginia was experiencing a severe recession and its unemployment rate was among the highest in the nation—AT&T threatened not to locate a major manufacturing facility in that state unless the monitoring law was changed.

More recently, secret monitoring has been eliminated in several telephone company worksites without any reported diminution in quality of service. In such cases, the absence of monitoring reduced accompanying financial costs for supervisory personnel and monitoring equipment.

By contrast with the United States, where monitoring is unrestrained and on the increase, several European countries restrict monitoring by law. In fact, America's chief competitors in the global marketplace refrain from the use of secret electronic monitoring. Without concealed electronic surveillance of their workforces, Japan and Germany have achieved robust economies and trade surpluses.

America's corporate leaders praise the quality and productivity of firms in these technologically advanced nations. Similarly, government regulation of secret monitoring could help revitalize America's competitiveness in the international arena.

VIEWS OF EXPERTS ON SECRET MONITORING

Industrial relations experts agree that secret monitoring is a misguided practice.

Professor Charles Hecksher of the Harvard School of Business has stated with regard to the use of monitoring:

> "Monitoring is a tool for bad managers. It's a crutch that allows bad managers to get away with a style we know doesn't work. The best way to get effective work out of people is to tell them what needs to be done and then get out of their way and let them do it."

In addition, the majority of human resources managers, who administer employee relations programs for America's corporations, disapprove of secret electronic monitoring. According to a survey of nearly 2,000 of these professionals, 82.4 percent do not approve of listening in on employees' telephone conversations, while 17.6 percent would listen in on them. Similarly, the impressive figure of 61.3 percent do not sanction the use of secret video cameras to monitor employees, while 38.7 percent approve of such activity.

In 1987, the Office of Technology Assessment published a pathbreaking report on workplace monitoring entitled "The Electronic Supervisor: New Technology, New Tensions." With regard to secret electronic monitoring, the report found:

> ". . . its intensity and continuousness raise questions about privacy, fairness and quality of worklife."

LEGISLATIVE SOLUTION

More than two centuries ago—before our Founding Fathers took up arms to fight the American Revolution—invasion of privacy meant forced entry into private homes by British soldiers and mercenaries. The framers of the Constitution, our

most sacred body of law, did not foresee the onrush of technology that would foster the use of electronic eavesdropping devices more insidious than any enemy soldier they faced.

Today, protecting the citizens from such concealed surveillance is increasingly becoming one of the leading concerns of the Information Age.

To stop the invasion of privacy, erosion of dignity and expansion of stress-related illnesses caused by secret electronic monitoring, CWA advocates the enactment of the Privacy for Consumers and Workers Act, S. 516, introduced by Senator Paul Simon (Democrat, from Illinois).

This legislation would provide employees for the first time with the "right to know" when and under what conditions monitoring will take place. It would allow workers to earn their living without being subjected to the environment of an electronic sweatshop.

The Privacy for Consumers and Workers Act would help close the widening gap between the growing use of electronic equipment for employee surveillance and governmental supervision of its use. In a 1985 report on electronic surveillance and civil liberties, the Office of Technology Assessment observed:

> "In the last 20 years, there has been a virtual revolution in the technology relevant to electronic equipment. . . . the law has not kept up with the technical changes."

Most important, enactment of the legislation would strengthen the right to privacy at a time when the expanding use of surveillance technologies at the workplace has endangered this most fundamental of American values.

University of Wisconsin-Madison

Department of Industrial Engineering
1513 University Avenue
Madison, Wisconsin 53706
Telephone: 608/262-2686

Electronic Performance Monitoring and Job Stress in Telecommunications Jobs

Michael J. Smith
Pascale Sainfort
Katherine Rogers
David LeGrande

Released by the University of Wisconsin-Madison
Department of Industrial Engineering and
the Communications Workers of America

October 5, 1990

Executive Summary, October 5, 1990

CWA, University of Wisconsin announce results of major Occupational Stress Study.

Today, representatives of the Communications Workers of America and Dr. Michael Smith, Chair of the Industrial Engineering Department-University of Wisconsin announce the results of "The CWA National Occupational Stress Study." Initiated during Spring, 1989, the scientific investigation sought to identify health concerns among 2,900 randomly-selected telecommunications VDT workers.

The landmark study is the first major occupational stress study conducted within the U.S. telecommunications industry. Also, it is the first major study to investigate the relationship between electronic performance monitoring and related well-being and health symptoms.

It was determined that the study be national in scope to represent telecommunications jobs across the U.S. To achieve a national geographic distribution, an operating company from each of the seven regional "Baby Bells" was randomly selected to have its workers participate. Within each company, four hundred employees were randomly selected for participation: 100 Directory Assistance Operators, 100 Service Representatives and 200 Clerks. In addition, a random sample of 200 AT&T workers in select jobs was also selected.

A questionnaire survey was used to gather information from the selected workers. The survey form was based upon previous forms used to study job stress in office work developed at the National Institute for Occupational Safety and Health and the Department of Industrial Engineering - University of Wisconsin. The questionnaire examined job demands, job content, supervisory relations, career issues, work standards, electronic monitoring, psychological moods, and somatic health complaints.

A total of 2900 workers were eligible to participate. Surveys were received from 762 employees.

Findings

Several important findings have been identified in the study. For example, electronic performance monitoring is seen as a major cause/promoter of psychological and physical health complaints. Monitored workers reported more boredom, high tension, extreme anxiety, and depression, anger, and severe fatigue than non-monitored workers. Also, monitored workers reported more musculoskeletal problems (i.e., wrist, arm, shoulder, neck, and back problems) and headaches than non-monitored workers.

A Comparison of

Psychological and Physical Health Symptoms and Complaints

Among Monitored and Non-Monitored VDT Workers

(Percent Reporting a Complaint)

Symptoms/Complaints	Monitored	Non-Monitored
depression	81	69
high tension	83	67
extreme anxiety	72	57
severe fatigue or exhaustion	79	63
loss of feeling in fingers/wrists	43	27
stiff or sore wrists	51	24
pain or stiffness in arms/legs	68	55
pain or stiffness in shoulders	79	66
neck pain into shoulder, arm, hand	64	41
neck pressure	81	60
back pain	79	73

Electronic Performance Monitoring and Job Stress in Telecommunications Jobs

Michael J. Smith*
Pascale Sainfort*
Katherine Rogers*
David LeGrande**

Abstract

A questionnaire survey of employees of telecommunications companies representative of each region in the United States was conducted to examine job stress in directory assistance, service representative and clerical jobs with specific emphasis on the impact of electronic monitoring of job performance. Surveys were sent to 2,900 employees using mailing lists of bargaining unit members obtained by the Communications Workers of America (CWA) from local telephone companies. Usable responses were received from 745 employees representing 7 operating companies and A,T&T. A range of working conditions were examined in the questionnaire such as job control, job demands, supervisory relations, job content, career development and performance monitoring. Also examined were job strain outcomes such as tension, anxiety, depression and somatic complaints. The results of this study indicate that electronic monitoring of employee performance adversely affected employee perceptions of their working conditions and was related to increased levels of job boredom, tension, anxiety, depression, anger and fatigue.

*Department of Industrial Engineering, University of Wisconsin-Madison
**Communications Workers of America, Washington, DC

Introduction and Methods

Recently, interest in the health effects of electronic performance monitoring, particularly psychological distress, has increased due to reports of potential problems (Smith et al, 1986; OTA, 1987). These reports indicated that electronic monitoring of employee performance had the potential to create working conditions that could be very stressful, such as reduced employee control over the work process, increased workload demands and negative supervisory interaction.

Monitoring and Stress

A major concern in electronic monitoring is the influences that it can have on worker self-image and on feelings of self-worth. In one sense, monitoring should enhance feelings of worth if the results of worker efforts are positive and the worker gets feedback to that effect. Likewise, management interest in the worker as a valuable resource can be demonstrated by the attention provided by monitoring. However, both effects may be seen differently by workers if poor performance can lead to some form of punishment or reprimand. This fear of evaluation can produce anxiety and heightened sensitivity to adverse feedback that may damage self-esteem and self-image.

Tied to fear of reprimand is the pressure to perform above "average." Some managers may feel that this is a desirable effect since it implies high production. But occupational stress research indicates that such work pressure is not conducive to good performance and brings about adverse health consequences (Smith,1987).

In fact, there are a range of stressful working conditions that could be produced by electronic monitoring of employee performance. These include heightened work pressure, routinized work activities, paced work, potential for increased work standards and workload, lack of control over the tasks, lack of decision latitude, reduced peer social support, reduced supervisory support and fear of job loss.

The following is a summary of the potential for various job conditions that could be adversely influenced by electronic monitoring of worker performance and produce stress.

Lack of participation in work activities has been demonstrated to result in an increase in negative psychological mood (Smith et al., 1981; Smith, 1987). In terms of organizational support, it has been shown that close supervision and a supervisory style characterized by constant negative performance feedback are related to high levels of stress and poorer worker health (Smith et al., 1981). The implication of these findings for performance monitoring is that excessive, impersonal electronic

monitoring of employee performance can produce close supervision and constant negative performance feedback which may promote worker stress.

It has also been demonstrated that workers' feelings of lack of involvement are related to stress and potentially to health complaints. (WHO, 1989). Electronic monitoring has the propensity to reduce worker feelings of job involvement since the technology is controlling their behavior. This may increase worker distress. The chances to participate and be involved in the job process can be diminished in work systems that are driven by employee performance monitoring.

Concern over chances for promotion has been shown to be a significant stressor for office workers while being passed over for promotion has been related to increases in both job stress and ill-health (Smith et al., 1981; Smith, 1987). Performance monitoring can have both beneficial and negative effects in this regard. If monitoring provides for more objective employee evaluations and employee promotions are tied into the evaluation process, then monitoring may have a positive benefit for workers who are good performers. However, if the monitoring is perceived as unfair and not representative of true performance, then this could produce a stressful influence.

The threat of job loss is a very potent stressor that has been tied to serious health disorders such as ulcers, colitis, severe emotional stress and patchy baldness as well as to increased muscular and emotional complaints (Smith, 1987). Monitoring can be used for employee dismissal due to unsatisfactory performance that can be quantified, and fear of such use can be very stressful.

Monitoring may reduce task complexity, variety, challenge, and skills use due to the need for management to simplify work tasks and break them down into measurable units that can be easily monitored. Such job characteristics have been shown to be stressful (Smith, 1987).

Monitoring can reduce the amount of discretionary control and participation unless specific actions are taken by management to include these elements in the use of the monitoring process. If supervisors use monitoring to badger employees about their performance, this reduces employee control, which is a recognized stress factor (Smith, 1987).

Mental workload factors, such as quantitative underload/overload can cause stress. Monitoring is often accompanied by the establishment of work standards to assess employee performance. These standards are not always based on scientific grounds, but sometimes are based on the capabilities of machinery. This can cause employees to work too hard (Smith et al., 1981). If the standards are excessive they will produce physical and psychological stress. On the other hand, monitoring could mitigate workload stress if it is used as a scientific method for establishing proper workload requirements.

Time pressure, such as having to meet deadlines, is a stressor that may interact with work hours and workpace. Studies have shown increases in stress level as difficult deadlines draw near (Smith, 1987). Monitoring may produce such deadline pressure that may be more damaging than simple deadline pressure because of its constant, daily nature.

In summary, there is no direct empirical research that supports the contention that electronic performance monitoring increases stress to the extent that it diminishes employee health. However, the foregoing review shows that electronic monitoring has the "potential" to adversely influence working conditions which have been shown to cause stress. Indeed, electronic monitoring may actually create these adverse working conditions such as paced work, lack of involvement, reduced task variety and task clarity, reduced peer social support, reduced supervisory support, fear of job loss, routinized work activities, and lack of control over tasks.

Methods:

Based on these concerns, in the Spring of 1989 the Communications Workers of America and the Industrial Engineering Department at the University of Wisconsin undertook a cooperative study to examine the mental health concerns posed by electronic monitoring of performance in select telecommunications jobs. This report represents the initial evaluation of the data to define potential health risks.

It was determined that this should be a national study to be able to represent telecommunications jobs across the country. To achieve a national geographic distribution, an operating company from each of the seven regional "Baby Bells" was randomly selected to have its employees participate. Employees in each selected company who were classified as directory assistance operators, service representatives or clerks were eligible to participate. At each location, four hundred employees were randomly selected for participation, 100 directory assistance operators, 100 service representatives and 200 clerks. In addition, a random sample of 200 employees in select jobs working for A, T & T was also selected.

A questionnaire survey was used to gather information from the selected employees. The survey form was based on previous forms used to study job stress in office work developed at the National Institute for Occupational Safety and Health (Smith et al, 1980 & 1981) and the Department of Industrial Engineering at the University of Wisconsin (Smith et al, 1986). The questionnaire survey examined job demands, job content, supervisory relations, career issues, work standards, electronic monitoring considerations, mental moods and somatic health complaints. Surveys were mailed first class to each selected participant. Included in the survey package was a letter from the National President of CWA explaining the importance of the survey and urging participation, a set of instructions, a survey form that takes approximately 20 minutes to complete and a pre-addressed, postage paid return envelop to the University of Wisconsin.

Participant identification numbers were included on each envelop to allow for follow-up of nonrespondents. A second mailing was made to all nonrespondents four weeks after the initial mailing. A total of 2,900 employees were eligible to participate. Surveys were received from 762 employees. Four weeks after the second mailing the survey forms were sent to a data processing contractor for data entry. A computer disk with the survey data suitable for use on an IBM-AT computer was produced and sent to the University of Wisconsin for data analysis. All statistical analyses were performed using SYSTAT-PC version.

Results

Job Stressors and Job Content Factors:

Tables 1-4 show the mean values of job stressors and job content features for monitored and unmonitored employees and across job categories. As can be seen in Table 1 the monitored employees reported higher workload and greater workload dissatisfaction than the unmonitored employees. However, the monitored employees reported less workload variation. The monitored employees also reported less control over their jobs. There was no difference in the extent of promotion potential, but the monitored employees reported greater career future ambiguity. The monitored employees also reported less fairness of their work standards.

Table 2 shows differences in reported job stressor levels across the three job categories. Clerks reported the lowest workload and the least workload dissatisfaction. However, they also had the greatest workload variance. Clerks reported more job control with directory assistance operators reporting the least amount of control over their job. The directory assistance operators reported the greatest career future ambiguity. There were no differences in the reported levels of promotion potential or fairness of work standards.

Table 3 shows that monitored employees reported less skill use, variety, job completeness and job meaningfulness than unmonitored employees. Table 4 indicates that directory assistance operators reported less skill use, variety and meaningfulness.

Supervisory Factors:

Tables 5 and 6 show differences in supervisory factors for monitored and unmonitored employees and across job categories. Table 5 indicates that monitored employees reported more problems with supervisory relations and a greater amount of supervisor feedback than unmonitored employees. Table 6 shows that directory assistance operators reported more problems with supervisors than clerks and more supervisor feedback than both clerks and service representatives.

Job Strain and Somatic Complaints:

Tables 7 and 8 illustrate differences between monitored and unmonitored employees and across job categories for measures of psychological strain. Table 7 shows that monitored employees reported more boredom, tension/anxiety, depression, anger and fatigue than unmonitored employees. Table 8 indicates that directory assistance operators reported more boredom than both service representatives and clerks. Directory assistance operators also reported more tension/anxiety and depression than clerks. Both directory assistance operators and service representatives reported more anger and fatigue than clerks.

Table 9 illustrates the percentage of monitored and unmonitored employees reporting somatic health complaints. These can be categorized into musculoskeletal problems, psychological problems and psychosomatic problems. It should be emphasized that the percentages of both monitored and unmonitored employees reporting somatic problems were high, but were within the approximate ranges as reported in previous studies of computerized clerical jobs (Smith, 1987). For the musculoskeletal problems, more monitored employees reported wrist, arm, shoulder, neck and back problems than unmonitored employees. For the psychological problems, more monitored employees reported high tension, severe fatigue or exhaustion, extreme anxiety and depression. For the psychosomatic problems more monitored employees reported headaches. However, there was equivalent reporting of heart palpitations and disturbances for monitored and unmonitored employees.

Comparisons Between Monitored and Unmonitored Employees Within Two Job Categories:

Comparisons were conducted between monitored and unmonitored employees within two job categories, service representatives and clerks. Table 10 illustrates the results of the comparisons between monitored (N=174) and unmonitored (N=80) service representatives. Monitored service representatives reported higher workload and greater workload dissatisfaction than the unmonitored service representatives. However, the monitored service representatives reported less workload variation. The monitored service representatives also reported less control over their jobs. There was no difference in the extent of promotion potential, but the monitored service representatives reported greater career future ambiguity. The monitored service representatives also reported less fairness of their work standards. Table 10 shows that monitored service representatives reported less variety and job completeness than unmonitored service representatives. Monitored service representatives reported more problems with supervisory relations than unmonitored service representatives. Monitored service representatives reported more

boredom, tension/anxiety, depression, anger and fatigue than unmonitored service representatives.

Table 11 illustrates the results of the comparisons between monitored (N=58) and unmonitored (N=203) clerks. Monitored clerks reported higher workload and greater workload dissatisfaction than the unmonitored clerks. However, the monitored clerks reported less workload variation. The monitored clerks also reported less control over their jobs. There was no difference in the extent of promotion potential, but the monitored clerks reported greater career future ambiguity. The monitored service representatives also reported less fairness of their work standards. Table 11 shows that monitored clerks reported less skill use, variety, job completeness and meaningfulness than unmonitored clerks. Monitored clerks reportad more problems with supervisory relations than unmonitored clerks. Monitored clerks reported more boredom, tension/anxiety and anger than unmonitored clerks.

Predictors of Strain:

Multiple regression and stepwise regression procedures were used to determine factors that were predictors of the psychological and health strain outcomes. These were examined for the entire sample and within each job category for each specific strain outcome. Then a matrix was constructed of the most frequently occurring predictors by strain outcomes. This matrix provides an opportunity to examine patterns of specific predictors across a number of strain outcomes. When examining the entire sample across 17 separate strain measures the following were the most frequent predictors of strain: (1) workload , (2) meaningfulness, (3) supervisory relations and (4) various demographic variables such as age, gender, tenure and job experience.

For directory assistance operators the most frequently observed predictors of strain were: (1) supervisory relations - 14, (2) demographic variables such as age and gender - 8, (3) meaningfulness - 6, (4) workload - 5 and (5) control - 4.

For service representatives the most frequently observed predictors of strain were: (1) demographic variables such as age and gender - 11, (2) meaningfulness - 9, (3) supervisory relations - 8, (4) workload - 5, (5) completeness - 5 and (6) career opportunities - 4.

For clerks the most frequently observed predictors of strain were: (1) workload - 13, (2) supervisory relations - 9, (3) career opportunities - 9, (4) demographic variables such as age and gender - 8, (5) meaningfulness - 6 and (6) workload variance - 5.

When examining the matrices of predictors of strain for the monitored and the unmonitored employees similar patterns were observed in the factors

that were predictors within each group, except that their rank in terms of the frequency of strains predicted differed somewhat. The important predictors were workload, supervisory relations, meaningfulness, and demographic variables such as age and gender. The unmonitored employees also had career concerns as a frequent predictor of strain.

A discriminant function analysis was carried out to determine job factors that differentiated the monitored from the unmonitored employees (See Table 12). The top three factors that differentiated the groups were: (1) control, (2) client relationships and (3) skill variety.

Discussion

The results of this study must be used with caution due to the low response rate. A majority of the employees selected to participate did not respond to the survey, and those that did respond may have had a bias for or against specific working conditions. A review of the distributions of responses within the three job categories indicated a good dispersion for all job variables and job strains for each of the jobs. There was no indication of a specific bias. The responses were within similar ranges and mean values as other populations of office workers that have been studied in the past (Smith, 1987). Even so, caution is advised, and verification of these results is warranted. In fact, two additional sites have already been selected for indepth evaluation to provide verification. These evaluations are expected to be completed next Summer.

The results of the entire sample indicate that electronic performance monitoring has adverse effects on employees' perceptions of how stressful their jobs are and on their reported levels of physical and psychological strain. Similar results were found for the comparisons of monitored and unmonitored employees within two job categories (service representatives and clerks). These results confirm that electronic performance monitoring has the potential to increase stress because of its influence on job characteristics that are well-known stressors.

Perceptions of job characteristics and physical and psychological strains were compared across the three job categories. Results showed that directory assistance operators have more negative job elements than service representatives and clerks. Directory assistance operators reported more strain than service representatives and clerks.

Specific job design factors that contributed to physical and psychological strains for both monitored and unmonitored employees were workload, meaningfulness of the job and supervisory relations. Discriminant analysis indicated that factors that differentiated the monitored and unmonitored employees, such as control and skill use, were not good predictors of physical or psychological strain. Secondary factors that also differentiated monitored and unmonitored groups were workload and supervisory relations. These were important predictors of strain for both monitored and

unmonitored employees, but it appears that these conditions were influenced by monitoring in a way that produced greater impact on the monitored employees.

References and Select Bibliography

Aronsson, G., 1989. Changed qualification demands in computer-mediated work. Applied Psychology: An International Review, 38:57-71.

Aronsson, G. and Johansson, G., 1987. Work content, stress and health in computer-mediated work. In: Knave, B. and Wideback, P.-G. (Eds.), Work With Display Units 86, Elsevier Science Publishers, The Netherlands, pp. 732-738.

Bergqvist, U.O., 1984. Video display terminals and health. Scandinavian Journal of Work and Environment Health, 10(2):1-87.

Carayon, P. and Smith, M.J., 1986. Office Ergonomics: An Overview. Ninety-fourth Annual Convention of the American Psychological Association, Washington, DC.

Cohen, B.G.F., 1984. Organization factors affecting stress in the clerical worker. In: Cohen, B.G.F. (Ed.), Human Aspects in Office Automation. The Netherlands, Elsevier Science Publishers, pp. 33-42.

Flynn, P.M., 1989. Introducing new technology into the workplace: The dynamics of technological and organizational change. Investing in People - A Strategy to Address America's Workforce Crisis. U.S. Department of Labor, Commission on Workforce Quality and Labor Market Efficiency, Washington, D.C., pp. 411-456.

Frese, M., 1987. Human-computer interaction in the office. In: Cooper, C.L., Robertson, I.T. (Eds.), International Review of Industrial and Organizational Psychology. Chichester: Wiley, pp. 117-165.

Ghiringhelli, L., 1980. Collection of Subjective Opinions on Use of VDUs. In: Grandjean, E. and Vilgliarri (Eds.), Ergonomic Aspects of Visual Display Terminals. Taylor and Francis, Ltd., London, pp. 227-232.

Johansson, G. and Aronsson, G., 1984. Stress reactions in computerized administrative work. J. Occup. Behav., 5:159-181.

Kalimo, R. and Leppanen, A., 1985. Feedback from video display terminals, performance control and stress in text preparation in the printing industry. J. Occup. Psychol., 58:27-38.

Lim, Soo-Yee, Sainfort, Pascale C. and Smith, Michael J., 1990. The Role of Job Design Factors in Office Ergonomics. In: Das, Biman (Ed.), Advances in Industrial Ergonomics and Safety II. Taylor & Francis, pp. 385-393.

Linton, Steven J. and Kamwendo, Kitty, 1989. Risk Factors in the Psychosocial Work Environment for Neck and Shoulder Pain in Secretaries. Journal of Occupational Medicine, 31(7):609-613.

MacKay, C.J. and Cox, T., 1984. Occupational stress associated with visual display unit operation. In: Pearce, B.G. (Ed.), Health Hazards of VDUs? Chichester: Wiley, pp. 137-143.

Murray, W.E., Moss, C.E., Parr, W.H., Cox, C., Smith, M.J., Cohen, B.G.F., Stammerjohn, L.W., and Happ, A., 1981. Potential Health Hazards of Video Display Terminals. Cincinnati, Ohio: National Institute for Occupational Health and Safety.

NIOSH, 1986. A Proposed National Strategy for the Prevention of Work-related Psychological Disorders. National Institute for Occupational Safety and Health, Cincinnati, OH.

Ostberg, O. and Nilsson, C., 1985. Emerging technology and stress. In: C.L. Cooper and M.J. Smith (Eds.), Job Stress and Blue Collar Work. John Wiley and Sons, New York, pp. 149-169.

OTA, 1985. Automation of America's Offices. Washington, DC: Office of Technology Assessment, U.S. Congress, OTA-CIT-287.

OTA, 1986. The Electronic Supervisor. Washington, DC: Office of Technology Assessment, U.S. Congress.

Sainfort, Pascale C. and Lim, Soo Yee, 1989. A Longitudinal Study of Stress Among VDT Workers: Preliminary Results. In: Smith, M.J. and Salvendy, G. (Eds.), Work with Computer: Organization, Management, Stress and Health Aspects. Elsevier Science Publishers B.V., Amsterdam, The Netherlands, pp. 241-247.

Sainfort, Pascale C. and Smith, M.J. Stress Outcomes Among VDT Users. In: Smith, M.J. and Salvendy, G. (Eds.), Work with Computers: Organization, Management, Stress and Health Aspects. Elsevier Science Publishers, B.V., Amsterdam, The Netherlands, pp. 233-240.

Sauter, S.L., Gottlieb, M.S., Jones, K.C., et. al., 1983. Job and health implications of VDT use: initial results of the Wisconsin-NIOSH study. Communications of the ACM, 26:285-294.

Sauter, S.L., Gottlieb, M.S., Rohrer, K.M. and Dodson, V.N., 1983. The Well-Being of Video Display Terminal Users. Department of Preventive Medicine, University of Wisconsin, Madison, WI.

Sauter, S.L. and Hurrell, J.J., 1987. Occupational health and the computer mediation of information work: research needs. In: Salvendy, G., Sauter, S.L. and Hurrell, J.J. (Eds.), Social, Ergonomic and Stress Aspects of Work with Computers. Amsterdam: Elsevier Science Publishers, pp. 211-217.

Schleifer, L.M., 1987. An evaluation of mood disturbances and somatic discomfort under slow computer response time and incentive pay conditions. In: Knave, B. and Wideback, P.G. (Eds.), Work With Display Units 86, Amsterdam: Elsevier Science Publishers.

Schleifer, L.M. and Amick, B.C. III, 1989. System response time and method of pay: Stress effects in computer-based tasks. International Journal of Human-Computer Interaction, 1:23-39.

Schleifer, L.M. and Shell, R.L., 1990. Computer monitoring of work performance and the alleviation of stress. In: Noro, K. and Brown, O. Jr. (Eds), Human Factors in Organizational Design and Management-III, Amsterdam: North-Holland.

Smith, M.J., 1984. Health Issues in VDT Work. In: J. Sandelin, S. Bennett, and D. Case (Eds.), Video Display Terminals: Usability Issues and Health Concerns. Prentice-Hall, Englewood Cliffs, NJ, pp. 193-228.

Smith, M.J., 1986. Job Stress and VDUs: Is the Technology a Problem? In: Proceedings of International Scientific Conference: Work with Display Units. Stockholm, Sweden: National Board of Occupational Safety and Health, pp. 189-195.

Smith, M.J., 1987. Occupational stress. In: G. Salvendy (Ed.), Handbook or Ergonomics/Human Factors. John Wiley and Sons, New York, pp. 844-860.

Smith, M.J., 1987. Mental and physical strain at VDT workstations. Behaviour and Information Technology, 6:243-255.

Smith, M.J. and Sainfort, P.C., 1989. A balance theory of job design for stress reduction. International Journal of Industrial Ergonomics, 4:67-79.

Smith, M.J., Stammerjohn, L., Cohen, B.G.F., and Lalich, N., 1980. Video Display Operator Stress. In: Grandjean, E. and Vigliani, E. (Eds.), Ergonomic Aspects of Visual Display Terminals. London: Taylor & Francis, Ltd., pp. 201-210.

Smith, M.J., Cohen, B.F.G., Stammerjohn, L.W. and Happ, A., 1981. An Investigation of Health Complaints and Job Stress in Video Display Operations. Human Factors, 23(4):389-400.

Smith, M.J., Carayon, P., and Miezio, K., 1986. Motivational Behavioral and Psychological Implications of Electronic Monitoring of Worker Performance. Washington, D.C.: Office of Technology Assessment.

Smith, M.J., Carayon, P. and Miezio, K., 1987. VDT technology: Psychosocial and stress concerns. In: B. Knave and P.-G. Wideback (Eds.), Work with Display Units 86. Elsevier Science Publishers, The Netherlands, pp. 695-712.

Starr, S.J., 1983. A Study of Video Display Terminal Workers. Journal of Occupational Medicine, 25:95-98.

Starr, S.J., Thompson, C.R., and Shute, S.J., 1982. Effects of Video Display Terminals on Telephone Operators. Human Factors, 24:699-711.

Stellman, J.M., Klitzman, S., Godon, G.C., and Snow, B.R., 1987. Work environment and the well-being of clerical and VDT workers. J. Occup. behav., 8:95-102.

World Health Organization, 1989. Work with Display Terminals: Psychosocial Aspects and Health. Journal of Occupational Medicine, 31(12):957-968.

Table 4
Job Content Factors Across Job Categories

Job Content Factors	Directory Assistance Operators	Service Representatives	Clerks
Skill Use**	6.0	8.2	7.8
Variety**	-2.4	-0.1	0.1
Completeness	10.3	9.8	10.1
Meaningfulness**	0.4	1.8	2.0

**Significant difference at the .01 level using an Analysis of Variance

Table 5
Supervisory Factors for Monitored and Unmonitored Employees

Supervisory Factors	Monitored	Unmonitored
Problems with Supervisor Relations**	3.8	3.0
Amount of Supervisor Feedback**	6.7	6.1
Supervisor Monitoring	5.3	5.1

**Significant difference at the .01 level using an Analysis of Variance

Table 6
Supervisory Factors Across Job Classifications

Supervisory Factors	Directory Assistance Operators	Service Representatives	Clerks
Problems with Supervisory Relations**	3.9	3.5	3.1
Amount of Supervisory Feedback**	7.1	6.4	6.0
Supervisory Monitoring	5.3	5.1	5.2

**Significant difference at the .01 level using an Analysis of Variance

Table 7
Psychological Strain of Monitored and Unmonitored Employees

Psychological Strains	Monitored	Unmonitored
Bored**	4.1	1.9
Tension/Anxiety**	13.2	9.4
Depression**	13.4	9.9
Anger**	13.0	9.2
Fatigue**	12.0	9.2

**Significant difference at the .01 level using an Analysis of Variance

Table 1
Select Job Stressors for Monitored and Unmonitored Employees

Job Demands	Monitored	Unmonitored
Workload**	24.0	20.6
Workload Variation**	7.4	9.3
Workload Dissatisfaction**	9.0	6.9
Job Control**	10.9	17.1
Career Future Ambiguity**	9.6	8.6
Promotion Potential	3.3	3.4
Lack of Fair Work Standards**	7.8	7.1

**Significant difference at the .01 level using an Analysis of Variance

Table 2
Select Job Stressors Across Job Categories

Job Demands	Directory Assistance Operators	Service Representatives	Clerks
Workload**	22.9	24.5	20.6
Workload Variance**	7.5	7.5	9.3
Workload Dissatisfaction**	8.6	8.8	7.2
Job Control**	10.2	12.4	16.6
Career Future Ambiguity**	10.2	8.0	9.5
Promotion Potential	3.2	3.5	3.3
Lack of Fair Work Standards	7.7	7.6	7.4

**Significant difference at the .01 level using an Analysis of Variance

Table 3
Job Content Factors for Monitored and Unmonitored Employees

Job Content Factors	Monitored	Unmonitored
Skill Use**	6.9	8.3
Variety**	-1.4	0.4
Completeness**	9.8	10.4
Meaningfulness**	1.0	2.3

**Significant difference at the .01 level using an Analysis of Variance

Table 8
Psychological Strain Across Job Categories

Psychological Strains	Directory Assistance Operators	Service Representatives	Clerks
Bored**	5.6	2.0	2.5
Tension/Anxiety**	13.4	12.2	9.8
Depression*	13.8	12.1	10.6
Anger**	12.5	12.5	9.8
Fatigue**	11.9	11.5	9.6

**Significant difference at the .01 level using an Analysis of Variance

*Significant difference at the .05 level using an Analysis of Variance

Table 9
Somatic Health Complaints of Monitored and Unmonitored Employees
(Percent Reporting a Complaint)

Somatic Health Complaints	Monitored	Unmonitored
Loss of feeling in fingers/wrists**	43	27
Stiff or sore wrists**	51	24
Pain or stiffness in shoulders**	79	66
Shoulder soreness**	76	57
Pain or stiffness in arms/legs**	68	55
Neck pain into shoulder, arm, hand**	64	41
Neck pressure**	81	60
Back pain**	79	73
Racing or pounding heart	55	43
Acid indigestion	70	61
Stomach pains	54	49
Headaches**	92	86
Depression*	81	69
Severe fatigue or exhaustion**	79	63
Extreme anxiety**	72	57
High tension**	83	67

**Significant at the .01 level using a Chi Square analysis

*Significant at the .05 level using a Chi Square analysis

Table 10
Job Characteristics and Job Strain of Monitored and Unmonitored Employees
Service Representatives

	Monitored N=174	Unmonitored N=80
Workload**	25.5	22.3
Workload Variance**	7.0	8.5
Workload Dissatisfaction**	9.4	7.6
Job Control**	11.1	15.5
Career Future Ambiguity**	8.4	7.1
Promotion Potential	3.4	3.7
Lack of Fair Work Standards**	7.8	7.1
Client Relationships**	11.9	10.4
Skill Use	8.0	8.9
Variety**	-0.3	0.6
Completeness**	9.5	10.5
Meaningfulness	1.6	2.2
Problems with Supervisor Relations**	3.7	3.1
Amount of Supervisor Feedback	6.5	6.3
Supervisor Monitoring	5.3	4.9
Bored*	2.3	1.4
Tension/Anxiety**	13.2	9.9
Depression*	13.2	9.7
Anger*	13.7	9.9
Fatigue**	12.6	9.1

**Significant difference at the .01 level using an Analysis of Variance

*Significant difference at the .05 level using an Analysis of Variance

Table 11
Job Characteristics and Job Strain of Monitored and Unmonitored Employees
Clerks

	Monitored N=58	Unmonitored N=203
Workload**	23.2	19.9
Workload Variance*	8.4	9.6
Workload Dissatisfaction**	9.2	6.6
Job Control**	12.8	17.9
Career Future Ambiguity**	10.7	9.2
Promotion Potential	3.1	3.3
Lack of Fair Work Standards**	8.0	7.2
Client Relationships*	8.5	7.5
Skill Use*	6.5	8.1
Variety**	-0.9	0.3
Completeness**	9.3	10.3
Meaningfulness*	1.1	2.3
Problems with Supervisor Relations**	3.5	3.0
Amount of Supervisor Feedback	6.0	6.0
Supervisor Monitoring	5.3	5.2
Bored**	4.0	2.1
Tension/Anxiety*	11.9	9.2
Depression	12.2	10.1
Anger*	12.7	8.9
Fatigue	10.7	9.2

**Significant difference at the .01 level using an Analysis of Variance

*Significant difference at the .05 level using an Analysis of Variance

Table 12
Job Design Variables Differentiating
Monitored vs Non-Monitored Employees

Discriminant Function Analysis Results

Job Design Variable	Standard Coefficient	Significance Level
control	-.609	**
client relationships	.545	**
workload	.012	**
skill variety	-.256	**
poor supervisor relationship	.097	**
workload variability	-.063	**
standards	.058	**
skill utilization	.000	**
task meaningfulness	.089	**
supervisor feedback	.129	**
task completeness	-.060	*
career/future ambiguity	-.052	*
supervisor monitoring	-.047	NS
promotions/advancements	.170	NS

* Significant at the .05 level.
** Significant at the .01 level.

Senator SIMON. Senator Metzenbaum is involved in the hearing for Mr. Gates, who is the nominee for head of the CIA, and has to get back there, but he would like to ask you a couple of questions, Mr. Bahr.

Senator METZENBAUM. Thank you, Mr. Chairman, and I apologize to the other witnesses. It is not from a lack of interest in your statements; I will read your statements. But when I was in private life, I had the privilege of representing Mr. Bahr's union back in Ohio, so I know that anything he answers for me is going to have almost a lawyer-client relationship, and I know I'll get a straight answer.

In your testimony, you mention that for a period of time West Virginia had a law that banned electronic monitoring. Did any employers that you know of leave the State as a result of that law?

Mr. BAHR. No employer to my knowledge ever left the State, but it was interesting to note that some blackmail took place after Governor Rockefeller went out of office. AT&T—and I use the word very deliberately—blackmailed the legislature and the Governor that they would not open an office in Charleston with 500 jobs unless that law was repealed. And that caused that law to be repealed.

Senator METZENBAUM. We will hear testimony today from the National Association of Manufacturers that the bill may be harmful to the productivity of American businesses. Do you have any comment on that?

Mr. BAHR. I think in two ways—let me go back and add when that law in West Virginia was still on the books, the C&P Telephone Company did transfer work from Washington, DC and Maryland to West Virginia, so we see that it did work.

Insofar as the impact on productivity, I would respond in two ways. First, we are at a time when American business is streamlining. The common word today we hear is "downsizing," and downsizing both in bargaining unit as well as managerial levels. So I think it is quite ironic that management sees no problem with having supervisor employees devote a considerable amount of time to doing anything but productive work, and that is the spying and listening in on workers.

The other side of the coin is that clearly the University of Wisconsin study as well as our knowledge of what is happening to our members and the testimony that was presented by this first panel indicates that there is a good deal of illness, absenteeism as a result of the stress that is caused by this kind of a practice that we do not see in any of the nations with whom we compete.

When I visited my colleagues in Japan and Germany on this very subject, they actually thought it was onerous to think that a practice like this existed. They would not even consider it—and the are our major competitors and eating our lunch.

Senator METZENBAUM. I have one more question. The NAM opposes the bill in part because they claim that workers would prefer not to know when their performance is monitored. The NAM suggests that if employees knew they were being monitored, they would be nervous or flustered, and their performance would suffer.

Do any of your members feel this way about electronic monitoring, that they would rather not know that they are being monitored?

Mr. BAHR. Senator, that's ridiculous. A statement like that is made from total lack of knowledge and experience. We are negotiating and have negotiated with employers monitoring with the employees' knowledge, and it works. In fact, you probably saw in the press that we just signed an agreement with NYNEX 11 months in advance of expiration. In that agreement is a clause that states that the CWA and IBW will work with NYNEX to eliminate all forms of secret monitoring and come up with a system that will provide the quality of service that the employees want—we know we are in a competitive environment—without the secrecy. So we would fully subscribe to it, and if that is the NAM's only concern, they ought to sign onto this bill and let it work.

Senator METZENBAUM. Maybe they will. Thank you very much, Mr. Bahr, and I thank the other members of this panel.

Mr. Chairman, I appreciate your courtesy.

Senator SIMON. I thank Senator Metzenbaum for his interest in this whole subject.

Dr. Marx, I understand we have an expert here, and we're happy to hear from you now.

Mr. MARX. Well, an "expert" can be defined as someone who is more than 10 miles from home.

Senator SIMON. Our first panel of three were experts in a very different way than you are.

Mr. MARX. Thank you, Senator. I am pleased to be here.

I am a professor of sociology at Massachusetts Institute of Technology. I teach and do research on the social, political, ethical and public policy aspects of new information technologies, with a particular interest in questions of privacy and civil liberties.

In my testimony, I consider five issues at a perhaps broader level which tries to put these things in a context of the whole society, of other countries and American history.

The five issues I consider in my paper are: first, the need to see that electronic monitoring of workers doesn't stand alone but is part of a much broader set of changes that are capable of destroying boundaries that are fundamental to our sense of self and the separation of the public and the private. Video cameras, drug testing, electronic location monitoring, satellite surveillance. This morning in the *Wall Street Journal* coming down, I read about a new device created by a Massachusetts company. It is a small electronic drug testing device that can detect microscopic amounts of drugs from the air, dust and clothing samples. It is hand-held. It is the size of a flashlight. It is a kind of vacuum, so you vacuum the person's clothes, you vacuum the desk where they were sitting, and it presumably will give you evidence of drug residue. And it can be done whether or not a person is there. That's simply one minor example.

The second broad point I make has to do with the importance of this kind of legislation in the United States' context where interest groups—in spite of my distinguished colleague to my right here—representing workers are not as strong as they once were, where we don't have the traditions and the laws that Europe have, which

guarantee workers a safe and healthy work environment with respect to management practices, not simply what's in the air. We also don't have the tradition of cooperation between workers and employers that one finds in Europe.

So Congress is really the last resort for generating these protections that are so badly needed.

I talk about some techno-fallacies and the world view of those who advocate unrestrained monitoring. I talk about some broad principles that ought to underlie laws and policies protecting us from unwarranted electronic surveillance. And finally, I talk about the possibility, ironically, of using monitoring to create a more equitable, accountable and productive work environment by extending it upward. If it really works for workers, if it is so terrific as the advocates claim, why not apply it to management, whose errors and violations can do far, far more damage than can an isolated worker.

As a professor, unaccustomed as I am to talking for 5 minutes, I will simply give some sense of the techno-fallacies and then some of the principles that I think ought to be there.

I have identified what I call a large number of "tarnished silver bullet techno-fallacies" of the information age. I am an ethnographer; I watch and I listen, and I hear things much as a musician knows that some notes are offkey—I hear things that I know are wrong, whether morally, empirically, legally or logically: "Turn the technology loose and let the benefits flow;" "monitoring is for the worker's own good;" "do away with the human interface;" "when you choose to make a phone call you are consenting to have your phone number released;" "the public interest is whatever the public is interested in watching"—these are all direct quotes—"there is no law against this;" "the system is free of human bias;" "the technology is neutral."

In the testimony, I identify six techno-fallacies, and I elaborate on these. The first is the fallacy of assuming that technology is only a means of increasing productivity and profits and improving service, rather than also a means—as it is in parts of Europe—to enhance job satisfaction for workers.

A second fallacy is the fallacy of assuming that personal inflation on workers or customers that the company can collect is just another commodity like raw materials to be combined, reused, or sold as the company sees fit without informing and obtaining the consent of the subject.

A third fallacy is the fallacy of implied consent and free choice, which one well-known employer said to an employee who complained about monitoring practice: "Well, if you don't like it, simply go and work somewhere else." But in fact if all employers in a particular area engage in these practices, that's a rather specious freedom of choice.

A fourth fallacy is the fallacy that machine-generated facts speak for themselves and are necessarily more valid, reliable and neutral than human-generated facts. There is much one can say about the "acontextual" nature of electronic data, that it is ripped out of its human context, that it needs to be interpreted.

Fifth is the fallacy of confusing quantity with quality and what can be easily measured with what is important.

The sixth and final fallacy is the fallacy of assuming that people are best controlled through deception and the creation of uncertainty by not telling them that they are monitored or when they will be monitored.

There is certainly empirical and theoretical evidence to contradict those.

Now, an antidote to having to always react negatively and after the fact to these fallacies is to develop positive, affirming principles. A nice beginning in this regard is the Code of Fair Information Practices developed in 1973 for the U.S. Department of Health, Education and Welfare. It contains five principles—a principle of informing subjects, a principle of data inspection, a principle of consistent usage, a principle of correction, and a principle of relevance. I would suggest adding to those a principle of co-determination, so that in a work context, people subject to information extraction technology have some involvement; a principle of minimization, so that only data that is relevant and pertinent is collected; a principle of validity; a principle of timeliness; a principle of data security; a principle of human review; a principle of redress; a safety net or equity principle; and a principle of consistency so that broad ideals rather than the specific characteristics of the technology determination privacy protection.

Let me conclude by noting that I was raised in Hollywood, CA, and one of my most vivid childhood memories was seeing the film, "The Wizard of Oz." I was terrified, as most of us were, by the power of the wizard. The fact that he was unseen made it possible to conjure up images of a truly ferocious entity who might be anywhere and remotely cause anything to happen. The lightning and thunder he controlled and his deep and authoritative commands were very intimidating.

But as you may recall, at the end of the film the little dog, Toto, pulls the curtain away, and the wizard is revealed to be an elderly and frail man. At once we hear him say: "Pay no attention to the little man behind the curtain with the microphone in his hand. The Great Oz has spoken."

But if the United States is to remain a decent and productive society in which technology is put in the service of its citizens, we must pay attention to the men and women behind the electronic curtain and not only to those in front of it. The Privacy for Consumers and Workers Act is important because it helps us do that.

Thank you.

[The prepared statement of Mr. Marx follows:]

PREPARD STATEMENT OF MR. MARX

Mr. Chairman and Members of the Subcommittee: My name is Gary T. Marx. I am Professor of Sociology at the Massachusetts Institute of Technology (M.I.T.) in the Department of Urban Studies and Planning. I previously taught at Harvard and the University of California at Berkeley. I teach and do research on the social, political, ethical and public policy aspects of new information technologies with a particular interest in questions of privacy and civil liberties.

I am the author or editor of 8 books and many articles. I have received research grants from many sources including the Guggenheim Foundation, the National Science Foundation, the National Institute of Justice and the Twentieth Century Fund. My most recent book is *Undercover Police Surveillance in America* (University of California Press, 1988) which received prizes from the American Sociological Association and the Academy of Criminal Justice Sciences.

I have worked on questions involving the social impact of new information technologies with a wide array of government, public interest and private sector groups including several national commissions, Congressional Committees, the Office of Technology Assessment, the Government Accounting Office, the Justice Department, the National Academy of Sciences and communications companies.

I will consider five issues:

(A) the need to see the electronic monitoring of workers as part of a much broader set of changes capable of destroying boundaries fundamental to our sense of self and the separation of the public and the private.

(B) the particular importance of legislation such as this in the United States where interest groups representing workers are relatively weak.

(C) some techno-fallacies characterizing the world view of those who advocate unrestrained monitoring.

(D) some broad principles that ought to underlie laws and polices offering protection from unwarranted electronic surveillance.

(E) the possibility of using monitoring to create a more equitable, accountable and productive work environment by extending it upward.

A. WORK MONITORING IS NOT ALONE: THE NEW SURVEILLANCE

The development of electronic work monitoring reflects broader changes in surveillance and must be seen alongside other forms of video and audio surveillance, electronic location monitoring, computer dossiers, night vision technology, drug testing, and biometric forms of analysis including DNA.

While these extractive technologies have unique elements, they also tend to share certain characteristics which set them apart from many traditional means. Some of the information gathering techniques found in the maximum-security prison are diffusing into the broader society. We appear to be moving toward, rather than away from, becoming a "maximum security society." [1]

Such a society is transparent and porous. Information leakage is rampant. Indeed it is hemorrhaging. Barriers and boundaries—be they distance, darkness, time, walls, windows and even skin, which have been fundamental to our conceptions of privacy, liberty and individuality give way.

Actions, as well as feelings, thoughts, pasts, and even futures are increasingly visible. The line between the public and the private is weakened; observations seem constant; more and more goes on a permanent record, whether we will this or not, and even whether we know about it or not. Data in many different forms, from widely separated geographical areas, organizations, and time periods can easily be merged and analyzed.

Surveillance becomes capital—rather than labor—intensive. Technical developments drastically alter the economics of surveillance such that it becomes much less expensive per unit watched. Aided by machines, a few persons can monitor many people and factors. This contrasts with the traditional supervisor walking behind employees or the private detective or guard watching a few persons and the almost exclusive reliance on first hand information from the unenhanced senses.

An aspect of this efficiency, and the ultimate in decentralized control, is self or participatory monitoring. Persons watched become active "partners" in their own monitoring. Surveillance systems may be directly triggered when a person uses a telephone or computer, enters or leaves a controlled area, or takes a magnetically marked item through a checkpoint.

There is an emphasis on the engineering of behavior characterized by prevention, soft control and the replacement of people with machines. Where it is not possible to actually physically determine behavior, or that is too expensive, the system may be engineered so that a record of the behavior is left.

As the technology becomes ever more penetrating and intrusive, it becomes possible to gather information with laser-like specificity and with sponge-like absorbency. If we think about the information gathering net as being parallel to a fishing net, then the mesh of the net has become finer and the net wider.

Like the discovery of the atom or the unconscious, new techniques surface bits of reality that were previously hidden, or didn't contain informational clues. People are in a sense turned inside out, and what was previously invisible or meaningless is made visible and meaningful. In focusing on the electronic monitoring of work, we must not forget that it is part of a much broader set of changes.

---

[1] This section draws from chapters 1 and 10 of G. Marx, *Undercover: Police Surveillance in America*, Berkeley, Calif., Univ. of California Press.

We face the danger of an almost unseen surveillance creep in which we unreflectivly back into a "cowardly new world." In this world deceptively easy technical solutions are offered to tough social and political problems.

The reality of this was brought home to me when I published a satirical newspaper article on April Fool's Day describing an imaginary new Restroom Trip Policy (RTP) (in Appendix). Written in the bureaucratic jargon of a company memo, the policy gave workers a weekly Restroom Trip Credit (RTC) quota of 40 trips. Access was controlled by a computer linked voice-print recognition system; stalls were equipped with timed tissue-roll retraction and flushing and door-opening capabilities which were automatically activated after 3½ minutes. There was also a capability for automatic urine analysis to permit drug testing without the demeaning presence of an observer.

I wrote the article as an extreme exaggeration of trends that I found disturbing—such as U.S. companies that electronically counted time spent in the restroom and gave employees demerits when they exceeded the established time limit (three were grounds for dismissal). Imagine my surprise when I learned that there is a Japanese company that markets a toilet stall that can in fact automatically test for drugs in urine and that in Europe some toilet doors do open automatically after an elapsed period of time.

I also realized how rapidly our culture has changed and how weakened our expectations regarding privacy and technology have become, when perhaps half the readers were so conditioned by contemporary electronic intrusions that they thought the memo was genuine. We had come so far so fast that people were ready to accept this outlandish, imaginary example as real. I was asked where the company was and some companies even wrote and asked where they could purchase the monitoring system.

In an effort to provoke thought and call attention to the possibility of back-sliding in a piece-meal fashion into a world in which technology serves to dominate, rather than to liberate, I have described an imaginary workplace in the year 1995 based entirely on techniques now in use, or that have been advocated. This article, entitled "The Case of the Omniscient Organization" is in the appendix.

The legislation considered here is part of a needed social corrective in which (if we are lucky) laws, public policy and even manners eventually will catch up to the changes and challenges technology creates. Such developments would keep accounts such as "the Omniscient Organization" in the realm of fiction and satire rather than accurate social science prediction.

B. THE IMPORTANCE OF SUCH LEGISLATION IN THE UNITED STATES

In the spirit of the French observer of the United States Alexis De Tocqueville, rather than legislation, I would prefer to see social order emerge out of a balance of interests among strong associations who can serve as a counter to government and to each other. Unfortunately in the United States for historic reasons the power of labor is relatively weak and it is growing weaker. The law then must compensate for the weaknesses of the social structure. In that regard such legislation is very important as a means for insuring decent treatment of workers and introducing greater balance into workplace relations. It is also consistent with a modern trend to limit the doctrine of "employment at will" in which employers had almost absolute control over the workplace and their workers.

The Privacy for Consumers and Workers Act along with legislation such as the 1986 Electronic Communications Privacy Act are vital correctives to the dangers posed by turning "the technology lose." The latter is more likely to happen in the United States than in Europe because of the absence of strong employee associations, work environment laws, data protection commissions and legislation and traditions requiring that work conditions be jointly set by labor and management. As is well known unions are declining in strength in the United States and this shows no sign of abating. The worker-management councils found in Europe are almost nonexistent here. Apart from regulated industries, protections derived from the 14th Amendment and health, safety and welfare rules, management has a very free hand in setting work conditions in the United States compared to Europe.

Congressional actions supporting privacy in the workplace (e.g. against unreasonable searches and seizures) are also needed because Constitutional protections apply most clearly to the actions of government not the private sector.

It is also interesting that unregulated monitoring is often justified by a need to be competitive. Yet in general in neither Europe nor Japan do we see equivalent monitoring of individuals. If we really wish to emulate other productive countries the last thing we would turn to would be unrestrained monitoring. Instead we would seek to involve workers in establishing the conditions of work that affect them.

C. SOME TECHNO-FALLACIES OF ELECTRONIC MONITORING

Technical innovations are often accompanied by beliefs that are lacking empirical support, illogical or in conflict with important values. I have identified a number of what can be called "Tarnished Silver Bullet Techno-Fallacies of the Information Age." [2]

Before technical innovations are blithely adopted, it is important to examine the broader cultural climate, the rationales for action and the empirical and value assumptions on which they are based. The web of tacit assumptions that undergird action needs to be identified and analyzed. As an ethnographer I watch and listen. Sometimes I hear things which seem wrong, whether empirically, logically or normatively, much as a musician knows that certain notes are off key: "Turn the technology loose and let the benefits flow;" "monitoring is for the worker's own good;" "do away with the human interface;" "when you choose to make a phone call you are consenting to have your telephone number released;" "the public interest is whatever the public is interested in watching;" "there is no law against this;" "the system if free of human bias;" "the technology is neutral."

In the case of work monitoring the following 6 techno-fallacies are particularly salient:

(1) *The fallacy of assuming that technology is only a means of increasing productivity and profits and improving service, rather than also a means to enhance job satisfaction for workers.* It is not clear in the long run that one can obtain the latter without the former. Policies as well as work related technology should be developed in conjunction with workers. In the United States it is most common for a new technology to be developed in isolation and simply thrust upon employees. This process means technology that reflects the short run financial interests of management rather than the well-being of workers. The United States contrasts with some European countries in this regard.

A useful documentary film made by independent video producer California Newsreel shows how in Scandinavia the introduction of computer-aided printing technology was designed not only with concerns about productivity (an exclusive focus on this may translate into speeding up the work process, lost jobs, and lessened skill requirements) but with a concern for how machines might enhance creativity while eliminating drudgery. The creation of a more meaningful and satisfying work environment should be an important social goal and accompany efforts to develop and introduce new technologies into the workplace. It is also likely to be associated with increased productivity.

(2) *The fallacy of assuming that personal information on workers or customers that the company can collect is just another commodity like raw materials to be combined, re-used, or sold as the company sees fit without informing and obtaining the consent of the subject.* Yet personal information has an almost sacred quality and means as well as ends may have a moral quality. There is a related fallacy here which holds that only the guilty have to fear being secretly watched. This view fails to appreciate the social functions of privacy. An important reason that we have envelopes around first class letters or doors on rooms is not to protect the guilty. It is because control over personal information is important to our conception of human dignity. We should not recreate the company town.

This fallacy ignores the importance of due process and the legitimacy of boundaries. It fails to differentiate between work and non-work related data generated by the employee and the need to make a distinction (as difficult as it may be) between the work and the worker. For example conversations that occur among reservationists while they are waiting for calls are different than those that occur with customers. Behavior in an employee lounge or restroom ought to be treated differently than that at the desk or in front of a machine (e.g. regarding the use of video cameras) and personal telephone calls should not be subject to monitoring. Before computers most employers would not randomly search through employee desks. But now with desk top computers tied into large networks, it is easy to ramsack computer files from afar. There should be provision for employees to make some personal use of the computers on their desks on their own time without fear that their private communication will be seen by others, absent some reasonable grounds for suspecting serious violations. Just as most reasonable companies don't try to enforce rules about the personal use of company provided pens, employees should be permitted some personal files that are beyond the company's prying electronic eyes.

---

[2] Some of these are reported in G. Marx, "Privacy and Technology," *The World and I*, Sept. 1991 on which this page is based.

(3) *The fallacy of implied consent and free choice in which it is assumed that in choosing to work for an employer, the employee consents to its practices.* It is assumed that employees are free to work somewhere else if they are not happy with the work conditions. Yet this is often a specious choice, if all employers in an area follow the same practices or other equivalent work is not available.

(4) *The fallacy that machine generated facts speak for themselves and are necessarily more valid, reliable, and neutral than human generated facts.* But information is not the same thing as knowledge, nor are facts automatically equivalent to wisdom. Humans design the machines. Machine generated data must still be interpreted and applied by a human—who may be biased or unfair. The seemingly "objective" quality of indicators can be a legitimacy mask serving disciplinary actions actually taken on other grounds. The machine offers no guarantee of equal treatment. On the average it is likely easier to fool a machine than a human observer. Data can not be understood apart from its context. As poignant testimony of the victims of monitoring make clear, there are many extenuating circumstances e. g., someone can be late to work because of weather or family emergencies, a person may exceed the average number of restroom trips because of an illness, a telephone operator dealing with the foreign born may exceed the time quota allotted for such transactions etc. Do we really wish a society in which machines, lacking in interpretive ability, compassion, and imagination have such power over individuals? A point related to the "acontexual" nature of much monitoring data is that it may distort the final product as noted in the next fallacy.

(5) *The fallacy of confusing quantity with quality and what can be easily measured with what is important.* In emphasizing "how many" and "how fast," it is easy to lose sight of "how well." A frequent criticism of monitoring is that in mechanically focusing on simple indicators (e.g., time spent on a case, number of cases or units processed, amount of time spent at a desk or logged into a computer), the goal may be forgotten. The performance indicator may become an end in itself. Such a system may distort productivity by creating incentives to meet the indicators, rather than to produce or offer a quality product. When the means substitute for the end, both the conscientious worker and the recipient of the product or service is hurt. The rigid application of narrow quantitative measures may lessen creativity and risktaking. Such a focus can also lessen the perceived need for, and skills of managers who fall back on automated answers without having to use their judgment about overall performance, account for their supervisory behavior, or help workers to grow in the job.

(6) *The fallacy of assuming that people are best controlled through deception and the creation of uncertainty not telling them that they are monitored, or when they will be monitored* (while the means are technical in this instance, this fallacy goes far beyond work monitoring). In fact the theory of secret electronic monitoring is likely to do exactly the opposite of what its proponents claim. There are many examples (and adequate theory) to predict that intensive and unpredictable monitoring will backfire more frequently than its opposite. It treats workers as unreliable children who must always stand in fear of whether or not someone is watching them. This is not an adequate mechanism for inducing good behavior. The mere fact that a technology makes it possible to do something (such as secretly monitor) does not mean that it is the right thing to do. One of the unrecognized positive aspects of having a supervisor walk behind and monitor a person is that it introduced a degree of accountability to the watcher as well the watched. With unseen and secret monitoring some of the latter is lost. The work place becomes even more unequal.

It is true of both the research literature and democratic theory that commitment, rather than deception or coercion, is the ideal manner of obtaining the desired behavior. We might even wonder whether unrestricted monitoring isn't part of a foreign counter-intelligence plot designed to make the American economy less productive. If one wanted to design a system for hurting American business and industry he or she would be hard pressed to do better than to argue for some of the worst examples of unrestricted electronic monitoring with their documented negative impact on productivity, costs, employee health and consumer service.

D. SOME PRINCIPLES FOR DEVELOPING PROTECTION FROM UNWARRANTED ELECTRONIC SURVEILLANCE

An antidote to having to always react negatively (and after-the-fact) to many of the above fallacies is to develop positive, affirming principles. As we approach one technological surprise after another, it is important that our response not be *ad hoc*, or based only on the characteristics of the technology (e.g., the Supreme Court holding that the interception of cordless phone communications or baby monitors is legal, while the interception of corded phone conversations is illegal) or on the type

of information (e.g., the protection of video rental records but not most other kinds of consumer transactions). Nor should it be based simply on the power the contending parties can mobilize on behalf of an issue. Protection should be based on principles and not on the attributes or power of the technology.

There fortunately is much room in our democracy for discussion of values and rights and for their evolution. People of good will may disagree on the relative importance of particular principles and on how they should be weighed. However this does not negate the importance of searching for principles on which laws and policies can be based.

A nice beginning in this regard is the Code of Fair Information Practices developed in 1973 for the U.S. Department of Health, Education & Welfare. The Code involves five principles:

—There must be no personal data record-keeping whose very existence is secret (principle of informed subjects).
—There must be a way for a person to find out what information about the person is in a record and how it is used (principle of data inspection).
—There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent (principle of consistent usage).
—There must be a way for a person to correct or amend a record of identifiable information about the person (principle of correction).
—Any organization creating, maintaining, using, or dissementating records of identifiable personal data must assure the reliability of the data for their intended use and must take precaution to prevent misuses of the data (principle of relevance).

Some other important principles particularly relevant to the work monitoring context include:

(1) a principle of co-determination so that in a work context those subject to an information extraction technology have some involvement in setting the conditions under which it is used;

(2) a principle of minimization such that only information that is pertinent to the task at hand is gathered;

(3) a related principle of validity such that there are reasonable grounds for having confidence in the accuracy and worth of the information collected;

(4) a principle of timeliness such that data are expected to be current and information which is no longer timely should be destroyed;

(5) a principle of data security and confidentiality such that the data is protected and available only for the intended purposes (in a commercial context this is related to a principle of joint ownership of transactional data such that both parties to a data creating transaction must agree to any subsequent use of the data and must share in any gains from its sale);

(6) a principle of human review such that electronically generated surveillance does not automatically lead to important decisions involving the subject without a human reviewing and interpreting the data;

(7) a principle of redress such that those subject to privacy invasions have adequate mechanisms for discovering and being compensated for violations;

(8) a safety net or equity principle such that a minimum threshold of privacy is available to all; and

(9) a principle of consistency such that broad ideals rather the specific characteristics of a technology determine privacy protection.

Fortunately most of the above principles are contained in this legislation, either explicitly or implicitly. I would, however, suggest adding to Sec. 5 Privacy Protections (p. 5), a clause (C) regarding the principle of validity. There must be adequate grounds for having faith in the measure (even if what it purports to measure is in fact relevant as required under Sec. 5(a). Measures may create false negative or false positives. Monitoring systems are hardly fool-proof in either mechanical or human terms. Due process requires confidence in the validity of a measure. The 1988 Employee Polygraph Protection Act which prohibits use of the polygraph in private sector employment contexts is an expression of this important concern over validity.

E. EQUITY AND THE WORKPLACE: EXTENDING MONITORING UPWARD

In the conventional view monitoring is seen only as a way to extend managerial control and not as a way to democratize the work place. In the American context where technology is generally designed and used only by management, it is likely to

increase workplace inequality. Given this imbalance an important public policy concern ought to be insuring that technology does not further exacerbate workplace inequality. This legislation is important in that regard. But technology could also be applied more equitably in the workplace by extending monitoring upward.

Advcoates of monitoring point to a number of benefits such as (1) increased productivity (2) accountability and deterrence as a result of the visible documentary record (3) "just desserts" regarding rewards and punishments (4) the protection of consumers and (5) avoidance of lawsuits (6) the protection of employees from unfair accusations and (7) job improvement as a result of feedback. Advocates of secret monitoring also advance claims such as catching violators in the act or deterring them, since they never know when they might be watched.

If in fact management believes this, then it would seem very reasonable to apply the same monitoring ideology and technologies to managers and higher level executives. In fact the case for monitoring them is much stronger than for monitoring those lower in the hierarchy, since if the former are performing inadequately or illegally much greater damage can be done—employees stand to lose their jobs and stockholders their investments if the company fails, not to mention the diminished service quality for consumers and liability issues. We might even adopt a principle that holds that the more central the function of a position and the greater the costs from its performing poorly, the greater should be the degree of monitoring.

If management is sometimes incapable of watching itself (as is certainly the case in some sectors given recent business scandals in banking, insurance and defense contracting) then why not have monitoring units made up of workers, stock holders, consumers and even government regulators who use the latest technical developments to carefully monitor managers? Imagine what could be accomplished if a full audio and visual record of all the behavior of senior executives and managers was available, as well as any entries into company computers. If weaknesses in performance are found, procedures are violated and quotas not met, they need not be fired—through counseling and retraining an effort should be made to deal with the problem.

Great things might be accomplished with respect to productivity, profits, customer service and conformity with the law and regulations (e.g. the prevention of leaks, price fixing, and corruption) if electronic monitoring was spread throughout the organization. Of course there would have to be fair warning and compliance with legislation such as this. The credibility of management advocates of monitoring increases to the extent that they are willing to apply the same technologies to themselves.

I was raised in Hollywood, California and one of my most vivid childhood memories is seeing the film *The Wizard of Oz.* I was terrified by the power of the Wizard. The fact that he was unseen made it possible to conjure up images of a truly ferocious entity who might be anywhere and remotely cause anything to happen. The lightening and thunder he controlled and his deep and authoritative commands were very intimidating.

But as you may recall at the end of the film the little dog Toto pulls the curtain away and the "Wizard" is revealed to be an elderly and frail man. At once we hear him say "pay no attention to the little man behind the curtain with the microphone in his hand. The great Oz has spoken." But if the United States is to remain a decent and productive society in which technology is put in the service of its citizens, we must pay attention to the men and women behind the electronic curtain—and not only those in front of it. The Privacy for Consumers and Workers Act is important because it helps us do that.

Should you have additional comments or questions I would be pleased to respond.

APPENDIX TO TESTIMONY OF GARY T. MARX

"Raising Your Hand Just Won't Do," *Los Angeles Times,* April 1, 1987.

"The Case of the Omniscient Organization," *Harvard Business Review,* March-April, 1990.

"Monitoring on the Job: How to Protect Privacy Without Destroying Privacy" with S. Sherizen, *Technology Review,* Nov. 1986.

"The Company is Watching You Everywhere," *New York Times,* Feb. 15, 1987.

"Bosses Should Nix Job In-scent-tives," *Newsday,* July 6, 1990.

Los Angeles Times Wednesday, April 1, 1987/Part II

Raising Your Hand Just Won't Do

By GARY T. MARX

As part of a research project on productivity, I recently came across the following innovative policy just adopted by a major corporation. It might serve as a model for other companies wrestling with this problem.

TO: ALL EMPLOYEES
FROM: EMPLOYEE RELATIONS DEPARTMENT
SUBJECT: RESTROOM TRIP POLICY (RTP)

An internal audit of employee restroom time (ERT) has found that this company significantly exceeds the national ERT standard recommended by the President's Commission on Productivity and Waste. At the same time, some employees complained about being unfairly singled out for ERT monitoring. Technical Division (TD) has developed an accounting and control system that will solve both problems.

Effective 1 April 1987, a Restroom Trip Policy (RTP) is established.

A Restroom Trip Bank (RTB) will be created for each employee. On the first day of each month employees will receive a Restroom Trip Credit (RTC) of 40. The previous policy of unlimited trips is abolished.

Restroom access will be controlled by a computer-linked voice-print recognition system. Within the next two weeks, each employee must provide two voice prints (one normal, one under stress) to Personnel. To facilitate familiarity with the system, voice-print recognition stations will be operational but not restrictive during the month of April.

Should an employee's RTB balance reach zero, restroom doors will not unlock for his/her voice until the first working day of the following month.

Restroom stalls have been equipped with timed tissue-roll retraction and automatic flushing and door-opening capability. To help employees maximize their time, a simulated voice will announce elapsed ERT up to 3 minutes. A 30-second warning buzzer will then sound. At the end of the 30 seconds the roll of tissue will retract, the toilet will flush and the stall door will open. Employees may choose whether they wish to hear a male or female "voice." A bilingual capability is being developed, but is not yet on-line.

To prevent unauthorized access (e.g., sneaking in behind someone with an RTB surplus, or use of a tape-recorded voice), video cameras in the corridor will record those seeking access to the restroom. However, consistent with the company's policy of respecting the privacy of its employees, cameras will not be operative within the restroom itself.

An additional advantage of the system is its capability for automatic urine analysis (AUA). This permits drug-testing without the demeaning presence of an observer and without risk of human error in switching samples. The restrooms and associated plumbing are the property of the company. Legal Services has advised that there are no privacy rights over voluntarily discarded garbage and other like materials.

In keeping with our concern for employee privacy, participation in AUA is strictly voluntary. But employees who choose to participate will be eligible for attractive prizes in recognition of their support for the company's policy of a drug-free workplace.

Management recognizes that from time to time employees may have a legitimate need to use the restroom. But employees must also recognize that their jobs depend on this company's staying competitive in a global economy. These conflicting interests should be weighed, but certainly not balanced. The company remains strongly committed to finding technical solutions to management problems. We continue to believe that machines are fairer and more reliable than managers. We also believe that our trusted employees will do the right thing when given no other choice.

Gary T. Marx, a sociology professor at MIT, is engaged in research on the monitoring of work and workers.

dignities of random testing or the presence of an observer.

The quality environment

Drawing on SciexPlan's research, our company believes that the physical environment is also important to wellness and productivity. Fragrant aromas such as evergreen may reduce stress; the smell of lemon and jasmine can have a rejuvenating effect. These scents are introduced to all work spaces through the air-conditioning and heating systems. Scents are changed seasonally.

Music is not only enjoyable to listen to but can also affect productivity. We continually experiment with the impact of different styles of music on an office's or plant's aggregate output. Since psychologists have taught us that the most serious threat to safety and productivity is stress, we use subliminal messages in music such as "safety pays," "work rapidly but carefully," and "this company cares." Personal computers deliver visual subliminals such as "my world is calm" or "we're all on the same team."

At the start of each month, employees are advised of message content. Those who don't want a message on their computers may request that none be transmitted—no questions asked. On the whole, employees who participate in the program feel noticeably more positive about their work. Employees may borrow from our library any one of hundreds of subliminal tapes, including those that help the listener improve memory, reduce stress, relax, lose weight, be guilt-free, improve self-confidence, defeat discouragement, and sleep more soundly.

On the advice of SciexPlan's dieticians, the company cafeteria and dining room serve only fresh, wholesome food prepared without salt, sugar, or cholesterol-producing substances. Sugar- and caffeine-based, high-energy snacks and beverages are available during breaks, at no cost to employees.

Work monitoring

Monitoring system performance is our business. The same technologies that keep engines running at peak efficiency can keep the companies that make engine components running efficiently too. That is the double excitement of the information revolution.

At DS, we access more than 200 criteria to assess productivity of plant employees and data-entry personnel. These criteria include such things as the quantity of keystroke activity, the number of errors and corrections made, the pressure on the assembly tool, the speed of work, and time away from the job. Reasonable productivity standards have been established. We are proud to say that, with a younger work force, these standards keep going up, and the incentive pay of employees who exceed standards is rising proportionately.

Our work units are divided into teams. The best motivator to work hard is the high standards of one's peers. Teams, not individuals, earn prizes and bonuses. Winning teams have the satisfaction of knowing they are doing more than their share. Computer screens abound with productivity updates, encouraging employees to note where their teams stand and how productive individuals have been for the hour, week, and month. Computers send congratulatory messages such as "you are working 10% faster than the norm" or messages of concern such as "you are lowering the team average."

Community morale

There is no community without honesty. Any community must take reasonable precautions to protect itself from dishonesty. Just as we inspect the briefcases and purses of visitors exiting our R&D division, the company reserves the right to call up and inspect without notice all data files and observe work-in-progress currently displayed on employees' screens. One random search discovered an employee using the company computer to send out a curriculum vitae seeking employment elsewhere. In another, an employee was running a football pool.

Some companies try to prevent private phone calls on company time by invading their employees' privacy. At DS, encroachments on employees' privacy are obviated by telecommunications programs that block inappropriate numbers (dial-a-joke, dial-a-prayer) and unwanted incoming calls. In addition, an exact record of all dialing behavior is recorded, as is the number from which calls are received. We want our employees to feel protected against any invalid claims against them.

Video and audio surveillance too protects employees from intruders in hallways, parking lots, lounges, and work areas. Vigilance is invaluable in protecting our community from illegal behavior or actions that violate our safety and high commitment to excellence. All employees, including managers, check in and out of various workstations—including the parking lot, main entrance, elevator, floors, office, and even the bathroom—by means of an electronic entry card. In one case, this surveillance probably saved the life of an employee who had a heart attack in the parking lot: when he failed to check into the next workstation after five minutes, security personnel were sent to investigate.

Beyond isolation

Our program takes advantage of the most advanced telecommunications equipment to bind employees to one another and to the company. DS vehicles are equipped with onboard computers using satellite transponders. This offers a tracking service and additional two-way communication. It helps our customers keep inventories down and helps prevent hijacking, car theft, and improper use of the vehicles. Drivers save time since engines are checked electronically. They also drive more safely, and vehicles are better maintained since speed, gear shifts, and idling time are measured.

In addition to locator and paging devices, all managers are given fax machines and personal computers for their homes. These are connected at all times. Cellular telephones are provided to selected employees who commute for more than half an hour or for use while traveling.

Instant communication is vital in today's international economy. The global market does not function only

from 9 to 5. Modern technology can greatly increase productivity by ensuring instant access and communication. Periodic disruptions to vacations or sleep are a small price to pay for the tremendous gains to be won in worldwide competition. DS employees share in these gains.

Great companies have always unleashed the power of new technology for the social welfare, even in the face of criticism. During the first industrial revolution, such beloved novelists as Charles Dickens sincerely opposed the strictures of mass production. In time, however, most of the employees who benefited from the wealth created by new factories and machines came to take progress for granted and preferred the modern factory to traditional craft methods. Today we are living through a Second Industrial Revolution, driven by the computer.

Advanced work-support technology is democratic, effective, and antihierarchical. DS's balance sheet and the long waiting list of prospective employees indicate how the new program has helped everybody win. To recall the phrase of journalist Lincoln Steffens, "We have been over into the future, and it works." We are a company of the twenty-first century.

HBR's cases are derived from the experiences of real companies and real people. As written, they are hypothetical, and the names used are fictitious.

dignities of random testing or the presence of an observer.

The quality environment

Drawing on SciexPlan's research, our company believes that the physical environment is also important to wellness and productivity. Fragrant aromas such as evergreen may reduce stress; the smell of lemon and jasmine can have a rejuvenating effect. These scents are introduced to all work spaces through the air-conditioning and heating systems. Scents are changed seasonally.

Music is not only enjoyable to listen to but can also affect productivity. We continually experiment with the impact of different styles of music on an office's or plant's aggregate output. Since psychologists have taught us that the most serious threat to safety and productivity is stress, we use subliminal messages in music such as "safety pays," "work rapidly but carefully," and "this company cares." Personal computers deliver visual subliminals such as "my world is calm" or "we're all on the same team."

At the start of each month, employees are advised of message content. Those who don't want a message on their computers may request that none be transmitted – no questions asked. On the whole, employees who participate in the program feel noticeably more positive about their work. Employees may borrow from our library any one of hundreds of subliminal tapes, including those that help the listener improve memory, reduce stress, relax, lose weight, be guilt-free, improve self-confidence, defeat discouragement, and sleep more soundly.

On the advice of SciexPlan's dieticians, the company cafeteria and dining room serve only fresh, wholesome food prepared without salt, sugar, or cholesterol-producing substances. Sugar- and caffeine-based, high-energy snacks and beverages are available during breaks, at no cost to employees.

Work monitoring

Monitoring system performance is our business. The same technologies that keep engines running at peak efficiency can keep the companies that make engine components running efficiently too. That is the double excitement of the information revolution.

At DS, we access more than 200 criteria to assess productivity of plant employees and data-entry personnel. These criteria include such things as the quantity of keystroke activity, the number of errors and corrections made, the pressure on the assembly tool, the speed of work, and time away from the job. Reasonable productivity standards have been established. We are proud to say that, with a younger work force, these standards keep going up, and the incentive pay of employees who exceed standards is rising proportionately.

Our work units are divided into teams. The best motivator to work hard is the high standards of one's peers. Teams, not individuals, earn prizes and bonuses. Winning teams have the satisfaction of knowing they are doing more than their share. Computer screens abound with productivity updates, encouraging employees to note where their teams stand and how productive individuals have been for the hour, week, and month. Computers send congratulatory messages such as "you are working 10% faster than the norm" or messages of concern such as "you are lowering the team average."

Community morale

There is no community without honesty. Any community must take reasonable precautions to protect itself from dishonesty. Just as we inspect the briefcases and purses of visitors exiting our R&D division, the company reserves the right to call up and inspect without notice all data files and observe work-in-progress currently displayed on employees' screens. One random search discovered an employee using the company computer to send out a curriculum vitae seeking employment elsewhere. In another, an employee was running a football pool.

Some companies try to prevent private phone calls on company time by invading their employees' privacy. At DS, encroachments on employees' privacy are obviated by telecommunications programs that block inappropriate numbers (dial-a-joke, dial-a-prayer) and unwanted incoming calls. In addition, an exact record of all dialing behavior is recorded, as is the number from which calls are received. We want our employees to feel protected against any invalid claims against them.

Video and audio surveillance too protects employees from intruders in hallways, parking lots, lounges, and work areas. Vigilance is invaluable in protecting our community from illegal behavior or actions that violate our safety and high commitment to excellence. All employees, including managers, check in and out of various workstations – including the parking lot, main entrance, elevator, floors, office, and even the bathroom – by means of an electronic entry card. In one case, this surveillance probably saved the life of an employee who had a heart attack in the parking lot: when he failed to check into the next workstation after five minutes, security personnel were sent to investigate.

Beyond isolation

Our program takes advantage of the most advanced telecommunications equipment to bind employees to one another and to the company. DS vehicles are equipped with onboard computers using satellite transponders. This offers a tracking service and additional two-way communication. It helps our customers keep inventories down and helps prevent hijacking, car theft, and improper use of the vehicles. Drivers save time since engines are checked electronically. They also drive more safely, and vehicles are better maintained since speed, gear shifts, and idling time are measured.

In addition to locator and paging devices, all managers are given fax machines and personal computers for their homes. These are connected at all times. Cellular telephones are provided to selected employees who commute for more than half an hour or for use while traveling.

Instant communication is vital in today's international economy. The global market does not function only

THE NEW YORK TIMES, SUNDAY, FEBRUARY 15, 1987

The Company Is Watching You Everywhere

By Gary T. Marx

CAMBRIDGE, Mass.

The USG Acoustical Products Company, based in Chicago, recently announced that employees at any of its nine manufacturing plants who smoke, whether at work or at home, might soon be out of a job unless they quit smoking. After a grace period of several months, the company said it would monitor employee health using a test that measures lung capacity, and any employees still believed to be smoking could be fired.

The company's actions appear to be in keeping with the spirit of advice given by Attorney General Edwin Meese 3d, who told corporate executives recently that management should "take its responsibility for surveillance" against drugs into locker rooms, parking lots and even nearby taverns.

Gary T. Marx, professor of sociology at the Massachusetts Institute of Technology, has just finished a book on undercover police investigations.

These efforts are part of a broad shift in the nature of monitoring of workers by employers. As technological methods of surveillance become more powerful and less expensive, and as the social climate becomes more receptive, increased emphasis is being placed on monitoring workers, even when they are away from work, and the distinction between on- and off-duty behavior is narrowed.

Privacy historically has been protected, partly because data collection was limited to what the unaided senses could detect. Today's surveillance technologies easily go further. Monitoring of employees is no longer restricted to a bounded work setting, such as a factory or an office. Now electronic leashes track the activities of delivery and repair people who work in the field far from a central office. (Ironically, it was because of the greater freedom these jobs afford that many people have been drawn to them in the past.)

A small computer — aptly named Tripmaster — installed on the dashboard of a truck can record speed, gear shifts, how long the truck idles and how long a driver stops for lunch or a coffee break. Another device can track vehicle location via satellite.

Even within large industrial or office complexes, an employee's whereabouts can be determined at all times. With the use of card key systems, the individual must check into and out of various work stations — including the parking lot, main entrance, a particular floor, a given office, a computer terminal and, in some settings, even the bathroom.

Video and audio surveillance, once restricted to high security areas, are increasingly found throughout work settings. They are indiscriminate, catching whatever comes within their purview, whether work related or not.

This was sadly discovered by two workers who left a factory as their shift ended, engaged in a heated discussion. A fight ensued and a video camera in the parking lot recorded it. They were fired. The employees filed a lawsuit, arguing that their activity outside the factory gate was a private issue, no matter how irrefutable the company's "evidence." A judge later ordered them reinstated.

Union grievances have been filed over the use of electronic surveillance in employee lounges and bathrooms. In one case, the introduction of new electronic surveillance occurred during a union organizing drive.

Major changes are occurring in the monitoring of employee telephone communications as well. In most work settings, private use of telephones has been tolerated, much as the taking home of pencils. But with the development of a technique called station message detail recording, this is changing.

Extensive detail can easily be captured on phone usage — even to other extensions in the same building. Incoming calls can also be tracked.

The number of workers engaged in "telecommuting" (using computers and telecommunications at home) is also increasing. Interchanges with a central office serve to deliver a work product and also to monitor work. In such situations, it is difficult to determine where the factory or office stops and the home begins.

One program permits managers to observe on their own screen all input entered by an employee from his home and all output from the central computer to the user's terminal. Other programs are available to send subliminal messages or statements, such as "Work faster."

From management's perspective, monitoring practices are generally seen as benign or even beneficial. They help contain costs, enhance security, improve productivity and service, and equitably allocate wards and penalties. Yet they also backfire.

Electronic sweatshops are no more appealing than the other kind. One manufacturing firm found that productivity declined and absenteeism, stress and turnover increased after comprehensive monitoring system was installed.

Just because something can be done does not mean that it should be done. The precedent, once established, can lead to other forms of monitoring, such as watching what overweight people eat, tracing spending patterns of those chronically in debt or tracking employees who engage in high-risk sports. Once this is widely accepted, surveillance of religious or political beliefs could be next.

Our heterogeneous society and free-market economy place a much higher value on separating the personal and economic realms than is the case with more corporatist states, such as Japan. The company town was distasteful, partly because its control extended far beyond the factory floor. It would be tragic if competitive and moralistic pressures lead to its reinvention through the use of electronic, biological or chemical surveillance.

Powerful new monitoring technologies can be used to improve workplace security, but they also threaten employee privacy rights.

MONITORING ON THE JOB

How to Protect Privacy as Well as Property

A LARGE manufacturing company hid microphones in the bathrooms of one of its plants in an effort to ferret out drug sales at work. The microphones were accidentally discovered, and the local union complained, claiming violation of a basic privacy right. Management defended the action as part of a program to eliminate drug use at work.

A bank conducted a random check of an employee's microcomputer and found a file of personal letters and a program for preparing income tax forms. The employee was warned to use the company's computer only for company business. The employee felt that her privacy had been invaded: it was as if the company had looked in her desk or purse and told her what could and could not be there.

Two workers left a factory as their shift ended, engaged in a heated discussion. A fist fight ensued, and a video camera designed to protect the company's parking lot recorded the fight. The employees were later fired. They protested that their activity outside factory gates was a private matter. A judge agreed and ordered that they be rehired.

The monitoring of workers is hardly a new phenomenon. Indeed, it has always been the responsibility of supervisors to watch workers. From the very beginning, factory systems were designed to facilitate managerial control. With the rise of mass production and the spread of the "scientific management" ideas of Frederick Taylor, jobs were divided into their smallest components. Time and motion studies were done to establish work standards and quotas. However, even then monitoring was essentially personal. It relied on individual supervisors, and

BY GARY T. MARX AND SANFORD SHERIZEN

ILLUSTRATIONS: FRED LYNCH

workers were likely to know when they were being watched.

In many ways, contemporary monitoring is a continuation of Taylorism. But new developments in electronic technology are taking that ethos to new heights (or lows, depending upon your point of view). The monitoring of employees is increasingly being done by machines. Much more is being monitored, and the monitoring has expanded from the production line to the office.

People may not know they are being watched. Furthermore, monitoring is no longer restricted to a bounded work setting such as a factory or an office. It can be done anytime, day or night, and from a location far removed from the actual work setting. Thus, an employee using a company computer at home can be observed, and a simple electronic transmitter can monitor the movement of people and vehicles far from the central office. Traditional social and legal protections are not as clearly applicable.

U.S. managers are under increasing pressure to monitor and improve productivity. Many companies also share a growing concern about product security and employee theft. Manufacturing processes and electronic systems for transmitting data and transferring funds are far more complex than they used to be, increasing the potential for costly abuses and errors. Rising concern over drug use at work, AIDS, and escalating health insurance costs also exerts pressure on managers to conduct more intensive screening and monitoring.

As a result, the concept of privacy itself is changing. In the name of improving company security and enhancing worker productivity, intrusions that would have been questioned or rejected in the past are now being accepted. The boundaries between acceptable and unacceptable intrusions are less clearly drawn. Where is the line between on- and off-duty behavior? When does the factory or office stop and the home begin? In the future, we may even have to confront questions about the right to control brainwaves and other biometric indicators thought to be relevant to work.

American companies today are at a crossroads. They can use new electronic technologies to increase their control over worker behavior and reinforce traditional patterns of nonparticipatory management. But such efforts will erode individual rights to privacy and may cause psychological stress and reduce productivity. Fortunately, companies can use the new monitoring technologies in a restricted fashion, recognizing that just because an intrusive form of monitoring can be done does not mean it *should* be done. With employee participation in setting standards and fair guidelines, some monitoring can even enhance privacy, security, and productivity.

GARY T. MARX is professor of sociology in the Department of Urban Studies and Planning at M.I.T. He has just finished a book for the Twentieth Century Fund on covert investigations. SANFORD SHERIZEN, a criminologist, is a computer-security expert based in Natick, Mass. He helps companies and government agencies develop information security programs. The authors have prepared reports on this and similar topics for the congressional Office of Technology Assessment.

The Value of Privacy

Privacy is not a simple concept with only one meaning. It embodies a variety of meanings and expectations. For instance, most Americans expect that an individual's behavior will not be observed, moni-

Just because an intrusive form of monitoring can be done does not mean it should be done.

tored, or recorded without that person's consent. They expect not to have to divulge personal information that is not directly relevant to the issue at hand. And they expect that the information they do divulge will be treated confidentially and not used in unexpected ways. Laws and administrative rules often tend to support these views.

But why is privacy so important in the first place? Privacy is an essential component of individual autonomy and dignity. Our sense of liberty is partly defined by the ability to control our own lives—whether this be the kind of work we undertake, who we choose to associate with, where we live, the kind of religious and political beliefs we hold, or the information we wish to divulge about ourselves.

Control over personal information is particularly important for our sense of self. When an individual's room, pocketbook, or body can be searched at will, when conversations and even thoughts are available for instant inspection by outsiders, openness and honesty lose their value. Distrust becomes institutionalized and an important and even sacred element of the social bond is damaged.

In practice, of course, privacy is not easy to protect. The privacy rights of different individuals or groups sometimes conflict. For instance, an employee's right to keep personal certain information about his or her health conflicts with an employer's interest in knowing about health conditions that may affect performance and medical insurance costs. An employee's right to know about hazardous conditions at work may conflict with an employer's right to protect proprietary information.

The issue is also complicated by the fact that privacy rights depend heavily on context. Intrusive behavior considered acceptable on the job is not always acceptable off-duty. Police wiretapping of suspected drug dealers with a warrant is one thing; employers wiretapping employee telephone calls is quite another. A supervisor watching employees on an assembly line is not likely to be questioned. But the use of a hidden camera and bug to gather equivalent data is. There are few, if any, forms of intrusive behavior that all people would agree are always illegitimate.

The Maximum-Security Workplace?

In a less technological age, our expectations about privacy were defined partly by what the unaided senses—sight, sound, smell, taste, and touch—were capable of detecting. The traditional physical boundaries of the workplace offered other limits to the gathering of information. Today's monitoring technologies easily transcend traditional barriers to data collection. Since monitoring is increasingly done automatically by machines, supervisors are no longer limited to what they can immediately observe. Nor are workers always able to know when they are being monitored. Phone systems designed as intercoms or paging devices permit managers to listen to conversations in other offices without being detected. Even in the few cases when union contracts or state laws require that notice of monitoring be given, workers will not necessarily know when the monitoring is being done.

Compare, for example, a video camera or video recorder with the traditional supervisor who occasionally walks by. Workers usually know when the supervisor is present. They also know that the monitoring is episodic—the supervisor can't be everywhere all the time. In contrast, camera and recorder are omnipresent and tireless; the worker can never be sure whether they are in operation or if their results will be reviewed. Moreover, in the past, the economics of monitoring tended to work against intensive mass surveillance. But technological breakthroughs have greatly reduced the cost of monitoring. Some companies are even using satellite technology to pinpoint the location of their trucks on a television screen.

Furthermore, monitoring devices with built-in microprocessors can now be made very small. This means that they can be placed in hidden locations and activated from distant places. By installing a tiny pinhole lens and video on the plane, for instance, it is possible for people on the ground to see and hear all activity on an aircraft up to 200 miles away. The market for such security products is expected to grow from $774 million in 1985 to $2.1 billion by 1992.

Workers increasingly participate in their own monitoring—even though such participation may be unwilling or unconscious. Technical devices automatically record data that workers generate: they capture information from the workers' voices or movements such as keystrokes or assembly-line actions, and they measure workers' effectiveness by monitoring security and quality-control systems. In data-processing jobs, for instance, the devices mon-

52-658 - 92 - 3

The camera and recorder are omnipresent and tireless; the worker can never be sure whether they are in operation.

itor the number of errors and corrections made, the speed of work, and time away from the desk. One Bank of America vice-president, commenting upon the 200 criteria he uses to assess productivity among workers in his credit-card division, notes: "I measure everything that moves."

The workers most likely to be monitored are those who use computers for telecommunications, word processing, programming, and service contacts. Companies such as AT&T, United Airlines, Equitable Life Insurance, and American Express use sophisticated devices to regularly monitor their employees.

Take, for instance, the development of a technique called station message detail recording (SMDR). Telephone systems often have built-in SMDR features that record on what telephone each call is made, what user identification code and extension is used, where the call goes, what time it is made, and how long it lasts. SMDR systems generate detailed reports that management can use for planning budgets, allocating and controlling costs, and monitoring activities. Among the functions that can be monitored are toll calls made after official business hours and telephone use during lunch hours. Employees who use the telephone to make personal calls can readily be identified, as can employees who leak information to the press or to competitors. Calls from one extension to another within the company can also be monitored. New developments in software also make it possible to capture the content of a conversation, although this is much less frequently done.

The monitoring of telephone communication is likely to become pervasive. In 1985, 20,000 SMDR and related systems were sold in the United States, and that number is likely to grow. As one airline-company executive put it, "Communications performance monitoring is going to be one of the major computer service fields in the next 5 to 10 years."

Thanks to other advances in software, employers can monitor employees working on microcomputers from the time they log on to the time they log off. One software product now on the market allows management to document the activities of anybody using the company computer system—without the user's knowledge. With the program, marketed by Clyde Digital Systems of Provo, Utah, and called "CNTRL," managers can observe on their own screen all input entered by the employee and all output from the computer to the user's terminal as it occurs. It can also be captured in a log, "creating a certifiable record to be used for disciplinary or legal proceedings," as the company's literature promises.

Software companies have even developed programs that allow employers to tell workers how their productivity compares with that of their co-workers. One program can be used to display messages on the video display terminal such as: "You are not working as fast as the person next to you."

A report by 9 to 5, the national organization of working women, describes a program called "The Messenger" that can be called up by the VDT operator. Calming images of mountains and streams are displayed along with subliminal messages such as "My world is calm." More ominous are subliminal programs that the worker may have no knowledge or control over. One such program entitled "Subliminal Suggestions and Self-Hypnosis" permits management to send any kind of message—such as "relax," "concentrate," or "work faster"—unbeknownst to the worker. The messages pass so quickly in front of the watchers' eyes they cannot be consciously detected.

Your Retinal Pattern or Your Life

Information security is a growing priority for many companies, particularly those involved in complex electronic fund transfers or confidential communications. The ability to gain remote access to computer systems had long posed a security problem, largely because both hackers and those with much less technical knowledge have found ways to bypass traditional precautions such as passwords and special cards.

To prevent unauthorized use, security firms are now developing biometric identification products for the commercial marketplace. These are based on the sensing of individual characteristics such as fingerprints, handwriting, voice, typing rhythms, hand geometry, and the distinct patterns of people's retinas. *Personal Identification News* magazine estimates that private companies spent more than $35 million in 1985 to develop biometric products.

These products can indeed improve the ability of federal agencies and private companies to limit access to top-security data. But they are also being used as a substitute for other managerial controls and supervision. A leading hotel, for example, used retinal-pattern identification to prevent workers from

punching in one another's timecards. And a growing number of organizations ranging from Avis, Con Edison, and Equitable Life Insurance to the Universities of Tennessee and Georgia use hand geometry to identify employees.

The new technologies, of course, may bring greater equity. After all, "pre-technological" monitoring by a human supervisor sometimes meant high-handed or discriminatory treatment. Technological monitors have no favorites; all workers are treated alike. Because so many parameters of job performance can now be monitored, the total result might be a fairer system. Furthermore, monitoring can extend up as well as down the organizational hierarchy. Video cameras, card key systems required to enter a room, and computer access codes make demands on all who encounter them.

However, intrusive monitoring may conflict with workers' traditional expectations of what is fair on the job. There is, of course, no formal protection for the privilege of whispering at work or of being free from observation. But most of us feel entitled to a sense of privacy in our communications at work. The new technologies are threatening that privacy and—for some workers—making it obsolete.

The use of biologically based technologies could jeopardize people's privacy off as well as on the job. Workers have already been fired from their jobs when drug tests have revealed evidence of marijuana use, even though the drug was used at a weekend party and job performance was not in question.

When Deception Becomes the Rule

The increased use of monitoring in the workplace could well backfire. People are wonderfully ingenious at finding ways to disrupt, distort, and deceive monitors. For example, typists may hold one key down to increase the number of key strokes recorded. They can always delete the file containing the errors later. Telephone reservation agents may learn to avoid calls that add to their average case time—by either disconnecting the call or simply withholding information. And workers required to provide urine samples may add chemicals that distort the test results or even turn in someone else's urine.

Monitoring may also create more adversarial relationships in the workplace. Workers may feel violated and powerless in the face of the new monitoring technologies. The result could be low morale, reduced productivity, and destructive countermeasures. Monitoring may even increase the violations or abuses it is intended to stop. Workers may feel challenged to beat the system or react out of anger and estrangement. When people feel they are not trusted, they often adopt an attitude similar to that of some police regarding corruption: "If you've got the name, play the game." In other words, as long as everyone thinks that you will take graft, you might as well do it.

One truck driver for the Safeway Co. with 40 years of experience recalled that he used to love his job because "you were on your own—no one was looking over your shoulder. You felt like a human being." But now a small computer on the dashboard of his truck (with the apt name of Tripmaster) keeps track of speed, shifting, excessive idling and when and how long he stops for lunch or a coffee break. As a result, the driver says he will retire early. He complains, "They push you around, spy on you. There's no trust, no respect anymore."

No comprehensive information exists on how technological monitoring affects productivity, but anecdotal evidence shows that overly zealous monitoring can be counterproductive. One large Midwestern electronics company for instance, found that productivity declined and absenteeism, stress, and turnover increased after a highly touted monitoring system was installed. The company eliminated the system within the year. The employees may have reacted like the directory-assistance operator who couldn't understand why her company had started

monitoring her: "I worked all those years before monitoring. Why don't they trust me now? I will continue to be a good worker, but I won't do any more than necessary now."

Increased monitoring can breed other problems as well. The emphasis on quantity at the expense of quality may result in an inferior product. With monitoring, employers can automatically speed up the work process so it is no longer in the employees' control. Also, to the extent that electronic supervisors displace people, the potential for growth and learning on the job may be diminished. Less contact with a supervisor may mean a more impersonal, less satisfying work environment.

New types of monitoring may also disrupt understandings between labor and management. The technologies may eliminate activities that workers have traditionally taken for granted as "perks" of the job. For instance, many employees (and enlightened employers) equate the custom of keeping personal letters in an office computer with the tradition of taking home paper and pencils. Yet under the new form of monitoring, such previously "tolerated" behavior may no longer be accepted.

Surveillance also has a tendency to expand. Under the Reagan administration, government agencies have already begun monitoring their employees extensively, and further monitoring is planned. Polygraph testing, once restricted to top-secret matters of national security, is now applied to leaks to the press. In an effort to stem such leaks, some government agencies also monitor employee phone use. One new computer program even compares a list of calls with reporters' phone numbers. Concern about employee drug abuse has led President Reagan to urge drug testing of many government employees as well as employees of government contractors.

There is another reason for making sure technological monitoring in the workplace does not get out of hand: monitoring could become much more extensive in society at large. Practices developed at work can easily spill over into other areas. The new biometric forms of identification are one example. The more widespread this practice becomes in the workplace, the easier it will be to create a mandatory national ID system.

A Permanent Class of Undesirables?

Another danger is that monitoring—in the form of pre-employment screening—may help create a class of permanently unemployed and underemployed people. Because traditional records systems were inefficient, many people, particularly those who had been imprisoned, were given a second chance. In the old days, moving to a frontier town meant the opportunity to start over. But this traditional freedom may be severely constricted as credit institutions and other organizations gather comprehensive databases on U.S. citizens and sell them to other companies. The past becomes haunting: there is no second chance.

An increasing number of database companies gather and sell information to prospective employers on everything from an individual's political activism to the filing of worker-compensation claims. These companies are relatively unregulated in their use of the databases. One factory worker was fired from a new job after his employer checked with a private computer network that tracked such claims. The employee had filed two claims for minor injuries (such as a broken finger) with previous employers and had collected modest compensation.

Many companies also use written tests to screen out job applicants. The Knight-Ridder newspaper chain, which owns the *Miami Herald* and the *Philadelphia Inquirer*, routinely requires applicants for reporting positions to take a battery of written tests designed to reveal their personality traits and philosophical views.

Other forms of monitoring—such as genetic screening—could eventually be used to discriminate

Monitoring may even increase the violations or abuses it is intended to stop.

against individuals not because of their past but because of statistical expectations about their future. People who carry antibodies to the AIDS virus but have not developed the disease are already being discharged from the U.S. military and isolated or fired from other jobs. Scientific advances are making it increasingly possible to identify the genetic traits that predispose people to widespread diseases such as diabetes and heart disease.

Eventually, the work force may become divided between people thought to be good risks and others. Not only would this create an enormous waste of human resources as people are locked out of jobs for which they are otherwise qualified, but some of these people could turn to crime to support themselves. The demands on the welfare system would certainly expand.

Omnipresent monitoring will almost certainly chill political and social expression. Security and control may be enhanced but at the cost of a less creative and dynamic society. If American democracy is to be destroyed, it is unlikely to happen by sudden catastrophic events. Rather, it will occur by slow, incremental changes defined in benign terms. As Justice Louis Brandeis said, "The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding."

Using Technology to Enhance Privacy

Monitoring need not always mean invading some aspect of privacy. In some cases, technological monitoring is actually less intrusive than direct human monitoring. Electronic monitoring of hand luggage at airports eliminates the need for direct searches of passengers' purses and persons. The use of electronic markers on library books and consumer goods also makes costly and demanding physical searches unnecessary.

New technologies can also be used to reduce the need for monitoring and protect privacy. Monitoring in some ways is an admission of the potential for a system to fail. One watches because things *can* go wrong. However, work situations can be structured so that violations, abuses, and errors are less possible. Under these conditions, technological developments can enhance privacy.

For instance, data encrypted on fiber-optic telecommunications lines are clearly more secure from unauthorized use than information left in a desk drawer or file cabinet. Telephones can be designed to allow users to dial only local calls, eliminating the need to monitor for long-distance abuse.

Access keys or codes for using computers and copying machines reduce the need for visual surveillance. Before such systems were developed, supervisors had to watch who was using copying machines and in some cases resort to informers to locate abusers. Where once telephone company staff had to listen to conversations to verify the quality of connections, technical developments now make it possible to do this without listening in on voice communications.

In the future, "smart cards" containing personal data carried by everyone may eliminate the need for central databases, returning us to an earlier period when personal data were much more in the possession and control of the individual. In one inexpensive "smart card" system, laser technology is used to encode and read a wallet-sized card that contains up to 800 pages of information. The information on such cards is constitutionally protected from unauthorized use—which is not the case for records held by a third party such as a bank. However, backup copies would have to be made, creating the potential for abuse. Furthermore, if carrying such cards became mandatory, they might well seem more Orwellian than central databases.

Even technologies that have the potential to invade privacy may have positive benefits for employees. Some workers welcome close monitoring when it is tied to a system of merit pay. The permanent records from monitoring can also protect the innocent from false accusations and document violations by the guilty. Video cameras designed to prevent theft from loading areas may increase safety in adjacent parking lots. And drug screens may prevent accidents and protect the health of employees.

Establishing a Code of Ethics

Given the new technologies' wide range of advantages and disadvantages, how best can we manage their use? Companies should begin by analyzing why they want to institute monitoring. For instance, will the monitoring be a direct part of the work process, or will it be added on—a procedure apart from the work process such as a drug screen?

Most monitoring technologies can be applied in a number of ways. A video monitor can be hidden or

Monitoring is no longer restricted to a bounded work setting such as a factory or an office.

visible, operated randomly or only when a light is on. Drug testing can be based on an inexpensive and relatively unreliable test or the opposite. Drug tests, polygraphs, and other forms of inspection can be general or specific, scheduled or random.

Given the variety of instruments, uses, and contexts, sweeping generalizations about monitoring technologies are inappropriate. In general, however, privacy is best protected when monitoring is minimally intrusive, is directly relevant to job performance, and is visible—i.e., a supervisor is walking by or a video camera has a flashing red light that indicates it is on. Highly intrusive forms of checking that are not directly related to work output should be restricted to situations where there are some grounds for suspicion.

A code of ethics does exist among certain manufacturers and vendors of monitoring technology. For example, AT&T, which provides telephone companies equipment for checking phone lines, requires subscribers to agree that they will use it solely for quality control and training. AT&T also requires that employees be notified in writing that they will be subject to such monitoring.

Some firms ask employees to help establish behavioral norms at work and thus cut down on the need for monitoring. For example, some companies have instituted programs whereby, if losses from employee theft are less than the previous year, employees split the money saved. Following a widespread practice in Europe, a few U.S. companies have agreed to use work monitoring only for group, rather than individual, output.

As the new monitoring technologies become pervasive and affordable, however, misuses are bound to increase unless clear guidelines are developed. Our work in analyzing and developing information-security and privacy programs for companies and government agencies has made it clear that legislation and company policies must:

- ☐ Apply to monitoring the same protection that applies to pre-employment background checks—that is, permit only information directly relevant to the job to be collected. The burden of proof for the need to monitor should lie with the employer.
- ☐ Require employers to provide employees with advance notice of monitoring as well as appropriate mechanisms for appeal.
- ☐ Require people to verify machine-produced information before using it to evaluate employees.
- ☐ Provide workers with access to information on themselves.
- ☐ Provide mechanisms for monetary redress for employees whose rights are violated or who are victims of erroneous information generated by a monitoring system.
- ☐ Apply a "statute of limitations" on data from monitoring. The older the data, the less their potential relevance and the greater the difficulty employees have in challenging the information.

Little is known about the extent of employee monitoring in the United States and the policies that govern its use. Research by companies and government agencies could provide policymakers with a greater awareness of monitoring as a social phenomenon.

In sum, technology is neither the enemy nor the solution. More and more U.S. companies are turning to monitoring devices to increase their control over employee behavior and improve internal security. But thus far, society has paid insufficient attention to protecting individuals' rights. The U.S. government and the private sector must work together to make sure that in our haste to protect our property, we do not destroy our basic freedoms. ☐

Senator SIMON. Thank you. You got a lot of words into those 5 minutes.

Mr. Rotenberg.

Mr. ROTENBERG. Thank you, Senator.

CPSR is a national membership organization of computer scientists. We have a particular interest in privacy issues and have testified before a number of panels in support of efforts to protect privacy. We also believe strongly that in the design of computer systems, workers should be able to participate and help shape the technology that affects their lives.

I should say at the outset that CPSR does not necessarily believe computer technology undermines privacy. There is certainly the Orwellian specter of large databases containing a great deal of personal information, and we are aware of this problem, but we believe at the same time that technology can be channelled in such a way as to promote worker satisfaction, improve democratic decisionmaking, and afford basic protection for human dignity.

Thus, our interest in this legislation is in supporting an effort that we believe will advance these goals.

Let me speak briefly about three points that we think are critical to this effort. As I stated before, we believe that worker participation in the design of computer systems is a critical aspect of technological development. It has a tendency to promote greater innovation and job satisfaction. Employees should know how technology is affecting their lives, and increasingly companies are beginning to understand this. As Mr. Bahr stated earlier, Professor Hecksher at the Harvard Business School has said that good managers have no need for secret monitoring. A study of Fortune 500 companies that was performed by David Linowes, the former chair of the Privacy Protection Study Commission found that employee relations improved at both IBM and Citibank when data collection about personal information was minimized. This is the first point. Workers should play a role in the design of the technology.

The second point is that businesses that collect personal information have a responsibility to their employees to safeguard that information. From a safety viewpoint, this responsibility is no different from the employer's obligation to ensure that the staircase is secure or that the ice has been removed from the entry way.

Computer people are particularly sensitive to this problem because we know that personal information can easily be misused. As Professor Gary Marx stated a moment ago, in 1973 HEW put together a Task Force on Privacy Protection and came up with a set of principles called the Code of Fair Information Practices. These were designed to give an outline for organizations that were collecting personal information and to ensure that privacy would be protected.

Now, there are five principles here that are really the foundation for privacy protection in this country. The first one is that there should be no secret personal data recordkeeping systems. People should beware of the information that is kept about them.

They should also know how the information is being used. That's an important part of information privacy. They should have access to personal information and the opportunity to correct and amend the information if necessary.

The organization that collects the personal information also has a responsibility to ensure its accuracy, its timeliness, and also its completeness so that information that is inaccurate will not cause some person unnecessary harm.

And finally, information that is collected for one purpose should not be used for another purpose without the person's consent.

These five principles, as I said, are a critical component of the principles that undergird privacy protection not only in the United States but in many countries abroad.

My third point this afternoon is that CPSR believes computers should assist but not replace human decisionmaking, and the Europeans are particularly sensitive to this problem. Joe Weizenbaum, a professor in computer science at MIT, wrote with great force in a book called *Computer Power and Human Reason* that we should be careful not to substitute the precision that a computer system provides with the reasoning that a person can make.

Finally, Mr. Chairman, I would like to say that for the past year there has been a great deal of work taking place on the privacy front regarding recent developments in the European Community and the efforts to develop an EC-wide privacy protection policy. It is becoming increasingly apparent that the United States lacks privacy protection in certain critical areas, and the absence of this privacy protection may in the years ahead have some consequences for international trade.

I have participated in a series of meetings with the Europeans, and one of the points that they oftentimes refer to is the failure of the United States to develop a comprehensive statute for workplace privacy. For that reason and for several others, we think this is clearly a step in the right direction and are very pleased with your efforts.

[The prepared statement of Mr. Rotenberg follows:]

Prepared Testimony
and
Statement for the Record

of

Marc Rotenberg, esq.
Director, Washington Office

Computer Professionals for
Social Responsibility (CPSR)
on

S. 516
The Privacy for Consumers and Workers Act

The Subcommittee on Employment and Productivity,
Committee on Labor and Human Resources,
United States Senate

September 24, 1991

CPSR Washington Office
666 Pennsylvania Ave., SE
Washington, DC 20003
202/544-9240
rotenberg@washofc.cpsr.org

Mr. Chairman, members of the Committee, thank you for the opportunity to testify today on S. 516, the Privacy for Consumers and Workers Act. My name is Marc Rotenberg and I am the director of the Washington Office of Computer Professionals for Social Responsibility.

CPSR is a national membership organization of computer scientists. Our membership includes a Nobel laureate and four winners of the Turing Award, the highest honor in computer science. CPSR has a particular interest in privacy issues, and we have testified before several Congressional committees in support of efforts to protect privacy.[1] We also support the development of computer systems that reflect the interests of individuals in the workplace and we recently hosted the first international conference in the United States on the topic of participatory design.

With me this afternoon is David Banisar, a student at Catholic University Law School and a law clerk with CPSR. We are pleased to be here today, and thank you for convening this hearing.

Mr. Chairman, I should say at the outset that CPSR does not believe computers necessarily undermine privacy. Computer technology can both enhance and diminish privacy protection. While many people are aware of the Orwellian specter of computer databases – and we share the concern that such databases have indeed been developed – we also believe that technology may provide solutions to some privacy problems. For example, encryption

---

[1] In general, the computer profession has a strong commitment to privacy protection. For example, The Association for Computing Machinery (ACM) Code of Professional Conduct states that:

> Ethical Considerations:
>
> EC5.1 An ACM member should consider the health, privacy, and and general welfare of the public in the performance of his work.
>
> EC5.2 An ACM member, whenever dealing with data concerning individuals, shall always consider the principle of individual privacy and seek the following:
>
> To minimize the data collected;
> To limit authorized access to the data;
> To provide proper security for the data;
> To determine the required retention period of the data;
> To ensure proper disposal of the data.

makes possible the confidential exchange of information through a computer network. In the workplace, encryption would make it possible to protect the contents of messages sent between employees and remove the temptation for a supervisor to monitor the communication. There is, from a privacy viewpoint, little difference between a sealed envelope and an encrypted communication – both provide an opportunity to exchange information with a clear expectation of privacy.

Therefore, we believe that legislative solutions should focus on the underlying activity rather than a particular technology. The goal should be to encourage information practices and shape technologies consistent with a society that values human dignity and protects democratic decision-making.

There is a clear need to develop such legislation. Currently, employment data is protected in patchwork fashion. Laws varies from state to state. Some states require all public and private employers to allow employees to inspect personnel files; others provide procedures when employees dispute the information; others restrict disclosure of the information to the public. No state has passed a comprehensive law which governs confidentiality, accuracy, relevancy, and proper disclosure of employment information.

In some cases, large private companies have established good internal policies to govern employee data. Many require periodic reviews during which the employees may read their evaluations, and may enter their comments before the review is placed in the permanent employee file. However, these policies are voluntary and most middle and small companies do not have similar ones.

Most employees are obliged to provide a great deal of information about themselves. Much of this information will be verified and supplemented by the employer.

> [T]he individual may be examined by the company physician, given a battery of psychological tests, interviewed extensively, and subjected to a background investigation. After hiring, the records the employer keeps about him will again expand to accommodate attendance and payroll data, records concerning various types of benefits, performance evaluations, and much

> other information [including, we might add, medical records where the employer provides medical insurance].[2]

In 1977 the Privacy Protection Study Commission found that the essential character of the employment relationship created obstacles to enforcement of an employee's privacy rights. Many employees, for example, would be reluctant to sue an employer for failure to produce records on request. The subjective nature of employment decisions would make it difficult to link an adverse decision to detrimental facts in an employee's record. Further, an employee might well risk reprisals for raising complaints about unfair information practices. The Commission recommended employers adhere voluntarily to a detailed code for fair use of information and that a data privacy board, if formed, study this problematic area in greater depth.[3]

In 1989, only three states limited the scope of an employer's investigation of an employee or applicant. Only a handful of states limited disclosure of record information by an employer to third parties.[4] A report published that year found that employers had the capacity to retain in records "information that has no justification being in personnel records," and concluded that:

> [a] responsible employer limits data kept in personnel files, allows employees access to their own files, and limits third party access. Policies vary widely on personnel information practices. Several states have enacted measures to protect individuals, but much more is needed.[5]

There are special reasons to favor a policy that keeps employers and employees out of court where there are grievances. A lawsuit typically means the end of the employment relationship, a disruption of the employees life, and loss of productivity. Yet the advent of new information collection techniques have placed employees under new and unprecedented kinds of surveillance. Employers find it necessary to collect and retain more

---

[2] Privacy Protection Study Commission Report, p. 223.
[3] Id. at 233.
[4] D. Linowes, *Privacy in America*, p. 38.
[5] Id. at 39.

information, in greater detail, to make informed hiring, promotion, strategic, and security decisions. Improved information handling techniques allow employers to store and access large amounts of information on individual employees. Third-party vendors of information, such as credit reporting agencies, augment the information available to an employer and help to create the fine-grained "data portrait" of an individual. Decisions taken solely on the basis of one's "data profile" or "data shadow" have raised great concern in Europe where a comprehensive privacy policy is now under consideration.

In short, the employment relationship is now fraught with delicate information-privacy issues. Court remedies are inadequate and no state provides comprehensive protection.

GOALS FOR WORKPLACE PRIVACY

Mr. Chairman, CPSR believes that there are three goals that should be pursued for new technologies in the workplace. First, workers should help shape the technology that affects their lives. Second, businesses which collect personal information on their employees should uphold their responsibility to safeguard this data. Third, computers should assist but not replace human judgment in the area of employment decision-making. Let me briefly explain these three points.

First, we believe that worker participation in the design of computer systems is a critical matter of fairness. As Dr. Lucy Suchman has said, "Critical analysts of new technology have pointed to the abuse of computerization by employers who believe that company profitability can be increased by decreasing employee autonomy." And Dr. Kristen Nygaard, a professor of computer science at the Institute of Informatics in Oslo, has shown there are alternative ways to view the development of technology in the workplace.

Worker participation promotes innovation and greater job satisfaction. The design of systems begins with a full and fair understanding of management practices and management goals. Employees should know how technology is used in the workplace. Increasingly, companies are beginning to see that technology can promote greater job satisfaction. As Charles

Hacksher of the Harvard Businsess School has said, good managers have no use for secret monitoring. And a study of Fortune 500 companies, conducted by the former chairman of the Privacy Protectlon Study Commission, found that employee relations improved at IBM and at Citibank after the collection of personal information was reduced.

My second point, Mr. Chairman, is that a business that collects personal information has a duty to protect the privacy of that information. From a safety viewpoint, this responsibillty is no different from the employers' obligation to ensure that a staircase is secure or that ice has been removed from an entry way. A poorly conceived information collection system places employees at risk, and even where the employer intends no harm, employees may suffer from the unnecessary disclosure of personal information. For example, storing sensitive medical information in an on-line system creates a risk that other employees may gain access to sensitive, personal files. Employers should take care to protect records that are collected by monitoring from accidental disclosure or pilferage.

In general, businesses should follow the Code of Fair Information Practices, a set of principles developed by a government advisory committee almost twenty years that were the foundation for the Privacy Act of 1974. Briefly stated, these principles require that:

- There must be no secret personal data record-keeping systems whose very existence is secret;
- A person should know what information about the person is in a record and how it is used;
- A person should be able to correct or amend a record of identifiable information about the person;
- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data; and, most importantly,

- Any information obtained for one purpose should not be used for another purpose without the consent of the person.

Privacy experts such as David Flaherty also recommend that organizations adopt a principle of data minimization – limiting the collection of personal information to only that which is necessary.

Finally, CPSR generally believes that computers should assist but not replace human decision-making. The Europeans are particularly sensitive to this problem. As MIT computer science professor Jospeh Weizenbaum suggested in *Computer Power and Human Reason*, we should be careful not to substitute the precision that a computer system provides with the reasoning that a person makes.

With regard to all three goals, we believe that the Privacy for Consumers and Workers Act is a step in the right direction and will help curb the abuse of electronic surveillance in the workplace. Legislation is necessary because alternative mechanisms have failed to work.

SUGGESTED CHANGES

Mr. Chairman, I would like to propose changes to the legislation. These changes are primarily intended to fill certain gaps and to ensure that the purpose of the bill is achieved in practice. As a general matter, I should note that privacy legislation typically shows the first signs of wear in those provisions that allow for disclosure, such as for a "legitimate business purpose." For example, the "routine use" exception in the Privacy Act of 1974 is now considered a loophole in an otherwise fine law that permitted the development of computer matching – the practice that Congress sought to avoid. I would therefore recommend that you look closely at those provisions of the bill that allow for disclosure and determine if it might be possible to further narrow the exceptions.

1) Narrow Law Enforcement Exception

One section of the bill that should be clearly changed is the provision for disclosure of personal data to law enforcement officials. We believe that

this exception is too broad, and may make employers unwitting accomplices in the surveillance of their employees. The standard for disclosure to law enforcement officials under a privacy statute is typically much higher. For example, the Video Privacy Protection Act, which safeguards the records of video customers held by video rental store, only permits the disclosure of personally identifiable information to a law enforcement agency "pursuant to a warrant issued under the Federal Rules of Criminal Procedure, an equivalent state warrant, a grand jury subpoena, or a court order."[6]

Similarly we would recommend removing the clause that permits disclosure where "pertinent to and within the scope of, an authorized law enforcement activity." Particularly in a provision designed to protect Constitutionally protected activity, we believe that a warrant requirement is the appropriate standard. And we propose revising the section to make clearer that the exception only applies to monitoring current permissible under law. It should not provide a blanket exception for law enforcement agencies.

2) Prohibit use of SSN for ID Number

Mr. Chairman, one issue that comes up across the privacy landscape is the need to restrict the use of the Social Security Number. Businesses are increasingly using the Social Security Number as employee identifier. This is not a good practice. The problem with the use of a Social Security Number as an identifier is that it allows organizations to obtain information about individuals often without their knowledge or consent. This tends to diminish an individual's ability to control information about himself or herself and leads to the compilation of elaborate dossiers. Numbering schemes that are designed for particular businesses help promote confidentiality because they strengthen the ties between the individual and the institution and create an expectation that information which is transferred to the institution will not be used for other purposes.

We would recommend that businesses be encouraged not to use numbering schemes based on the Social Security Number. If such a

---

6 18 USC 2710(2)(C).

provision is not appropriate for the bill, perhaps the need to restrict the use of the SSN could be discussed in the committee report.

3) Include Code of Fair Information Practices

We would also suggest that the report on the legislation include the Code of Fair Information Practices and how such principles should be applied in the workplace. David Linowes, the former Chairman of the Privacy Protection Study Commission, describes in *Privacy in America* how the Code is currently applied by many American businesses. This would be useful information for organizations that are developing privacy protection policies.

4) Protection of Constitutional Freedoms

We would also suggest that the Committee report reflect a broad interpretation of First Amendment rights as applied to the workplace. As you may know, a 1983 Supreme Court decision imposed a fairly narrow interpretation of First Amendment freedoms. Without arguing whether that case was correctly decided, we believe that the opportunity for greater monitoring today than the Court was aware of when the case was decided would argue for a stronger standard.

NEED FOR LEGISLATION

Mr. Chairman, I would like to make two final points about the importance of the legislation. There is growing sentiment in Europe today that the United State has failed to provide adequate privacy protection following the rapid technological developments of the past two decades. This summer CPSR, in cooperation with the United States Privacy Council, conducted a survey of privacy law in the United States and found that there was inadequate protection for employment records. Many states have passed laws to protect these records, but the laws are inconsistent and the degrees of protection vary greatly. It is our belief that the passage of workplace privacy legislation would begin to address some of the concerns raised by the Europeans and, over the long-term, promote the development of technologies that better serve business needs.

52-658 - 92 - 4

Finally, Mr. Chairman, I would like to note that Congress has played an increasingly important role in protecting privacy. This is the lesson of privacy legislation in the 1980's. For example, as the cable industry took off in the early 1980's, concern about the privacy of subscriber information also grew. In 1984 a law was passed to ensure the protection of subscriber information.

Electronic mail, a great boon to communications, also raised concern about the security of the contents of electronic messages. The Electronic Mail Association was as worried as its customers, perhaps more so, because of the concern that a new mail service would not be very useful if privacy could not be assured. The Electronic Communications Privacy Act of 1986 responded to the need for privacy protection for this new form of communication.

And, when a nominee to the Supreme Court found that his choice of videos that he watched with his family in their home became the subject of an article in a local newspaper, Congress looked at the new technology and developed legislation to protect the rental list of video users.

The introduction of the polygraph machine raised questions about the appropriateness of government agencies, courts and private companies using an automated form of lie-detection to determine the truthfulness of a person's statement. In 1988, Congress responded with the Employee Polygraph Protection Act which prohibits most private companies from giving polygraph or lie-detector tests to current or prospective employees.

In each instance, it seems clear that Congress is ready, willing, and able to assess the privacy implications of new technologies and to adopt appropriate legislative safeguards. So, too, it should be with workplace privacy. As a recent article in the Harvard Law Review notes, the market mechanisms and common law remedies "fail to protect workers from abusive practices."[7]

---

[7] "Assessing the New Hazards of the High Technology Workplace," 104 *Harv.L.Rev.* 1898, 1916 (1991)

Senator SIMON. Thank you very, very much.

Mr. Bahr, you used a phrase in your final sentence that we have been bringing up in a lot in another hearing on a U.S. Supreme Court nominee—the right of privacy. There are those who say there is no right of privacy guaranteed by the Constitution. But the reality is the Constitution says you can't go into your home and search it without a warrant. The Constitution says you can't have troops quartered in your home.

Then the 9th Amendment was added at the suggestion of Alexander Hamilton. James Madison wrote the Constitution and wrote the Bill of Rights, and Alexander Hamilton in correspondence said if we have a Bill of Rights, some people will say these are the only rights people have. So the 9th Amendment was added, saying other rights not spelled out here are reserved to the people.

When they wrote the Constitution, they didn't have any idea we were going to be having telephones, computers, and all the kinds of things we have today, but the right of privacy that all three of you have talked about is really part of the spirit of the Constitution, in my opinion.

So I think it is one of the things that we need to safeguard in this country, and part of the aim of this bill is to safeguard that very fundamental right.

I'd like to ask all three of you this next question. We also want to have a country that is productive, and one of the first three witnesses said that having this kind of secret monitoring is like having someone stand over your shoulder when you are working. I suppose we have all had that experience of someone standing behind us while we are typing something or writing something, and you have that uneasy feeling. For example, the reporters over there, you worry about somebody stealing your story while you are working.

Does that inhibit productivity to have that uneasy feeling, Mr. Bahr?

Mr. BAHR. Mr. Chairman, one of the buzz words that we've been dealing with for a number of years, certainly within the beltway, is "competitiveness." Many things go into making an enterprise competitive. One aspect is the concept of employee involvement, participative management. How, on the one hand, can you say that you recognize that the front line workers know more about the production end of the business than we used to give them credit for—I'm talking about management—and depend on them to restructure their work, to have more input into the productive mechanisms of the company, and then turn around and secretly monitor them. What kind of signal does that send out? I think it is quite contradictory.

Yet progressive management is doing both. How far does this go. Because of a loophole or an omission in the Omnibus Crime Act, we are now in Federal court in Atlanta and had to file a civil suit against a major company, Northern Telecom, which we learned just a couple of years ago in connection with an organizing campaign at a factory in Nashville bugged the entire plant. There were secret bugs in the sprinkler systems, in the lavatories, in the public pay phone. Those bugs remained from 1976 to 1984. We have those

tapes; they are in the court's protection now. But where does this stop? And it is not a criminal act. We had to file a civil suit.

For 8 years, those tapes never stopped running. They recorded all kinds of conversations. They were originally designed just to learn what the union activists were doing, and after winning the election, what were they talking about in connection with collective bargaining.

Senator SIMON. And, if I may interrupt, they did nothing to add to the productivity of the company.

Mr. BAHR. Well, I could suggest to you right now, with the knowledge that this happened, I don't think they're getting too great productivity from the workers who are there today. It certainly did not increase productivity; of course, we didn't know it was happening.

Senator SIMON. Dr. Marx talked about co-determination, and Mr. Rotenberg talked about worker participation. You have entered into an agreement with NYNEX. One of the realities in our society is that only 16 percent of workers are organized. Canada has 35 percent, similar figures in Japan and Western Europe.

That worker participation or co-determination sometimes just is not there. Does that create problems in terms of reaching the kind of agreement that you have reached with NYNEX?

Mr. BAHR. We recognize that the vast majority of workers impacted by this practice are unorganized, and certainly then depend on the Congress for protection.

Senator SIMON. Dr. Marx, you have looked at this from a great many perspectives. As you look at the legislation that is before us, are there changes that you would like to see, modifications?

Dr. Marx. Perhaps you might want to add a clause—and I have the exact place in my testimony, I don't recall now—where you specify three or four conditions. One was reliability, but I would suggest adding perhaps a principle of validity. It isn't enough that you require that the information that is collected be relevant; it also must be valid. And as the Congress recognized several years ago when it banned polygraph exams in most private contexts, whether or not a technique is valid is a crucial principle. So I guess I would like to see some greater recognition of the importance of validity of a tactic because we don't want tactics to work because of a big scare factor. In fact, the polygraph often worked not because it "really worked" but because people were deceived into believing it worked. So I think it is important to have a principle of validity either explicit or implied in there.

Senator SIMON. Mr. Rotenberg, do you have any comments, or are there any changes you'd like to see?

Mr. ROTENBERG. Mr. Chairman, in my testimony I made four suggested changes for the legislation. We thought first of all that you may wish to narrow the law enforcement exception to the disclosure. I have had some experience with privacy statutes in the past, and it is oftentimes the exceptions that become the loopholes.

Certainly, in the area of work monitoring there is going to be enormous reservoirs of personal data that are generated, indicating a person's location at a particular time, whom they were with, and oftentimes what they were doing. In that circumstance, you would want to be very careful about its subsequent disclosure.

I suggested also some effort to restrict the use of the Social Security number as an employee identification number. There are some businesses in this country that use the SSN for employee identification. There are problems with that from a privacy viewpoint, which the Congress recognized in 1974.

Senator SIMON. And what about my earlier question to Mr. Bahr on productivity; do you see any relationship between the practices of secret monitoring and productivity?

Mr. MARX. Yes, I jokingly suggest in my testimony that if this were a different period, and the CIA and the FBI were less restrained, we might want to have them investigate the advocates of monitoring—and I wonder if it isn't even a counter-intelligence operation to spread unrestrained monitoring among American workers, because if you wanted to do anything to decrease productivity, I think you would do exactly that.

And I find it terribly interesting that in spite of the well-intended rhetoric about productivity and what that often implies, we should become more like the Germans and the Japanese. In fact, the Germans and Japanese don't do this. They don't have unrestrained individual monitoring; they tend to do the opposite.

So if productivity is the concern, the logical leap would imply we should become more like them, not less like them.

Senator SIMON. Mr. Rotenberg.

Mr. ROTENBERG. Speaking with colleagues in the computer profession, the question that is asked first when you talk about technology in the workplace is how do you design a system that will respond to the worker's needs, to help the workers do a better job, what factors should be taken into account and what the end product looks like.

Now, if you begin by asking that series of questions, you may end up with a policy much closer to the one described by the last witness on the first panel with Northwest Airlines. Where technology responds to people's needs, it tends to extend their goals in a more productive manner.

Senator SIMON. Yes, Mr. Bahr.

Mr. BAHR. Mr. Chairman, I have just been advised that under an agreement that we have with US West that eliminates secret monitoring, we have seen a dramatic increase in productivity as well as the profit statement in that there has been a dramatic reduction in absenteeism and a concurrent drop in utilization of the health plan, an area where we all strive to contain costs. So there is a direct relationship.

Senator SIMON. That's very interesting.

We thank all three of you. My hope is that we can move ahead with this legislation before very long. I appreciate your testimony.

Our final panel includes Vincent Ruffolo, president of Security Companies Organized for Legislative Action, of Chicago; Lawrence Fineran, assistant vice president of government regulation and competition, with the National Association of Manufacturers; and Edward A. Merlis, vice president for policy and planning of the Air Transport Association.

We are pleased to have all three of you here. Mr. Ruffolo, as I Indicated earlier, I think some of the suggestions you make in your testimony frankly can be incorporated. I have not had a chance to

read in advance the testimony of the other two panelists. But my hope is that we can come up with something that is constructive.

You have someone accompanying you, Mr. Ruffolo. Do you wish to identify him for the record?

Mr. RUFFOLO. Yes. This is Larry Sabbath. He is with Rowland and Sellery, who represent our association here in Washington.

I might add that I was very happy to hear you say, Senator, what you did relative to that the problems we feel we have might be addressed with some type of redrafting or amendment, and certainly we would look forward to working with you and your staff toward that end.

Senator SIMON. We will be working with you on that. We'll ask you to be our first witness, Mr. Ruffolo.

STATEMENTS OF VINCENT RUFFOLO, PRESIDENT, SECURITY COMPANIES ORGANIZED FOR LEGISLATIVE ACTION, CHICAGO, IL, ACCOMPANIED BY LARRY SABBATH, ROWLAND AND SELLERY; LAWRENCE FINERAN, ASSISTANT VICE PRESIDENT OF GOVERNMENT REGULATION AND COMPETITION, NATIONAL ASSOCIATION OF MANUFACTURERS, WASHINGTON, DC; AND EDWARD A. MERLIS, VICE PRESIDENT FOR POLICY AND PLANNING, AIR TRANSPORT ASSOCIATION, WASHINGTON, DC

Mr. RUFFOLO. Thank you, Senator.

My name is Vincent Ruffolo. I am president of A&R Security Services, headquartered in Blue Island, IL. We are a privately owned business providing security guard service, alarm systems, fire systems, and investigative services, and we employ approximately 1,300 people.

I am also the chairman of SCOLA, Security Companies Organized for Legislative Action. This is a coalition of five associations representing the guard, alarm, armored car and investigative industries. Our organization represents more than 3,000 firms in the private security industry, with more than one million employees.

We appreciate this opportunity to share our concerns about S. 516, the Privacy for Consumers and Workers Act. We believe that the bill is drafted with such broad and vague language that it would seriously impair a business' ability to safeguard its patrons, employees and to protect personnel and business assets. It would also make it difficult to follow through on investigations that may require off-premises documentation.

Section 5(a) of the bill prohibits collecting information through electronic monitoring which can be identified with an individual employee if the information is not "relevant to the employee's work performance." Such a prohibition could make obsolete several electronic systems used by employers for legitimate and necessary security purposes because that information collected by these systems may not be deemed relevant to each employee's work performance. Let me cite a few examples of the impact of such a prohibition.

Card access control systems are used by many businesses to protect workers and the business premises. These access control systems open doors, recording both authorized entries and unauthorized attempts. Keeping such records—these are in a computer, now;

it just doesn't open the door; it records them in a computer—keeping these records would fall within the bill's definition of electronic monitoring, and to the extent that such information might not be deemed relevant to work performance, the use of such systems would be prohibited.

What a dilemma for an employer—should he or she deactivate an expensive system which protects workers and company assets, or continue using it and risk being found liable for violations of the act?

And let me stop and say that I have been in business for 25 years, in this business for 29 years. We have put in a lot of access systems, we do a lot of investigation, and I have never had anyone suggest—I don't say it doesn't happen—I have never had anyone suggest that you use an access control system to monitor whether someone goes to the washroom or is taking breaks. Now, maybe it is happening, but I am saying that I have never heard of anyone—no one ever came to my company and asked for us to use this equipment in such a fashion, and I don't believe across the board anyone uses it for other than what it is intended for.

Security cameras are used not only in heavily trafficked areas like banks or groceries, hospitals, where they serve as an important deterrent to theft, but also in remote areas such as parking lots, underground passageways, where the primary concern is the safety of persons in those areas.

Under this bill as it is written, employers would be obliged to abandon using this form of technology because the cameras record all activities within their range without regard to whether the activity captured on film or tape is related to work performance.

Reviews of bank, telephone, credit card usage could also be prohibited. Employers naturally want to be able to review invoices to assure that the company is paying only for business expenses.

These reviews can reveal that an employee is spending his day calling dial-a-porn on long-distance or is making personal purchases on a company credit card. The bill defines "electronic monitoring" to include the "collection, storage, analysis and reporting of information concerning an employee's activities by means of a computer." Under some circumstances, such misconduct might be deemed unrelated to work performance, rendering the employer's records and their use unlawful.

In those cases in which monitoring is permitted, the bill requires that employees and job applicants be notified of how and when they will be subject to electronic monitoring. If monitoring is not continuous, S. 516 requires a signal light or beep to warn employees that the monitoring system is being activated. Thus, an employer would be put in the absurd position of having to advise suspected thieves when they are being observed.

As an example, we just did a job for a hospital where they had a problem in the drug area, losing drugs. Now, there are different methods to try to find out how you are losing drugs. There were about 25 people who had access to this area. A common method is to put a hidden closed-circuit camera—now, that might be abhorrent to some people but the cold, hard facts of life are that here we have drugs going out the door—forget the dollar amount; let's just look at the human suffering that will be caused by the drugs on

the street—so you put a closed-circuit television covertly. Under the bill as it is written, Senator, we'd have to warn those employees that starting next Monday, we're going to start monitoring you guys and ladies to find out who the bad guys are.

So we would be out of business. We wouldn't be able to uncover those types of thefts. And this is how it is done a lot. You just don't go to the police. The police can't do much for you. They are overtaxed, they are overburdened; there are fewer and fewer policemen to deal with the growing problem. It falls on the individual business, and it falls on private security, and the tools are slowly leaving us.

The results of the legislation may or may not be intended. Perhaps some of these infirmities can be remedied through more careful drafting of the bill. But the bill is extremely vague and appears to encompass a very broad range of legitimate activities.

Section 6(c), for example, says an employer "shall not maintain, collect, use or disseminate personal data obtained by electronic monitoring which describes how an employee exercises rights guaranteed by the First Amendment unless authorized by statute or the employee."

By any interpretation, the scope of the First Amendment includes a wide range of activities. Was the intention of this section of the bill to prohibit monitoring of any type of speech? I have yet to find anyone, including proponents of the bill, who can tell me the purpose or scope of Section 6(c).

Proponents of the bill have cited concerns with the use of electronic monitoring to measure productivity. If that is the true goal of the bill, then I suggest they present a bill which is limited to controlling monitoring for the purpose of setting and enforcing production quotas. There is no need to put the security of consumers and employees at risk.

Thank you, Senator.

[The prepared statement of Mr. Ruffolo follows:]

PREPARED STATEMENT OF MR. RUFFOLO

My name is Vincent L. Ruffolo, and I am President of A&R Security Services Inc., headquartered in Blue Island, Illinois. We are a privately owned business, providing security alarm, security guard, fire systems, and investigative services employing approximately 1,300 people.

I am also the Chairman of Security Companies Organized for Legislative Action (SCOLA), a coalition of five associations representing the guard, alarm, armored car, and investigative services industries. Our organization represents more than 3,000 firms in the private security industry with more than one million employees.

We appreciate this opportunity to share our concerns about S. 516, the "Privacy for Consumers and Workers Act." We believe that the bill is drafted with such broad and vague language that it would seriously impair a business' ability to safeguard its patrons and employees and to protect personal and business assets. It would also make it difficult to follow through on investigations that may require off-premises documentation.

Section 5(a) of the bill prohibits collecting information through electronic monitoring which can be identified with an individual employee if the information is not "relevant to the employee's work performance."

Such a prohibition could make obsolete several electronic systems used by employers for legitimate and necessary security purposes because the information collected by these systems may not be deemed relevant to each employee's work performance. Let me cite some examples of the impact of such a prohibition:

1. Card access systems are used by many businesses to protect workers and the business premises. These access control systems will open doors, recording both au-

thorized entries and unauthorized attempts. Keeping such records would fall within the bill's definition of electronic monitoring, and to the extent that such information might not be deemed "relevant to work performance" the use of such systems would be prohibited. What a dilemma for an employer—should he or she deactivate an expensive system which protects workers and company assets or continue using it and risk being found liable for violations of the Act?

2. Security cameras are used not only in heavily-trafficked areas like banks or groceries, where they serve as an important deterrent to theft, but also in remote areas, such as parking garages or underground passageways, where the primary concern is the safety of persons in those areas. Under this bill, employers would be obliged to abandon using this form of technology because the cameras record all activities within their range, without regard to whether activity captured on film is related to work performance.

3. Reviews of bank, telephone, and credit card usage could also be prohibited. Employers naturally want to be able to review invoices to assure that the company is paying only for business expenses. These reviews can reveal that an employee is spending his day calling dial-a-porn on long distance or is making personal purchases on a company credit card. The bill defines electronic monitoring to include the "collection, storage, analysis, and reporting of information concerning an employee's activities by means of a computer. . . ." Under some circumstances, such misconduct might be deemed unrelated to work performance, rendering the employer's records and their use unlawful.

In those cases in which monitoring is permitted, the bill requires that employees and job applicants be notified of how and when they will be subject to electronic monitoring. If monitoring is not continuous, S. 516 requires a signal light or beep to warn employees that the monitoring system is being activated. Thus, an employer would be put in the absurd position of having to advise suspected thieves when they're being observed.

These results of the legislation may or may not be intended. Perhaps some of these infirmities can be remedied through more careful drafting. But the bill is extremely vague and appears to encompass a very broad range of legitimate activities. Section 6(c), for example, says an employer:

> "Shall not maintain, collect, use or disseminate personal data obtained by electronic monitoring which describes how an employee exercises rights guaranteed by the First Amendment unless authorized by statute or the employee. . ."

By any interpretation, the scope of the First Amendment includes a wide range of activities. Was the intention of this section of the bill to prohibit monitoring of any type of speech? I've yet to find anyone, including proponents of the bill, who can tell me the purpose or scope of Section 6(c).

Proponents of the bill have cited concerns with the use of electronic monitoring to measure productivity. If that is the true goal of the bill, then I suggest they present a bill which is limited to controlling monitoring for the purpose of setting and enforcing production quotas. There is no need to put the security of consumers and employees at risk.

Senator SIMON. Thank you.

Mr. Fineran.

Mr. FINERAN. Mr. Chairman and members of the subcommittee, thank you for the opportunity to present the views of the National Association of Manufacturers on S. 516, the Privacy for Consumers and Workers Act. I understand, of course, that NAM's written statement will be included in the hearing record.

Senator SIMON. That is correct.

Mr. FINERAN. My name is Larry Fineran, and I am the assistant vice president and director, government regulation, competition and small manufacturing for NAM.

NAM represents 12,500 member companies, over 9,000 of them small manufacturers. NAM also uses direct telephone marketing itself in our national division.

NAM firmly believes that the legislation is unnecessary. Furthermore, the legislation fails to recognize the realities of the modern plant or office. We take no exception to the parts of S. 516

that suggest that employees generally subject to monitoring should be so informed upon being offered this position.

For the most part, this is standard practice. The legislation, however, goes well beyond this and will distort labor-management relations.

Employee privacy should be respected to the extent practicable, but employees should be expected to perform the work assigned, and modern machinery should be allowed to assist employers in gauging performance productivity.

Random and periodic silent monitoring is a very important management tool. S. 516, however, will interfere with the effectiveness of monitoring by requiring a contemporaneous signalling device. This is, of course, intended to notify the employees of the exact time that monitoring is occurring.

In NAM's international division, which again markets directly to small manufacturers by telephone, monitoring has been found to be a very effective management and training tool with the support of the membership managers. NAM respects their privacy by providing them with a switch on their telephones that allows them to make calls that are not subject to the monitoring device while on breaks. Other companies provide either pay or employer-paid telephones for the same purposes.

Before I go on, I do just want to make one reference in response to Senator Metzenbaum's earlier question to Mr. Bahr. I initially started my first job out of college on telephones myself, and some of what this is based on is my own personal experience. I admit that there may be some people with different experiences with monitoring, but you can also have positive.

It was one thing for me to know that at any given time a supervisor could have been somewhere in the background listening if she was listening. It would be another thing for me to have known, that we'd be given a signal light or some other beep tone. I would be the type of person who would have become nervous and flustered had I been notified that right now somebody is listening in to this conversation versus just going about doing my job and doing it in the most effective way possible.

I think most of my coworkers felt the same way. We had talked about it. Now, again, there may be different types of monitoring and different types of experiences, but in the environment I was in that was generally the way it was.

And again I do want to emphasize for the record that I am sure there are employees who are probably functioning quite well right now, and that light comes on, and they aren't going to function as well as they do right now. And I think if you think it all the way through, their evaluations will probably be somewhat affected, to the detriment of those employees.

Many of our member companies employ customer service representatives. The interaction of these employees with customers reflects directly on the company. In addition, it is important that companies be able to ensure that these employees comply fully with corporate policies as well as Federal and State statutes ranging from telemarketing fraud to such laws as the Fair Debt Collections Practices Act which prohibits abusive and harassing type tactics.

But S. 516 is not limited to customer service or other telephone operators. Many of NAM's member companies have been able to cut cost production and boost quality through the use of telephone equipment that automatically monitors the productivity of each employee and even entire factories. This has helped to streamline production processes and make US industry more competitive. NAM is concerned that the bill may make it more difficult to use this information in establishing production goals.

And again in response to Senator Metzenbaum's earlier question about productivity, I do want to emphasize that in most of the references to productivity within NAM's testimony, we are looking at the bill in totality, not simply its effect on the customer service reps and the operators. Again, what has been lost a lot in this debate is that it is affecting the creation of computer-aided manufacturing or will hinder the use of that in the future because a lot of it is based, obviously, on computerized information. Again, our testimony goes into that a little bit deeper.

In addition, as Mr. Ruffolo said, S. 516 will hinder corporate security efforts. For example, a company is supposed to notify somebody suspected of breaching security that from henceforth their calls and computers will be monitored. In addition, what can an employer do in the situation of a secure area that is monitored by video and/or audio devices, and employees begin to exercise their First Amendment rights by talking about current events or wearing buttons. Is the employer expected to turn off the camera or the sound?

NAM opposes any legislation that will interfere with the ability of modern and future equipment that can assist domestic companies in their fight to remain competitive. Otherwise the United States may as well let the information age pass it by.

If I can just say one more thing, Senator, when I was talking earlier about the importance of companies being able to monitor to ensure compliance with corporate policies such as courteousness, etc., I think as a Senator you might want to keep track of other legislation that is wending its way through Congress, dealing with telemarketing fraud and changing a lot of the ways that some of the telemarketing companies do business.

Congress obviously is going to put the burden and the onus of enforcing these new laws as well as other State statutes, specifically with telemarketing, and again with the Far Debt Collections Practices Act, all of that is on the employer. And again, when you think about a signalling light, if there is a change in the law with a telemarketer, for instance, they probably will not want to change in many ways, but if they see that light to on, they are going to change for their supervisor, and they are going to change their lines like they are supposed to. And it will take a long time, a lot longer, for that company to root out the people that they may have problems with. Granted, customers will start complaining, and their attorneys general may start complaining, but it will take a lot longer to find out what is going on.

Thank you.

[The prepared statement of Mr. Fineran follows:]

PREPARED STATEMENT OF MR. FINERAN

PRIVACY FOR CONSUMERS AND WORKERS ACT—EXECUTIVE SUMMARY

NAM opposes enactment of S. 516 as both unnecessary and counterproductive. Effective electronic monitoring should pose line threat to employee privacy while ensuring employee compliance with Federal and state statutes as well as corporate policies.

Employee privacy should be respected to the extent practicable. But employees should be expected to perform the work assigned and modem equipment should be allowed to assist employers in gauging performance.

The proposed legislation goes well beyond telephone monitoring of customer service operators and will hamper security programs as well as efforts to regain domestic productivity and competitiveness.

Mr. Chairman, members of the subcommittee, thank you for the opportunity to offer the views of the National Association of Manufacturers (NAM) on the impact of S. 516, the "Privacy for Consumers and Workers Act." My name is Barry Fineran and I currently serve as the association's assistant vice president and director, government regulation, competition and small manufacturing.

In addition to traditional manufacturing, many NAM members provide customer service through "800" telephone numbers, sell their products or services over the telephone, offer a variety of financial services, and operate retail outlets. And NAM itself markets directly to small manufacturers through our National Division office. Assurance of quality is critical for both products and services.

The language of S. 516, however, makes clear that it is not limited to these activities. By its very definition, "electronic monitoring" includes all forms "of visual, auditory, or computer-based surveillance." This means, in effect, that any modern business—service or manufacturing—will be impacted negatively by S. 516.

NAM's primary objection is that the legislation fails to recognize a basic tenet of employment that has existed since the beginning of commerce: That one is expected to perform the work assigned according to the employer's standards in return for payment. A corollary of this is that employee interaction with customers reflects directly on the employer.

Members of Congress constantly speak to the need for domestic businesses to be responsive to consumers if they expect to be competitive in the global economy. NAM's members agree with this, and many have implemented quality control, customer service and internal security programs, which often rely on various forms of electronic monitoring to be successful.

NAM takes no exception to the parts of S. 516 that suggest that employees generally subject to monitoring should be so informed upon being offered the position. This is standard practice. Neither does NAM object to sharing information gleaned from monitoring with employees in a timely fashion. The legislation, however, goes well beyond this and will distort labor-management relations.

I have first-hand experience with this issue since my first job after college involved telephone solicitation. From there, I was moved into a supervisory position. While on the phones, I was subject to monitoring and generally found the comments of my supervisor helpful. It was one thing, though, to know that at any given time a supervisor could have been evaluating my performance versus knowing for certain that at a particular point I was being monitored. Had I known, I would easily have become nervous or flustered. From discussions with my colleagues at that time, I know that most if not all of them felt the same way.

Monitoring is the most effective management tool to ensure compliance with statutes such as the Fair Debt Collections Practices Act, which prohibits abusive, deceptive and unfair tactics in the course of collecting debts. In addition, legislation now wending its way through Congress and various state legislatures dealing with telemarketing practices will make monitoring even more important if companies are to make certain that their employees are implementing the new laws correctly. Employees who perhaps do not follow new company policies mandated by such legislation will be aided by knowing when monitoring is occurring since they can "perform" for the supervisor.

For instance, some employees may decide not to change their practices in order to comply with new laws governing the use of marketing by telephone. But, they will certainly know to alter their behavior when a monitoring signal is activated. Without the ability to silently monitor, how does Congress expect employers to implement such statutory changes effectively? After all, the legislation holds the employ-

er liable for compliance. While S. 516 makes a concession for signaling in cases where monitoring is continuous, there is no practical way for employers to handle these situations effectively except in periodic, random intervals.

In NAM's National Division, which again markets directly to small manufacturers by telephone, monitoring has been found to be a very effective management and training tool, with the support of the membership managers. They report that they find the feedback from supervisors helpful, especially during the initial training period. NAM also respects their privacy by providing them with a switch on their telephones that allows them to make calls that are not subject to the monitoring device while on breaks. Other companies provide either pay or employer-paid telephones for the same purposes.

The effect, if not the intent, of S. 516 on employees subject to periodic monitoring is likely to be misrepresented employee evaluations. Good employees who are unnerved when a signaling light or beep tone is activated will receive less stellar evaluations than they otherwise would have, while other employees may be able to mask their actions.

Employees certainly have a right to privacy when it comes to dealing with problems of a personal nature, as long as they do so on time set aside by their employer and as long as their performance is not affected. While there may be anecdotal evidence provided of some abuses, the fact is that employees are paid for the time spent at work. Employers thus should be allowed to control the use of employer-provided equipment for non-work related purposes. There is a very fine line in this regard, but the legislation unfortunately will tie the employer's hands.

Suppose, for instance, that an employer decides to monitor the effectiveness of an electronic mail system, which was entirely paid for by the employer to increase efficiency, productivity and customer service, and a gambling pool is discovered. Or consider an employee who uses employer-provided equipment to run a business on the side after hours and on weekends. To extend the hypothetical, let's assume that the employees involved have been performing their jobs generally well.

Under the terms of this legislation, may the employer confront the employees with the information, or will this be considered personal data that "is not relevant to the employee's work performance?" In this case, apparently the bill would prohibit even the collection of such information even though the employees themselves entered it into the company's computer system.

There are many other hypotheticals such as these that may be raised. The point is, simply, that employers should and must be able to have free access to the computer equipment that they bought and paid for without fear of unintentionally having collected personal data arguably irrelevant to an employee's work performance. Still, such data may assist the employer in assessing an employee's character, productivity or loyalty.

Loyalty does, of course, become entirely relevant in the case of suspected corporate spying. This issue is a real concern of many companies, especially in high-technology industries. A business victimized by corporate spying will find itself at a strong competitive and strategic disadvantage. But S. 516 severely hampers the ability of employers to rout out such suspicions since the suspect employee must be notified that monitoring is taking place.

The bill also conflicts with security controls mandated by the Department of Defense. Card keys or other authorizations measures, for instance, must be used to control access to areas containing classified data. Yet, card keys rely on personal identifying information and, by their very nature, track employee movements. In addition, the production and quota provision of the bill raises questions about the practice of having employees use electronic identifiers to differentiate time spent for the government and for the corporation on shared machinery.

Similarly, the use of personal identifiers for access to computers and computer files will be put in jeopardy since they have the potential of tracking employee productivity. But, these identifiers are obviously necessary features for controlling access to sensitive files.

And how is an employer expected to control the collection of "personal data obtained by electronic monitoring which describes how an employee exercises rights guaranteed by the First Amendment"? Sensitive or remote areas may be continuously monitored by video and audio surveillance for either corporate or employee security. Must the employer turn off the camera and sound if employees begin to discuss current events? Won't this leave the area exposed to possible non-First Amendment right abuses during the time when monitoring is not being conducted? Or consider video surveillance cameras in parking lots. Their purpose is employee protection, but the provision raises questions as to the permissibility of the practice

since some employees will almost assuredly have bumper stickers on the cars expressing "rights guaranteed by the First Amendment."

Of more concern to manufacturers trying to meet the challenge of global competition, the legislation also seems to threaten the use of modern technologies and techniques by inhibiting the use of computers and high-technology machinery in the manufacturing process. Many of NAM's member companies have been able to cut costs of production and boost quality through the use of equipment that automatically monitors the productivity of employees and even entire factories. These advanced techniques may rely heavily on statistical process control, numerically controlled machines and other closely monitored systems. This has helped streamline production processes and make U.S. industry more competitive. Where a factory once needed several layers of managers to keep manufacturing lines running productively and efficiently, now it may need only one. Corporate management should not be prohibited from using information obtained through computer-aided manufacturing (CAM) unless managers are physically on the shop floor looking over the shoulders of employees.

We are moving toward an ever-increasing technological workplace. This has generated fears in some of an Orwellian world. Some may promote the language of Section 6(b) that data "obtained by electronic monitoring [cannot be used] as the sole basis for setting production quotas or work performance expectations" as a way of saving employees from such a scenario. But these fears are as unfounded as those of the Luddite movement in early 19th century Britain, which wanted to keep England out of the industrial revolution because machinery was performing work previously done by hand, and which refused to recognize that failure to modernize in and of itself would jeopardize the availability of jobs for the very workers the movement professed to protect.

Computer-aided manufacturing should be seen as helpful to productive workers, since subjective perceptions—as personality conflicts with a supervisor—will be overridden by the objective analysis. CAM, for example, will be able to tell management which workers or work teams are most productive and which may need additional help. But if U.S. factories are somehow discouraged from moving forward with CAM, then American workers will be the ultimate losers as domestic factories won't be modernized even as overseas factories become increasingly efficient.

Cash registers present a similar dilemma. Many of NAM's members have divisions where they are commonplace. The modern cash register requires employees to use an identification number when signing on and is hooked-up to a central location within the store or selling area. It used to be that managers would count out each cashier's receipts and compare these with the money taken in during the shift. Today, computers assist in this function and the lime of managers has been freed for other duties. Yet, the legislation seems to require that we return to the days when cashier-register comparisons were done entirely by hand.

Similarly, loss prevention and security efforts will be set back significantly should S. 516 become law. Video and audio surveillance has greatly improved the effectiveness of these programs—to the benefit of employees as well as employers.

Electronic monitoring, like any other management tool, can be used well and for lifting the overall quality of life in the workplace. Admittedly, however, it also can be abused. But, if used wrongly, employers will be confronted with morale problems and decreases in customer satisfaction, product standards and even profits. It is certainly an area ripe for labor-management relations, but legislating in this area faces the prospect of creating more problems than it solves.

NAM opposes any legislation that will interfere with the ability of modern and future equipment that can aid in gauging either the effectiveness or the accuracy of employees or inhibit security programs. Otherwise, the United States may as well let the information age pass it by.

In short, NAM views this legislation not only as unnecessary, but also as counterproductive. Effective monitoring not only ensures compliance with various federal and state laws and provides customers with the assurance that employees are following corporate guidelines, but also respects privacy to the extent practicable. It also helps domestic companies meet the global challenge through increased productivity.

Senator SIMON. Mr. Merlis, I am happy to have a witness whose last name I can pronounce properly the first time.

Mr. MERLIS. And a former constituent. Mr. Chairman, I am Edward Merlis, vice president, policy and planning, of the Air Transport Association of America.

I am pleased to have this opportunity to appear before you today to discuss the position of the ATA member airlines on S. 516, Privacy for Consumers and Workers Act.

Our members collectively account for approximately 97 percent of the revenue passenger miles flown in the United States and over 95 percent of the freight ton miles. We fly more than 19,000 passenger flights each day and carry nearly 1.3 million passengers on those flights. We use some 4,300 aircraft and employ 545,000 persons to perform these services.

If ever there were an industry for which an electronic data collection and interpretation system is essential, it is the airline industry.

Unfortunately, the broad sweep of S. 516 has the potential to undermine the safety, security and consumer protection practices which our industry has adopted over the course of many years. Many of these practices are a direct result of Federal aviation regulations which would conflict with the requirements of S. 516.

While my written statement goes into some detail on those matters, I would just like to review a few of them. Let me begin by discussing security.

A fundamental component of effective security is that systems are covert. To require "a signal light, beeping tone, verbal notification, or other form of visual or oral notice of electronic monitoring," as prescribed by section 3(b)(3), is tantamount to providing a road map to those intent on breaching security.

A potential perpetrator of a crime who is outside the audible or visual range of the light, beeping tone, or verbal notification is also of necessity outside the range of the monitoring device. Thus, the establishment of this requirement alone would compromise a particularly important component of our security systems.

Many aircraft and airport security measures have been instituted in order to comply with Federal aviation regulations to restrict and monitor access to secure areas. Institution of the requirements proposed in this bill would clearly lessen levels of security, perhaps sufficiently to fail to comply with the FAA regulations for which those requirements were instituted.

The airline industry engages in electronic monitoring and data collection and retention of that data in order to comply with a host of other Federal aviation regulations concerned with flight crew schedules and hours of duty, aircraft accident investigations, and maintenance activities, to name but three. All employees subject to this monitoring know of its existence and the complication of the data derived from this monitoring.

Three aspects of the bill interfere, though, with our routine practices in this regard. The notification pursuant to 3(a) is superfluous and costly—very costly, I might add, for as we read the bill, if a software enhancement were to result in additional data being collected which might be personally identifiable, a new notice would have to be issued because the previous notice was now inaccurate.

Outside consultants called upon to review safety-related data to improve the sanctity of our air transportation system are, by the terms of section 5(b), precluded from reviewing this material if it is at all personally identifiable.

The section 3(b)(3) requirement for oral-oral or visual notice of electronic monitoring are obtrusive and would divert from the attention which should be paid, for example, by a crew flying an airplane.

The third major area in which the industry uses monitoring is to further the interests of our cargo customers and our passengers. One of the hallmarks of the overnight package delivery business has been their outstanding reliability. This reliability is due to these delivery services maintaining extensive monitoring capabilities which track packages from pickup to delivery. Employee notification of these techniques is superfluous. Most of the employees about whom data is being tracked generate the data themselves. As a matter of fact, this is the device which United Parcel uses, and its employees enter the data, know full well what all the data is, and therefore to require notice would be just an extra burden and cost on the company.

The customer benefits from these electronic monitoring capabilities without which these companies would be less distinguishable than the Postal Service.

With regard to our passenger operations, less than one percent of our reservations agents' calls are monitored for quality assurance and compliance with Federal law. Inasmuch as the industry has a complex series of frequently changing schedules and fares, this monitoring is designed to identify training and staffing needs to satisfy our customers. Intermittent monitoring of telephone reservation lines and analysis of the data and performance characteristics observed assist the carriers and the employees in fulfilling customer needs and expectations.

Furthermore, we are faced with legal obligations to disclose certain information pursuant to the Department of Transportation's consumer protection regulations. While passengers may not request this information, failure to provide it is subject to stiff fines. All telephone reservations employees are aware they are subject to being monitored, and to require a signal whenever monitoring is taking place would defeat the quality assurance objectives of the monitoring.

Mr. Chairman, I have highlighted only a few of our concerns with S. 516. The written statement contains more detail and additional areas. Needless to say, after enduring $4 billion in losses in 1990, we should not be confronted with new, expensive and unwarranted requirements which are superfluous and have the potential to undermine passenger and crew security and long-established safety systems.

I would be pleased to respond to any questions which you may have.

[The prepared statement of Mr. Merlis follows:]

PREPARED STATEMENT OF MR. MERLIS

The Air Transport Association of America appreciates the opportunity to inform the Committee of our opposition to S. 516. ATA is the trade and service association of the U.S. airline industry. We have 20 air carrier members and two foreign air carrier associate members. We believe that the bill would severely impede or eliminate reasonable and necessary safety, security and quality assurance monitoring in the airline industry.

Electronic monitoring of employees is an indispensable means for the airline industry to assure the safety, security and services that airlines provide to the travelling and shipping public. Electronic monitoring in our industry is not intended to harm the employee. It is not a manipulative or coercive device.

The complex nature of airline operations, which involve both profound safety related and consumer driven logistics, necessitates the use of electronic monitoring. U.S. airlines operate 19,000 flights each day and carry nearly 1.3 million passengers on those flights. Our passenger and cargo members use some 4,300 aircraft and employ 545,000 persons to perform the air transportation services. Given that scale of activity, we must rely upon electronic monitoring to assure the quality of services that we provide the public. We could not maintain essential operational standards without the use of electronic monitoring.

The monitoring of employees is not a new development. Employers have historically monitored the performance of their employees. It is a reasonable exercise of managerial oversight responsibilities. What has changed in more recent times has been the method of supervision. Due to the nature, sophistication and reliability of current technology, electronic monitoring of employee activities is now commonplace and, although it is newer in origin, electronic monitoring is no more invasive than traditional personal supervision. Indeed, for most employees, electronic monitoring is invasive than direct personal supervision. Our employees are aware of it; they therefore are not "blind sided" by the practice. Consequently, we look upon S. 516 as an unwarranted impediment to legitimate airline monitoring activities.

In addition to these considerations, our opposition to S. 516 is prompted by the vagueness of various key provisions of the bill, which we fear could be interpreted to erect insurmountable obstacles to our efforts to insure safe and secure service through electronic monitoring.

One serious ambiguity in the bill is the relevancy requirement of section 5(a). This provision would prohibit an employer from using electronic monitoring to collect "personal data" about an employee which is not relevant to his or her "work performance."

The scope of the term "work performance," if narrowly construed, could eliminate the use of reasonable and worthwhile monitoring. That result would occur not because the particular practice was intrinsically unreasonable but because it fell outside a cramped interpretation of "work performance." The term poses another serious problem Some of the information that the bill would categorize as "personal data" that an airline collects is intended to provide it with an aggregate view of its operations rather than as a measure of a particular employee's performance. For example, an airline might record the number and duration of calls that its reservations agents handle during the day and assemble that data to obtain an overall picture of its reservations activity. Section 5(a) would appear to prohibit the collection of such data because it would not be directly pertinent to the employee's work performance.

The bill would impede a number of our industry's electronic monitoring activities. Those affected activities are summarized below.

Airline Reservations. Telephone calls to airline reservations centers are intermittently electronically monitored. The purpose of the monitoring is to assure high-quality customer service, identify training and staffing needs, and assure compliance with U.S. Department of Transportation (DOT) consumer protection regulations. Fewer than one percent of such calls are monitored.

For example, one of our members has reported that on average they take 5,000,000 calls per month. Of these calls, approximately 48,000 are monitored, equating to less than one percent of the calls. That company also enforces a policy that no "personal" calls are to be monitored and makes separate company lines and pay phones are available for personal calls.

Quality assurance monitoring is especially important for commercial passenger reservation calls because of the complexity of, and frequent changes to, airline fares and schedules. The same considerations apply to calls related to freight and express package services. Monitoring is also important because DOT consumer protection regulations require airlines to disclose to consumers the existence of joint marketing arrangements among airlines, which are commonly referred to as code-sharing agreements. (Violation of DOT regulations subjects airlines to civil penalties of up to $10,000 per violation.)

Section 3(b)(4) of the bill would require a business that engaged in telephone observation to provide the affected consumer with a periodic signal light, beep tone, or oral notification indicating that the observation is occurring. The "beep tone" requirement would inevitably result in consumer questions, which would prolong the conversation, and increase staffing needs. The "beep tone" also would tend to dis-

rupt the thought processes of the customer and the reservations agent, which is not the intention of the bill. One airline has estimated that a one second increase in the average length of a reservations call would annually cost it $600,000 in additional labor and communications costs.

Also noteworthy is the fact that airline employees are well aware that calls are being monitored. Through pre-employment, orientation, training, and evaluation processes, employees are repeatedly informed of the monitoring. Employees understand this and accept it.

In view of the fact that electronic monitoring is intended to benefit the consumer, there is no need to impose a disruptive notification requirement on those calls.

Security. The effect of the bill's notification requirements would effectively eliminate essential security activities in the airline industry.

Electronic devices are used to restrict and monitor access to security-sensitive areas on airports, such as ramps. They are used to fulfill an airport access control requirement that the Federal Aviation Administration (FAA) has imposed upon airlines and airport operators. Notifying employees of such monitoring would be expensive, because of the great number of affected employees, and superfluous, because persons authorized to have access to such areas at an airport know of the access monitoring. Furthermore, the surest way to defeat security controls is to let potential perpetrators know of their existence, method of operation, and location.

Electronic monitoring is also used to combat theft. For example, video cameras are used in undercover investigations. If an airline received reports from passengers of pilfered luggage or packages, it might install a concealed camera in baggage handling or package sorting areas to determine whether pilferage was occurring. The prior written notice and contemporaneous visual or aural notice requirements of section 3(a) and (b) would destroy the usefulness of such investigative techniques.

Crew Scheduling. Computers are used to establish and track the work schedules of the 140,000 pilots and flight attendants of the airlines. This information is essential to assigning crews to airline flights. Moreover, because there are FAA and contractual limitations on the number of hours that a pilot can fly in a month, the number of hours he or she flies each day must be carefully monitored, since weather and air traffic control delays can mean that a pilot will exceed his or her projected flight time. The consequence of not doing this would be grounded pilots and disrupted flight schedules, and disgruntled passengers. Similarly, DOT regulations restrict the number of hours that drivers (who work for the air freight carriers) can work on a daily and weekly basis. Electronic monitoring is indispensable to insuring the safety of the driver and that of the general public.

Notifying employees of the use of computers to compile and analyze work scheduling information would be expensive and unnecessary, since employees have for years relied upon computer-generated work schedules.

Package Tracking. Airlines that provide overnight delivery services rely on electronic tracking (from the time it is picked until it reaches its destination) to determine the location of packages and the employees delivering them. Such comprehensive tracking is essential to assure reliable service to customers.

The bill would require an airline to notify a delivery driver of what is already obvious to him or her. The airline is monitoring the progress of the deliveries that the driver is making.

Aircraft-to-Ground Communications. Both the FAA and air carrier operations departments monitor and record their communications with aircraft flight crews while they are on the ground and in the air. The FAA requires that air carriers record those communications. This monitoring occurs for safety and accident investigation reasons.

Flight crews realize that both airlines and the FAA record such communications, and therefore notification to them is unneeded and would be expensive.

Cockpit Voice Recorders and flight Data Recorders. FAA regulations require that large commercial transport aircraft have systems that record cockpit conversations and systems that record aircraft performance, such as speed, altitude and rate of climb or descent. These recorders provide essential information for aircraft accident investigators.

Flight crews are well aware of this government-imposed monitoring and consequently there is no need to inform them of it.

Maintenance Activities. Electronic means, most notably bar coding, are used in airline maintenance operations to track maintenance activities and access to spare parts. Such monitoring eases compliance with FAA maintenance requirements, simplifies parts inventory accounting, and can be of assistance in aircraft accident investigations.

Notifying all employees who perform maintenance functions or handle parts of this tracking would be expensive and duplicative because employees know of these tracking programs.

Training. Airline employees receive initial training when they are first hired and thereafter receive recurrent training annually. Training programs are sometimes videotaped to allow the instructor and the trainee (which, for example, may be a pilot, flight attendant, or customer service agent) to critique the trainee's performance in the training session. The beneficiary of this videotaping is the employee. By way of illustration, FAA regulations require flight attendants to give passengers a safety briefing before an aircraft takes off. Both initial and recurrent training of flight attendants concentrates on properly conducting such a briefing.

Notifying the employee of its use is unnecessary because he or she is aware of its use as an instructional aid.

Personnel Records. Various personnel records, including those involving payroll, medical benefits, and retirement benefits, are stored on computers. Such storage is far more efficient than maintaining these records on paper and most companies have procedures in place that control access and protect the confidentiality of such records.

Employees know of the existence of such records. In fact, they receive periodic statements from their employers about such records. There consequently is no need for employers to incur for these records the added expense of the notification requirement of S. 516.

Workplace Improvements. Proposed alterations in workplace procedures are analyzed, often with the assistance of computers, to determine their effect on airline operations. These changes are typically intended to improve the efficiency or safety of airline operations. For example, airline personnel might videotape or electronically analyze check-in procedures at an airline terminal to determine if improvements to those procedures could be made. However, since such observations or analyses could be traced to individually identifiable employees, this activity would be subject to the requirement of S. 516.

The bill would create a significant additional barrier to developing workplace improvements. Section 5(b) would prohibit the disclosure of electronically collected information to persons outside a company, except pursuant to employee approval, a court order or to a law enforcement agency. This would cripple the ability of companies to use outside consultants, which are often the most economical source of expertise about a particular matter. Using them permits sophisticated advice to be obtained for a specific project without the need for the company to invest substantial resources to create such a capability internally.

Productivity Analyses. Productivity data are gathered not only to measure work performance for the purpose of job evaluations in some firms but also to determine the volume of business, efficiency in dealing with consumers, and the need to add resources to meet consumer demand. The use of electronic monitoring works to minimize reliance on "subjective" standards. Such data gathering would be covered by the bill.

To summarize our testimony, four conclusions can be drawn from this review of the bill.

First, electronic monitoring has become an indispensable means to assist the airline industry in providing its services safely, securely and efficiently. Much of that monitoring is tied to government regulatory requirements.

Second, electronic monitoring has become a routine management tool in our industry. It is not a device that is sprung on unsuspecting employees.

Third, the adverse effects of S. 516 would be extraordinarily broad. It would reach into virtually all air carrier activities, however mundane they might be.

Fourth, the bill's notification requirements would prove costly. Not only would we suffer the recurrent expense of notifying employees of monitoring, but the way we do business would be impeded.

S. 516 would create expensive and unnecessary compliance costs for our industry. Electronic monitoring is a routine, reasonable practice in the airline industry. Bearing unwarranted costs would be especially difficult for our industry and, ultimately, for consumers. We suffered a $4 billion loss in 1990 and a $1 billion loss in the first half of 1991. Neither employees nor consumers will be served by saddling the airline industry with unnecessary additional expenses at this time.

For these reasons, we respectfully urge that S. 516 be rejected.

Senator SIMON. Thank you, Mr. Merlis.

You heard the earlier witness mention the newer practice of Northwest Airlines. Are you critical of that new practice?

Mr. MERLIS. Not at all. I think it's great that Ms. Maurel has such a positive attitude toward her job, and she acknowledged that she has benefited from the new monitoring which they have instituted.

One thing she did say was that S. 516—and I'll quote—"will probably not affect the way Northwest monitors." Regrettably, I think she is wrong. S. 516 would require a disruptive beep tone on the line when she is being monitored. S. 516 would require a new written notice any time a software change resulted in different data being collected. S. 516 would reduce the safety of the parking lot where employees park their cars by reducing the level of security in that lot, and S. 516 would reduce the safety of the planes that she rides and the airports through which she might work.

So, while I agree, and I think it is wonderful that she enjoys that new monitoring, I don't think the bill and the practices that they engage in exactly coincide at the moment.

Senator SIMON. Let me just mention there are a number of companies that already use the beep and have no adverse experience at all. Some of the questions that I mentioned to Mr. Ruffolo—and I think his testimony particularly—we can accommodate some things. And when there are security questions, we can work things out.

Mr. Fineran, do you think Germany and Japan have made a mistake in not going in this direction—and they also seem to have greater increased productivity than we do.

Mr. FINERAN. Well, I would say NAM just opposes the enactment of this legislation. Again, we don't oppose enlightened management like Northwest Airlines, but we think in particular this legislation just goes way too far. I am not familiar with any of the laws in Japan or Germany technically, but for instance, this legislation that you have will affect electronic mail systems. It will make it illegal for an employer, for instance, to confront employees that it may have found out through electronic mail system one way or the other were organizing a racist rally because it is illegal to maintain, collect, etc., information of personal nature that is not relevant to an employee's work performance. And that is not necessarily relevant.

Again, I just think the legislation goes way too far, and again I do want to emphasize that NAM does not think any legislation of any form is necessary, but we do not oppose the notification upon employment by any means, so I think that that is fine.

Senator SIMON. Let me just say—and I won't get into all the specifics because I have to get on to another meeting—but many of the criticisms, frankly, are a misreading of the law, or we can clarify and make sure that they don't go in the direction that you are talking about.

Mr. Fineran, what would you think of your employer, NAM, monitoring your phone conversations and what you do?

Mr. FINERAN. Well, first of all, I was, again, in a job where I was monitored, and it didn't bother me at all in that customer service or telemarketing type of job. Again, I think that you have to put some of these jobs in perspective. For instance, I do not monitor my secretary. I don't care if she has personal phone calls. I know she does, but she gets her job done, and that is what's important to me.

However, I am not normally a first contact with a customer who doesn't know the company at all, and I think especially if you are dealing with cold call situations in telemarketing or, again, with customer service, the only effective way—again, from my own experience having been on the phone—the only effective way to really know what is being said is to do it randomly and silently.

Senator SIMON. Do you think your secretary would do a more effective job if you did monitor, or a less effective job?

Mr. FINERAN. Frankly, I really wouldn't want to, but I know what you are getting at. All I can say is if my employer did go ahead and monitor every single one of my calls, that would be a signal to me that if I were going to make a personal call or of personal nature, to go to a pay phone or another nonmonitored phone if I wanted to do such; other than that, just stick to it.

Now, again, some of the examples cited by Ms. Cameron and again in today's *Wall Street Journal* do not make for great workplaces. I'll be the first to admit that. And I think, as NAM says in its testimony, like any other management tool or management technique, this practice can be used well or it can be abused, and to the extent that it is abused you are going to see a decrease in employee morale; probably productivity will be negatively decreased if it is abused, and we don't deny that. We are just saying that we don't think there is cause for legislation in this area.

Senator SIMON. Mr. Ruffolo, someone suggested to me if there is too much resistance to this that we simply accept the practice but just add a provision that employees also have the right to monitor employers.

What would you think of that approach? I would say as a former businessman myself, I don't know whether I would particularly like that.

Mr. RUFFOLO. Well, first of all, I am not in favor as a philosophy of monitoring employees. I think it is counterproductive—although there might be some business that that's the way you track how things are going. But I certainly don't know of any. That's not what I'm here for.

What you should be doing is trusting your employees, and they are going to treat you likewise and are going to give you some respect.

Senator SIMON. You are a pretty good witness. I agree.

Mr. RUFFOLO. We certainly don't do anything like that, nor do I know anybody who does that.

Senator SIMON. Good. And I think you have some constructive suggestions here.

We appreciate your testimony, and we will be moving ahead. Frankly, we'll be getting back to all three of you. I hope we can work something out. I'm not saying that the National Association of Manufacturers is going to endorse our bill, but we may be able to get a bill that meets some of the concerns raised. The concerns raised by Air Transport can be considered as well. As you know, I am in a State with a huge number of people who have an economic interest in the air industry, and I want it to be a thriving industry, and I want it to be a safe industry. I also think we have a problem, 5 years from now there is going to be some other new technology

we're going to have to deal with. There is a sensible restraint that we have to work out, and I hope we can work that out.

Senator Thurmond wanted to be here as well as Senator Kassebaum. They may submit questions to all of the witnesses. We will keep the record open for 2 days in case other members of the Senate wish to submit questions.

[The prepared statement of Senator Thurmond follows:]

PREPARED STATEMENT OF SENATOR THURMOND

Mr. Chairman: It is a pleasure to be here this afternoon to receive testimony on electronic monitoring in the workplace. I wish to join you in extending a special thanks to all the witnesses who have joined us today.

While the notion of monitoring workers by electronic means may be offensive to some, the fact of the matter is workers have been monitored for many years. However, the manner in which it is done has changed.

Years ago, we did not have sophisticated computers, telephone systems, or cameras for ensuring efficiency, accountability and productivity in the workplace. What we had were supervisors who personally made the rounds in their companies. With the advance of technology, that has changed. In some cases, new electronic devices have replaced that function. While having a person supervising is preferable to an electronic monitoring device, that is not always the most efficient or productive use of a supervisor's time. In short, many businesses find it essential to use electronic monitoring as a means of staying competitive in the 1990's and into the next century.

The bill before the subcommittee today—S. 516—would substantially limit the ability of companies to maintain a quality workplace. It does this by placing strict limitations on the use of cameras, telephones, computers, and other such electronic devices to monitor employees. While employee privacy should be protected in certain situations, the privacy must be balanced against the need of businesses to maintain quality services in a competitive market.

A threshold question we must address is "Is this legislation necessary?" There is evidence that many employers already give notice to employees that they may be subject to monitoring. In other cases, there are other protections. For example, some employers protect against monitoring of non work-related calls during breaks by providing separate unmonitored private phones.

A second question is "Do we really have a problem with companies ruthlessly monitoring employees or are there simply a few bad players which we hear about?

A third question is "Should the Federal Government mandate the type and manner of notice to be given, or should we leave that to those who negotiate collective bargaining agreements? In House testimony earlier this year, Pacific Bell testified about the inclusion of monitoring in a negotiated agreement with the Communication Workers of America. Perhaps that approach should be given further thought.

On the whole, I believe most employers use monitoring to help ensure a quality product and quality workplace, and not for sinis-

ter eavesdropping purposes. I am also realistic and realize there are few bad apples. However, I do not believe the current language in this bill represents the best possible approach in this matter. For example, the bill would require prior written notice to an employee about:

—the forms of monitoring to be used;

—the personal data to be collected;

—the frequency of each form of electronic monitoring which will occur;

—the use of personal data collected;

—interpretation of printouts or other records of information collected through monitoring;

—existing production standards and work performance expectations; and

—methods for determining production standards and work performance expectations based on electronic monitoring statistics.

In addition, I have concerns about the breadth of Section 6(c) of the bill and its practical meaning. That section prohibits the collection or use of data "obtained by electronic monitoring which describes how an employee exercises rights guaranteed by the First Amendment unless such use is authorized by statute or by the employee to whom the data relates or unless pertinent to and within the scope of, an authorized law enforcement activity."

Mr. Chairman, there is no doubt about some type of notice being reasonable. Whether we should mandate that, and if so, exactly what form and manner that should take, is a different question. I look forward to hearing from our witnesses.

RESPONSES TO SENATOR THURMOND'S QUESTIONS FROM MS. CAMERON

Question 1. Balancing employee interests and quality of service, efficiency and competitiveness.

Answer. Although 9to5 supports legislation which puts the dignity and privacy of workers and consumers first, we do not see these needs in competition with efficiency and quality of service.

There are several companies, including Northwest Airlines and Bell Canada which have found that restricting the use of workplace monitoring to be a means of achieving better service and competition. Many corporate and academic studies have shown that restricting the use of monitoring reduces employee stress, absenteeism and turnover, and increases productivity and morale.

In western Europe and Japan, where our greatest economic competitors are, cultural, legal and collective bargaining restrictions make the use of electronic monitoring, as it is practiced in the country, nearly unthinkable. For example, a corporate spokesperson at SAS, the tremendously successful Scandinavian Airline, said that electronic monitoring1 as described by reservationists who have called 9to5, runs completely contrary to SAS' philosophy of treating each employee with respect as an individual, and encouraging the teamwork approach to increasing productivity.

Question 2. Federal mandate concerning "notice."

Answer. It is true that there exist "good employers" in the area of computer monitoring, and 9to5 sees as part of its mission to publicize these cases; for example awarding to Al Checci, CEO of Northwest Airlines, a Good Boss of the Year in 1590, for changing the monitoring policy for reservationists.

9to5 feels that such "good players" show that the standards set out in S. 516 are not undue restrictions on businesses. S. 516 sets basic protections for all employees, so that those who do not have an enlightened employer or union contract do have the protection of government from invasion of privacy and abusive monitoring. Government regulations are appropriate and necessary in the area of computer monitoring just as they are in the area of minimum wage and health safety standards.

Question 3. Expectations of privacy in the workplace.

Answer. Certainly there is less expectation of privacy in the workplace than in the home. 9to5 recognizes the right of employers to assess the quality of work of its employees. The problem that S. 516 seeks to address is the ability of employers, through electronic technology to cross a delicate line from monitoring the work, to monitoring the worker.

Personal phone calls should definitely be out of bounds to an employer. A visual or aural signal is needed to alert both consumers and workers to the presence of a supervisor on the line. Employees should have the privacy of spending personal time in the bathroom or making private phonecalls without their employers counting or listening.

Americans are greatly concerned about this issue of privacy in the workplace, and S. 516 is an appropriate way to address the need for new standards. A 1987 study by the Bureau of National found a 20-fold increase in workplace privacy suits over a three-year period. A 1990 national survey by the National Consumer's League found that an overwhelming majority of workers believe that employers have no right to pry into their personal affairs, including 93 percent who said employers have no right to monitor personal phone calls.

Question 4. Technology vs. management behavior.

Answer. The goal of the bill that we support is to put reasonable limits on how employers may use electronic technology.

Question 5. Job stress

Answer. Certainly S. 516 would not eliminate many severe stressors in the jobs described by Renee Maurel and Carol Scott. Handling several hundred calls per day; dealing with the public for eight hours a day; having your minutes per call, seconds between calls, minutes per day away from the computer are all counted and tallied are stress-producing job characteristics, which would not be changed by the passage of S. 516.

The additional stress of unannounced phone surveillance, of not having access to records kept about you, of having your job evaluation based solely on monitoring results, is unnecessary and is addressed by this bill. S. 516 is not a cure-all, but it is an protection against some of the worst abuses of electronic monitoring.

Question 6. Other means of quality assurance.

Answer. S. 516 would not ban electronic monitoring. Passage of this bill would simply mean that employers would have to notify workers of monitoring practices, limit the disclosure of monitoring results, make those results available to the employee, and include other measures of job performance in making job evaluations.

The use of more personal supervision seems a potentially positive outcome of this legislation. Gordon Macpherson, president of Incoming Calls Management Institute has suggested several alternatives to monitoring, including using "shoppers" or "mystery callers;" inviting callers after each call to leave recorded messages concerning the quality of service; providing group incentives; applying the Tom Peters' concept of "management by walking around;" and supervisors trusting their own abilities to develop loyal, well-trained employees.

Question 7. Alternatives to electronic monitoring

Answer. Again, S. 516 would not cause companies to "loose monitoring as a management tool." I can see no way in which use of credit reports or integrity tests would become necessary as a result of placing some restrictions on covert monitoring practices. The experiences of Northwest Airlines and Bell Canada seem, in fact, to point in the opposite direction: The result of using less monitoring has been an improvement of morale and productivity, and a decline in health complaints and absenteeism.

Responses to Senator Thurmond's questions from Ms. Maurel

Question 1. We have heard testimony this afternoon about problems that some employees have with electronic monitoring. As we all know, the other side of the coin is the need for electronic monitoring so that companies can continue to provide quality products and services, and operate efficiently in a competitive market.

What do you think is the proper balance between these two competing interests?

Answer. My company, Northwest Airlines, is now providing a quality product and operating efficiently in a competitive market. We are all feeling better about our company even though we are still monitored 8½ hours a day. When monitoring is used against employees instead of used as information or as a training tool, that is when stress occurs. I don't really know what the proper balance is, I just know that the difference in my life is 180 degrees opposite of how I used to feel.

Question 2. With electronic monitoring, there are obviously companies who use it in a proper manner and stories of those who do not. Unfortunately, the "good play-

ers" are rarely given the attention and recognized for their reasonable monitoring practices. It seems the Federal Government continues to get more and more involved in the workplace and requires more and more of businesses—some requirements which may be needed and others which are not.

As a policy matter, is a broad particularized Federal mandate about "notice" really necessary or do you think there are other less restrictive means for achieving the same objective?

Answer. Giving "notice" is a new concept. The U.S. workplace seems to be mired in the traditions and beliefs of the past: The sweatshop, the assembly line, control your employees, they will work harder. Wrong giving "notice" is no elementary that I find it hard to believe it isn't the accepted attitude.

Question 3. As policy makers, we hear of employee concerns about "invasions of privacy" when monitoring takes place. However, as a general principle, the workplace is a public place and there is a diminished expectation of privacy, as compared to the home, for example.

Do you have any comments about the fact that there is a diminished expectation of privacy in the workplace?

Answer. The workplace is not private. The company must accumulate data. The company must monitor my work. I just never want to be abused by the statistics.

Question 4. Are your concerns really with the technology of electronic monitoring or are your concerns with the behavior of management?

Answer. My concerns are both with the technology and management behavior. The current technology is difficult for me to fathom and it is growing so fast that I cannot comprehend the future scope of growth someone should gage it. I believe it should be the Federal Government. Northwest Airlines today is managed by the "good buys" but who's to say that in the future my company won't be purchased by a Frank Lorenzo type who will return me to the Dark Ages?

Question 5. We all experience some degree of stress in everyday living—it is a part of life. The real question seems to be—is the stress we hear about solely attributable to electronic monitoring or is it caused by other factors as well? Would you care to comment on that statement?

Would S. 516 really eliminate the problems of stress which have been described here this afternoon?

Answer. Stress is everywhere, caused by just about everything. I can only tell you of my experience. Because monitoring is no longer a negative factor at Northwest Airlines reservations, I no longer dread going to work, I no longer have that knot in my stomach. That stress has been relieved and I can deal with the other stresses with a little more space.

Question 6 and 7. If the use of electronic monitoring is banned or severely restricted, wouldn't employers use other means to ensure quality products and services such as increased tests for substance abuse, the use of more personal supervision, and more frequent performance testing and reviews? If electronic monitoring is lost as a management tool, would you support the use of tougher pre-hire reviews? This might require more use of credit reports, integrity tests, and higher educational requirements. Is that a preferred alternative to electronic monitoring?

Answer. Whatever is changed will be replaced with something else. That is evolution. Maybe more personal supervision, more frequent testing is the answer. Maybe personalization is the key. Maybe my feeling like a person and not a robot is what has changed my life. I believe so. Tougher pre-hire reviews is a great concept. Integrity tests, higher education requirements are far better in my opinion than having just anyone hired and then trying to mold them into an automation through electronic monitoring.

I don't know if I am very qualified to answer these very intelligent questions. I do know that I am a much more productive worker due to the changes at Northwest Airlines. I am much happier, much less stressed than ever before. I can only wish the same for every American worker who is monitored daily.

Questions from Senator Thurmond to Mr. Rotenberg

Question 1. Do you believe that employers have the right to use electronic monitoring in order to protect their personnel and company property against intruders and theft?

Question 2. Section 6(c) of the bill prohibits employers from collecting information which describes how an employee exercises First Amendment rights.

Because almost all speech is protected by the First Amendment, this provision seems to totally prevent the use of monitoring by employers.

How could employers using a camera or other monitoring device avoid collecting information about protected speech?

[Responses to Senator Thurmond questions from Mr. Rotenberg were not received at press time.]

RESPONSES TO SENATOR THURMOND'S QUESTIONS FROM MR. BAHR

Question 1. Do you believe that employers have the right to use electronic monitoring in order to protect their personnel and company property against intruders and theft?

Answer. Yes, employers have the right to use electronic monitoring in order to protect their personnel and company property against intruders and theft. I would assume such monitoring would be in the form of security cameras or alarms in areas of the premises. As employees of the enterprise, the workers would be aware of the monitoring devices. Additionally, the devices would not be installed for the purpose of "spying" on the workers.

Question 2. Mr. Bahr, as you know, Section 5(a) would ban electronic monitoring to collect information "not relevant to the employee's work performance." If a bank has a security camera scan its premises, it would likely record many activities of employees, not all of which are relevant to work performance—such as chatting with a friend or taking a coffee break. This section appears to prohibit the use of the camera. Do you believe such use of the camera or other security devices should be banned as the bill appears to require?

Answer. My understanding is that the intent of Senator Simon's bill is not to ban monitoring but rather that employees must be made aware that they are being monitored. Obviously, all employees (as well as potential bank robbers) are aware that there are cameras monitoring the activity in the bank. No, I do not believe cameras or other devices required for security of the premises be banned by the bill, nor do I believe the bill does, so.

Question 3. Section 6(c) of the bill prohibits employers from collecting information which describes how an employee exercises First Amendment rights. Because almost all speech is protected by the First Amendment, this provision seems to totally prevent the use of monitoring by employers. How could employers using a camera or other monitoring device avoid collecting information about, protected speech?

Answer. I am not a constitutional lawyer and cannot give a legal response to your question. Unfortunately, rights that American workers have when outside of their workplaces do not carry forth into the workplace. The invasion of privacy horror stories told by countless workers that this bill is attempting to rectify, are apparently not covered by First Amendment rights. In conclusion, Senator, what Senator Simon seeks to do is to bring some human dignity and respect for the individual into the workplace. My understanding is that passage would not ban monitoring but would only require the worker to be aware that he or she was to be monitored at a given time. I hope this adequately responds to your concerns.

RESPONSES TO SENATOR THURMOND'S QUESTIONS FROM MR. MARX

Question 1. Do you believe that employers have the right to use electronic monitoring in order to protect their personnel and company property against intruders and theft?

Answer. Of course employers, as private citizens or government have the right (and indeed often the obligation) to protect their personnel and company property using electronic monitoring. But this should be done consistent with high ethical standards, the law, and common sense. As I note in my testimony, the debate around this bill is not about goals, it is about means. The glory of the United States is that it is a society under law in which means have a moral quality, as well as ends.

While I don't think it actually applies in this case (since protecting the innocent need not imply letting the guilty go), I am reminded of Justice Holmes words in Olmstead, "For my part I think it less evil that some criminals should escape than that the government should play an ignoble part." That sentiment also ought to apply to the private sector. Morality and value conflicts aside, pragmatism is a key variable here. The evidence suggests that unrestrained monitoring is actually counter-productive and will lead some employees to attempt to sabotage management's efforts. In this case protecting the innocent is likely to also mean fewer threats to company property.

Question 2. Section 6(c) of the bill prohibits employers from collecting information which describes how an employee exercises First Amendment rights.

Because almost all speech is protected by the First Amendment, this provision seems to totally prevent the use of monitoring by employers.

How could employers using a camera or other monitoring device avoid collecting information about protected speech?

Answer. I think what is important here is re-affirmation of the principle that First Amendment rights should be protected and there should be common sense on the part of employers and enforcement agents in implementing this. In supporting this part of the bill I responded to it's spirit, rather than its technical details. Perhaps some minor rewording and clarification is required here. But this is a procedural or technical objection that does not detract from the overall desirability of the Bill. In my testimony on pp. 13–15 I indicate the broad principles needed in the electronic age to guide data collection and use. This act supports those principles.

Question 3. Dr. Marx, S. 516 requires that employees be given notice of monitoring through buzzers, lights, or other similar means whenever monitoring is taking place.

Wouldn't this mean that no electronic monitoring could be done as part of a company investigation of an employee suspected of stealing?

Most thieves would be smart enough to wait until the monitoring light goes off, wouldn't they?

Answer. Again I think the key issue is the value of fairness and due process. I agree that where there are grounds for suspicion management should be able to proceed without warning the suspect. However it is a mistake to think that the only evidence of wrongdoing would come from electronic monitoring. In addition where monitoring is widely used it may serve as a deterrent. On balance more theft might be prevented via letting people know that they are being watched, than would be generated by warning violators. also by entering in the middle of a conversation it would be more difficult for a thief to cover up misbehavior. There are also issues of trade-offs and the damage from warning potential thieves must be balanced against the good that can come with threatening employees with dignity and creating a positive work environment.

Should you have additional comments or questions I would be pleased to respond.

RESPONSES TO SENATOR THURMOND'S QUESTIONS FROM MR. RUFFOLO

Question 1. Based on your experience and background, is it reasonable to say that most employees receive notice that they may be subject to monitoring when they go to work for a firm or company?

Answer. My experience is with the use of video cameras and other forms of monitoring done for security purposes. Employees who work for banks, groceries, and other businesses where security cameras are used are well aware of the presence of the cameras. Those employees who work in locations where card-access "keys" are used are aware that these card access devices keep track of employees who enter the secure area.

Question 2. We all know that crime, unfortunately, is on the increase in this country, and increasingly, because of the heavy burdens on our overworked police departments, the job of preventing crime is falling to private security firms. Are security companies and employees being given any new tools to fight crime? Are you getting any help from State legislatures?

Answer. It is getting more difficult for employers—including security companies—to conduct comprehensive, effective reviews of prospective employees. We are increasingly being held accountable for the activities of our employees, but we are not given good tools for doing background checks. Fear of liability has made most employers reluctant to provide any information when called for a job reference. Our attempts to screen prospective employees for felony convictions are frustrated by lengthy delays, typically from 3 to 9 months. Many states also deny us the ability to review motor vehicle records.

As you know, there are substantial restrictions on our use of polygraphs, and Congress is also considering limiting the use of credit reports and honesty tests.

Rather than providing help to us, I'm afraid we're having to fight against this kind of legislation at the State level too.

Question 3. Based on your experience, do employers or security personnel often misuse video cameras, for example, by taping in locker rooms, or is misuse a rare thing?

Answer. I have been in the security business for 28 years, and cannot recall even being asked to videotape in locker rooms or other private areas. I don't doubt chat if someone searches long enough it is possible to find an example of where a camera

has been used inappropriately, but that does not justify restricting the use of security cameras where they are effective tools for preventing or detecting crime.

One point that seems to have been overlooked during the debate on S. 516 is that electronic monitoring is commonly used to protect employees. An employee working late in an office building will certainly be more secure if the locks on the building are controlled by card access capable of identifying whomever is attempting the building. And a night clerk working in a convenience store certainly would be safer with a video camera scanning the store. Some internal investigations have also been done to prevent sex abuse from other employees.

Question 4. Based on your background, how effective could investigations of employees suspected of theft be if employees had to be warned before they could be investigated by electronic means?

Answer. Thefts in the workplace don't normally occur in front of witnesses. If an employer can identify the thief through other means, then the use of video may not be necessary. But if, for example, drugs were missing from a hospital pharmacy where six people had access, and the records didn't show who was responsible for the shortages, installation of a camera would be an appropriate and necessary investigative tool. Not only is the camera likely to find who is responsible for the crime, it would help clear suspicion from the other 5 people with access to the drugs.

Obviously, the installation of the camera at the hospital pharmacy would not result in apprehension of the responsible party if he or she had to be warned in advance, as required by S. 516. Although the announced use of a camera probably would stop the thefts from the pharmacy, it would not result in apprehension of the criminal. The individual who had been stealing the drugs would remain free to steal from other locations in the hospital, and management would remain suspicious of five innocent people.

Question 5. Some people argue that good management and investigative work can make the use of electronic security tools unnecessary. How would your work or the work of businesses be affected by the loss of these tools?

Answer. Good management and top-notch investigative work do not eliminate the need for electronic monitoring where it is appropriate. In fact, I believe that the judicious use of electronic monitoring for security purposes in many instances is a sign of good management.

No matter how competent, management will need to secure the business against intruders. In many instances this will be through an alarm, video, or card access system. In some businesses, such as the airline and banking industries, this security is required by Federal law.

As I indicated above, it is very difficult for employers to screen new employees thoroughly today. Also, most managers don't stand over the shoulder of their employees and watch them every minute. So regardless of how good a manager an employer is, he or she is at risk from internal theft. Once shortages occur, a manager should be free to work with security professionals to determine the responsible party and to deter further thefts. Sometimes, some form of electronic monitoring is called for as in the hospital example I cited above. There is no reasonable alternative that would accomplish the job of protecting the premises.

The loss of these technologies would make it impossible to prevent or detect some crimes. I don't think that's a price Americans want to pay.

Responses to Senator Thurmond's questions by Mr. Fineran

Question 1. Based on your experience and background, is it reasonable to say that most employees receive notice that they may be subject to monitoring when they go to work for a firm or a company?

Answer. In positions where monitoring is employed as a standard management practice, such as switchboard operators or customer service representatives, nearly all scrupulous employers provide notification upon employment. This notice most likely will include the ways in which information obtained from monitoring will be used and how the employee will be evaluated.

Using the definition of "electronic monitoring" in S. 516, however, employees may not be told that monitoring may occur simply because the so-called monitoring is incidental to the position. For example, employees who use word processors are not given a detailed description of how the employer uses information entered into the computer. But, the computer automatically stores the information it receives and thus becomes a form of monitoring under the definition of S. 516. A firm should feel free to ensure that equipment bought for the purpose of corporate productivity and improvement is being used for proper and authorized purposes. Employees generally know to call the data processing department to retrieve a back-up document, indi-

cating that they are aware that their work is kept for a time in the computer or on back-up tapes even though they may not have been told formally.

Question 2. Based on your experience, do employers or security personnel often misuse video-cameras, for example, by taping in locker rooms, or is misuse a rare thing?

Answer. I am unaware of any such incident. In general, however, legitimate videotaping of locker rooms or bathrooms could occur where there is probable cause for suspecting inappropriate behavior such as drug dealing. Most companies have policies against misuse, if for no other reason than to guard themselves against adverse publicity or from potential lawsuits using current Federal or state statutes. If misuse were common, I am certain that there would be more reported incidents.

Question 3. Based on your background, how effective could investigations of employees suspected of theft be if employees had to be warned before they could be investigated through electronic means?

Answer. While notification may help to reduce violations of corporate security and policy in a general manner, it tends to be counterproductive in individual cases. If, for instance, there appears to be general pilfering in a warehouse, a notice that video surveillance will begin should cut down considerably on the number of incidents. On the other hand, it would make it more difficult to determine who was and was not pilfering. In the case of embezzling, the corporation may find it necessary to obtain information through telephone logs, or monitoring of computer work and telephones. It is not hard to understand why companies would want to keep such an investigation secret, since notification would alert a guilty party of the company's suspicions and may give him or her time to cover culpable actions and evidence. In addition, how is a company supposed to conduct an investigation if it is forbidden from computer files where an employee may have input information that "is not relevant to an employee's work performance?"

Moreover, employees may not be notified formally of security procedures such as the fact that an access key records the employee's personal identification number, date, time and location of use. This is the case at NAM, which uses the information to determine who may have been in the building during a weekend when a theft occurred. The information may also be used to determine how a confidential document may have been leaked since it may indicate who was in a secure area at a given time.

Question 4. Some people argue that good management and investigative work can make use of electronic security tools unnecessary. How would your work or the work of businesses be affected by the loss of these tools?

Answer. In a word, drastically. In small offices monitoring may be considered unnecessary since everybody knows the level of work performance of everyone else. But in a vast majority of offices, it may be regarded as an essential management tool.

While it is true that a good training program is vital for telephone personnel, objective analysis provided by random, silent monitoring may also be viewed as an integral component. It provides an opportunity for both the employer and employee to benefit from hearing how the employee interacts with customers.

No amount of training will dissuade an employee who insists on chewing gum that the sound of it smacking in a customer's ear will be irksome unless mention is made either by a supervisor or the customer. Which is better? For a supervisor to point out the transgression or to allow a customer to become affronted? Without random, silent monitoring the employee will know when to remove the gum in order to avoid being caught by a supervisor. In the meantime several customers may have been left with a negative view of the company's courtesy.

Some companies may choose not to use random, silent monitoring for customer service or other telephone personnel; this does not mean that such a policy is right for every firm. The degree and manner in which the practice may occur should be allowed to vary.

Companies should be left to determine for themselves which policies—such as monitoring—work best within the particular corporate structure and philosophy. A poorly-run system will be counterproductive. This is not a reason, however, for a legislative mandate.

RESPONSES TO SENATOR THURMOND'S QUESTIONS FROM MR. MERLIS

Question 1. Based on your experience and background, is it reasonable to say that most employees receive notice that they may be subject to monitoring when they go to work for a firm or company?

Answer. Most employees know that they will be subject to monitoring when they are hired. Most employees know that their performance will be reviewed in order to determine when the employee merits a raise or promotion. The form of that review, including the types and frequency of monitoring, is usually spelled out to employees. Details of some covert monitoring for security purposes may not be spelled out—to do so would defeat the security objective. For example, security cameras may be installed in a baggage make up room to protect against or detect actual thefts of passenger baggage.

In the airline industry, telephone monitoring or service observation is a management technique to determine how employees speak with our customers. In this industry, the initial telephone contact is often the most crucial step in a transaction. Therefore it is in our interest to encourage employees to provide efficient, accurate service to the consumer and incumbent upon management to monitor individual employee performance.

Question 2. Based on your experience, do employer or security personnel often misuse video-cameras; for example, by taping in locker rooms, or is misuse a rare thing?

Answer. Misuse of security video-cameras is unpardonable and particularly costly to an airline. Misuse of security video-cameras takes expensive equipment away from security objectives and is not tolerated. Since reviewing video-tapes is a time consuming process, misuse also takes security personnel away from their assigned tasks.

Question 3. Based on your background, how effective could investigations of employees suspected of theft be if employees had to be warned before they could be investigated through electronic means?

Answer. Surveillance would be severely compromised if employees suspected of theft had to be warned before investigation by electronic means were launched. The terms of S. 516 are so broad its enactment would inhibit security investigations which extend to work place environments in which employees and non-employees mix; it would limit collection used to target who should be the subject of a theft investigation; and it would undermine the utilization of security devices for our passengers and employees in situations unrelated to job performance, i.e., detection of trespassers.

Question 4. Some people argue that good management and investigative work can make the use of electronic security tools unnecessary. How would your work or the work of businesses be affected by the loss of these tools?

Answer. The elimination of electronic security devices threatens to compromise the safety of the air transportation system. The deterrent effect of security devices should not be underestimated. In the years since the program began, the presence of magnetic scanning devices and x-ray machines at airports has resulted in the detection of thousands of weapons which were thus not illegally transported in the passenger cabins of airliners. The presence of security cameras in banks has served as a deterrent to bank robberies in the years since these have been instituted. Good management and investigative work are not substitutes for the fruits of technology which have resulted in many lives saved and crimes not committed.

Whether or not S. 516 is enacted, airlines will have to continue electronic monitoring for the safety and security of their passengers and employees.

RESPONSES TO SENATOR KASSEBAUM'S QUESTIONS FROM MR. MERLIS

Question 1. The most obvious application of this legislation in the airline industry would be to the monitoring of telephone calls to reservation centers. It, however, would also be applicable to employee fraud investigations that relied upon electronic monitoring. Could you address the impact this bill would have on the effectiveness of the airline industry to investigate charges of employee theft/fraud?

Response: From listening to the proponents of the legislation at the hearing, it appears as though the legislation was intended to deal with telephone monitoring. Regrettably it has been drafted so broadly as to affect all methods of electronic surveillance used for security, whether related to theft/fraud conducted by employees or others, employee security, and passenger security.

For example, the bill eliminates the utility of videotaping to prevent or investigate theft of baggage or electronic scanning of computer records designed to prevent or apprehend financial mismanagement. Even if the perpetrator of the perceived crime were not an employee, airlines would be precluded from undertaking appropriate investigations by these methods because information captured, retained, and scrutinized in the pursuit of the perpetrator would undoubtedly result in the collec-

tion of data which he or she would argue was not "relevant to employee work performance."

Secondly, a suspected perpetrator would know whenever electronic surveillance was being undertaken due to the requirement to provide affected employees with "a signal light, beeping tone, verbal notification, or other form of visual or aural notice, at periodic intervals, that indicates that electronic monitoring is taking place." (section 3(b)(3)). Fulfilling the requirements prescribed by section 3(b)(3) is tantamount to providing a road map to those intent on breaching security: A potential perpetrator of a crime who is outside the audible or visual range of the "light, beeping tone, or verbal notification" is also, of necessity, outside the range of the monitoring device. Thus, the establishment of this requirement alone would compromise a particularly important component of our security systems.

Question 2. It has been suggested that the language of S. 516, as drafted, is overly broad. In order to comply with the provisions of the bill, would the airline industry be in conflict with any FAA safety or security regulation, and if so, could you please state one or two specific examples?

Response: FAA security regulations impose access controls at certain locations in airports. These access controls provide security for the. aircraft, maintenance equipment and crew positioned on the ramp and intentionally compile data which identifies the individuals passing through the controlled access point and the time of passage. Clearly that personal data is not relevant to the employee's work performance and therefore is prohibited from being collected pursuant to the terms of section 5.

We are concerned that the audible tone notification (section 3(b)(3)) would interfere with communications between the flight crew, the air traffic controllers, and the flight operations base. Furthermore, the extraneous sound might interfere with accident investigation interpretation. The alternative to the "beep tone"—a signal light—would be distracting to crew members.

FAA safety requirements necessitate the recording of communications between the flight crew and the flight operations base. Much of the information collected in both the verbal format and the non verbal data stream has no bearing on employee work performance yet that compilation does identify the individual employees. That too would be precluded by the bill while required by the FAA.

FAA required maintenance data collected electronically may contain information having no bearing on actual employee work performance and therefore could not be collected, retained, and reviewed under the terms of the bill.

Question 3. Would an exemption in the bill to allow monitoring for compliance with FAA safety and security regulations adequately address the concerns of the airline industry with respect to this bill?

Response: No. We feel exempting FAA safety and security regulations insufficiently addresses the complexity of our business. Some FAA rules establish performance requirements which may be met through a number of different ways.

Furthermore, the bill is so broadly drafted it still would impede the ability of airlines, and other businesses, to conduct ordinary and necessary business activities. Even if FAA safety and security regulations were exempted from the bill, there is a very broad gray area which would subject airlines to expensive litigation.

For example, the bill does not exclude from its coverage terms and conditions of employment. Without such an exclusion, an employer could not collect any "personal data" on an employee "through electronic means which is not relevant to the employee's work performance." This would preclude electronic data collection of such basics as employee parking permit information, beneficiaries on company sponsored group life insurance, and identity of a health insurance carrier.

We believe the bill precludes the use of videotapes for security purposes. We could not employ the use of videotape cameras for employee security of a parking lot, for example, since those tapes may have nothing to do with "employee work performance," but clearly are forms of "electronic monitoring" containing "personal data."

We believe the bill precludes the retention of the services of a non-employee consultant or expert to analyze information which may also contain personal data. We are concerned the information disclosure limitation (section 5(b)) might preclude the use of such non-employee consultants or experts in analyzing safety or maintenance data which is collected.

We believe the bill limits package delivery companies in their tracking of packages tendered to them and which are in the custody of a delivery person.

With respect to covert monitoring for security purposes, we are concerned that the required forms of notice would undermine the security objective, undermine the deterrence effect of security systems, and provide a potential felon with critical information necessary to escape detection.

Whether or not FAA safety and security matters are retained in the bill, S. 516 does not indicate who has the option of dictating which form the notice of monitoring must take—the employer, the employee or the customer.

We are concerned that each modification to a data collecting software package risks requiring a new notice pursuant to section 3, since the predecessor notice would now be incomplete in some respect.

We are concerned with the ill-defined requirements to disclose electronic monitoring to prospective employees. Does a discussion at an employment office concerning potential job opportunities constitute a "meeting" within the meaning of section 3(b) for which notice of existing forms of electronic monitoring is required?

We believe the bill is unclear as to the extent and terms and conditions under which an employer has to provide "access to all personal data obtained by electronic monitoring" within the meaning of section 4. For example, would an employee be allowed to watch in their entirety videotapes taken at a facility subject to video monitoring? Would the employer be violating the privacy requirements of the bill if he failed to excise from such videotapes all employees, other than the one who requested the access to the "personal data obtained by electronic monitoring."

We are concerned the bill will add substantial costs for segregating and retaining data files containing information both relevant to and not relevant to an employee's work performance and permitting employee's access to the relevant information but not the non-relevant information.

Lastly, we feel the bill unjustifiably undermines the utility of telephone monitoring or service observation, a management technique to determine how employees speak with our customers. The make or break point in our transactions often occurs at the initial telephone contact. Therefore it is in our interest to encourage employees to provide efficient service and incumbent upon management to monitor both the aggregate picture of the business as well as individual employee performance.

Whether S. 516 is enacted or not, monitoring will and must continue to be used as a management tool to gauge efficient and effective customer service. This bill would eliminate the most efficient methods of monitoring employee telephone responses.

Senator SIMON. I thank all of you very, very much.

The subcommittee stands adjourned.

[Whereupon, at 4:35 p.m., the subcommittee was adjourned.]

○

150 93