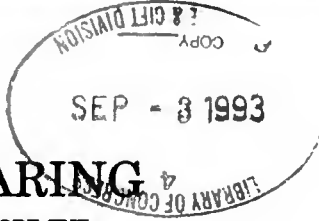


United States ...

S. HRG. 103-150

THE PRIVACY FOR CONSUMERS AND WORKERS
ACT

C693
248



HEARING
BEFORE THE
SUBCOMMITTEE ON
EMPLOYMENT AND PRODUCTIVITY
OF THE
COMMITTEE ON
LABOR AND HUMAN RESOURCES
UNITED STATES SENATE
ONE HUNDRED THIRD CONGRESS
FIRST SESSION

ON
S. 984

TO PREVENT ABUSES OF ELECTRONIC MONITORING IN THE
WORKPLACE, AND FOR OTHER PURPOSES.

JUNE 22, 1993

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



U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON : 1993

69-804cc

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402
ISBN 0-16-041308-7

COMMITTEE ON LABOR AND HUMAN RESOURCES

EDWARD M. KENNEDY, Massachusetts, *Chairman*

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

NICK LITTLEFIELD, *Staff Director and Chief Counsel*
SUSAN K. HATTAN, *Minority Staff Director*

SUBCOMMITTEE ON EMPLOYMENT AND PRODUCTIVITY

PAUL SIMON, Illinois, *Chairman*

TOM HARKIN, Iowa	STROM THURMOND, South Carolina
BARBARA A. MIKULSKI, Maryland	DAN COATS, Indiana
JEFF BINGAMAN, New Mexico	JUDD GREGG, New Hampshire
HARRIS WOFFORD, Pennsylvania	ORRIN G. HATCH, Utah
EDWARD M. KENNEDY, Massachusetts	NANCY LANDON KASSEBAUM, Kansas
(Ex Officio)	(Ex Officio)

BRIAN KENNEDY, *Chief Counsel and Staff Director*
TODD ATWATER, *Minority Counsel*

(II)

91-117533

KF26
 h2737
 1993a

C O N T E N T S

STATEMENTS

TUESDAY, JUNE 22, 1993

	Page
Simon, Hon Paul, a U.S. Senator from the State of Illinois, prepared statement	2
Ettienne, Franklin, room service busser, Boston, MA, and Charles Piller, senior associate editor, Macworld, San Francisco, CA	3
Piller, Charles, prepared statement	6
Johnson, Gwendylon, board of directors, American Nurses Association, Washington, DC; Barbara J. Easterling, secretary-treasurer, Communications Workers of America, Washington, DC, and Lewis L. Maltby, director, National Task Force on Civil Liberties in the Workplace, American Civil Liberties Union, New York, NY	12
Prepared statements of:	
Ms. Johnson	14
Ms. Easterling	18
Mr. Maltby	
3	
Thurmond, Hon. Strom, a U.S. Senator from the State of South Carolina, prepared statement	28
Gerdelman, John, senior vice president, customer markets, MCI, Arlington, VA; Michael J. Tamer, president, Teknekron Infoswitch Corporation, Fort Worth, TX, and Richard J. Barry, member, Security Companies Organized for Legislative Action, Boston, MA	27
Prepared statements of:	
Mr. Gerdelman	30
Mr. Tamer	34
Mr. Barry	38
Bowers, Diane K., president, Council for Marketing and Opinion Research	43

APPENDIX

Articles, publications, letters, etc.:	
Bosses with X-ray Eyes, by Charles Piller, a special report from Macworld	46
Vasco, Sarah Ann, Southern California Gas Company, letter from, dated June 16, 1993	57
Letter to Senator Paul Simon, from Richard A Barton, senior vice president, government affairs, Direct Marketing Association, Inc., Washington, DC, dated June 25, 1993 (with attachments)	60

THE PRIVACY FOR CONSUMERS AND WORKERS ACT

TUESDAY, JUNE 22, 1993

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

The subcommittee met, pursuant to notice, at 9:35 a.m., in room SD-430

Dirksen Senate Office Building, Senator Paul Simon (chairman of the subcommittee) presiding.

Present: Senators Simon and Thurmond.

OPENING STATEMENT OF SENATOR SIMON

Senator SIMON. The subcommittee hearing will come to order.

We are having a hearing today on S. 984, the Privacy for Consumers and Workers Act. What we aim to do is to protect the privacy of people at workplaces, as well as consumers, and do it in a way that will not inhibit and harm businesses. And we think that can be done.

We have had a number of constructive recommendations related to the bill as it was originally introduced in the last session of Congress. They have been included in this legislation. It is very easy in a world of increasing technology to give away basic rights of privacy that are implied in the Constitution. The phrase, "the right of privacy," is not used in the Constitution, but when the Constitution was written, they said, as they wrote it in 1787, that you couldn't be forced to have troops quartered in your home. They said you couldn't invade your home unless you had a very specific search warrant.

And then the Ninth Amendment was written by James Madison when he wrote the Bill of Rights. He sent a rough draft of the Bill of Rights around to a few people, and Alexander Hamilton wrote back and said if you spell out these rights in the Bill of Rights, there will be some people who will say these are the only rights people have.

So James Madison wrote the little-noted Ninth Amendment, which is extremely important to our basic liberties, and in that Ninth Amendment, he says other rights not spelled out here are reserved to the people.

So when you combine that with the provisions on quartering troops, and you have to have a specific search warrant, there is clearly an implied right of privacy that is there in the Constitution.

But those who wrote it did not imagine telephones and computers and television screens and all the things we have today.

How do we apply those basic principles to the technology of today? That is the fundamental question we are asking here today, and we have a fairly long list of witnesses. We will abide by the 5-minute rule, and we will enter all statements in the record, but we will be fairly strict in the enforcement of the 5-minute rule.

Let me also apologize to witnesses in advance. At 10:30, the Senate is scheduled to have a vote, and I will have to go over, so we will have at that point a 10- or 15-minute recess and then resume the hearing.

[The prepared statement of Senator Simon follows:]

PREPARED STATEMENT OF SENATOR SIMON

Today the Subcommittee on Employment and Productivity will hear testimony regarding S. 984, the Privacy for Consumers and Workers Act, which would prevent abuses of electronic monitoring in the workplace.

I believe the legislation before us today reflects a number of constructive recommendations, some of which were suggested at a hearing held before this subcommittee last Congress.

As I have said before, the Privacy for Consumers and Workers Act does not prohibit electronic monitoring from ever being used; it does say it should not be abused. S. 984 is simply a right-to-know bill, and strikes a careful balance between the demands for technological change and the need to protect an individual's privacy.

Just over the horizon are more technology breakthroughs and refinements that we can't even envision today. Unless we begin now to define privacy—and in particular workplace privacy—as a value worth protecting, these new technologies will be upon us before we are ready for them. Weighing these issues will allow us to be the masters of the technology, instead-of its slaves.

Employees should not be forced to give up their freedom, dignity, or sacrifice their health when they go to work.

Given rising health care costs and our nation's health care crisis, employees' health should not be over looked. Workplace stress is one of our country's leading health problems. The stress that employees face due to electronic monitoring is costly. According to a 1993 International Labor Union report, American business loses \$200 billion annually in health care costs and lost productivity. The American Civil Liberties Union (ACLU), reports that stress is the symptom of potentially serious medical problems most frequently reported by employees who are subjected to covert telephone and computer surveillance. The ACLU also reported that workplace stress alone is costing more than \$50 billion annually. This is a cost we cannot afford.

Moreover, current electronic monitoring practices operate as a form of de facto discrimination. Women are disproportionately represented in the types of jobs that are subjected to electronic monitoring; such as clerical workers, telephone operators, and customer services representatives.

Countries such as Japan, Germany, Sweden, Norway, Austria, Britain, and France seriously limit or regulate the electronic monitoring practices of business because of strong beliefs of workers'

right-to-privacy, and concerns for worker health and productivity. These strong competitor countries go much farther than S. 984. Moreover, in Japan, laws to regulate or limit electronic monitoring aren't needed. Japanese employers on the whole do not electronically monitor their employees, except for some limited personal data such as payroll records, employee qualifications, and service records. The practice of not engaging in electronic monitoring stems from a general reverence for privacy in Japanese society. One would think that given our own history, our reverence would be as great.

I look forward to the testimony being presented today.

Our first witnesses are Franklin Ettienne, a room service busser from Boston, MA, and Charles Piller, senior associate editor of Macworld, from San Francisco.

We are very pleased to have both of you with us. Mr. Ettienne, we'll start with you.

**STATEMENTS OF FRANKLIN ETTIENNE, ROOM SERVICE
BUSSEER, BOSTON, MA, AND CHARLES PILLER, SENIOR ASSO-
CIATE EDITOR MACWORLD, SAN FRANCISCO, CA**

Mr. ETTIENNE. Good morning, ladies and gentlemen.

Senator Simon, my name is Franklin Ettienne. I am honored by the invitation to address this committee.

I have lived in the United States of America for 7 years. My country of birth is Haiti. It was not easy for me to leave my home and family, but I wanted to come to America to study and have a better life.

In October 1986, I landed in America. I was very happy and excited. I no longer had to be scared of the military or secret police. In America, no one is persecuted, everybody is welcome. It is the country of freedom.

My first job in America was at a restaurant washing dishes. At the same time, I went to school to learn English.

In 1987, I started to work at the Sheraton Boston Hotel. I knew I was expected to work hard and be honest. After 6 months, my reward was being promoted to room service busser. I was proud to work at the Sheraton, and I believed they respected me and my work.

My new job gave me the opportunity to support my wife and two children, as well as go to school full-time. I am a junior at Bunker Hill Community College and have made the national deans' list.

I am a member of Local 26 of the Hotel Employees Restaurant Employees International Union. In August of 1992, the union asked me to look at some videos that had been secretly taped in the men's locker room of the Sheraton Boston Hotel. I was shocked at what I saw; shocked and upset. The video showed me on break, studying and doing homework in the locker room. Coworkers were shown, dressing and undressing.

I could not believe what I saw. I was very angry. I felt that the Sheraton Hotel had taken something away from me. Instead of the anticipation that my work and school were giving me, the opportunity to build a better life for myself and my family, I began to feel nervous and under stress.

I was very proud to get this invitation to address the U.S. Senate. I thought it was important to come to this hearing so that what happened to me will not happen to other people who come to America with the same hopes for freedom.

I want to bring up my three children with the expectation that they can have their privacy and freedom. In America, sometimes you take freedom for granted. People in other countries are fighting and dying for it. Yet the Sheraton Hotel, without hesitation, has denied this to their workers. I hope this committee acts to protect our rights.

I know the Sheraton is concerned about their regulations. Yet they must find a way to enforce rules without sacrificing our individuality or the personal freedom this country is based on.

I have applied to become a U.S. citizen and have studied with my union education program. I have read the history of many Americans who built the foundations of dignity and respect for individual freedoms. It is those values that make me and my family strong.

I respectfully suggest you keep in mind protecting these liberties when you put your bill together.

Thank you.

Senator SIMON. We thank you. We wish you the best, and we hope you'll raise that right hand and become an American citizen very soon; you are going to be a good one.

Mr. Piller.

Mr. PILLER. Thank you very much, Senator Simon.

As a consumer and business magazine, Macworld is naturally interested in the role computers play in the workplace, and we have closely followed the growing concern expressed by many computer users that computer-based surveillance undermines personal privacy on the job.

Drawing on our expertise about the way in which computers operate, we recently published a wide-ranging investigation into the effects of electronic technologies on workplace privacy.

We have known for some time that electronic monitoring has become pervasive in occupations involving highly repetitive tasks. But as we began our study, we found little hard data regarding how easily electronic surveillance could be applied to professional or technical jobs. We also noticed that employers themselves have not been polled about their use of electronic surveillance tools.

Therefore, Macworld conducted a three-tiered investigation. We looked at software products that manage the workplace computing environment, conducted a nationwide survey of employers to determine their electronic eavesdropping practices, and spoke to employers and workers about their views on this subject.

To save time, I will concentrate on the survey, but I would be happy to answer questions on any aspect of the report.

Before I explain the survey results, however, I should note that our software tests show that in an office environment using a full-featured network operating system, and operated by a competent network administrator, every computer and all data transferred within that network is an open book.

Employees who assume that their jobs are too varied or complex to evaluate by machine fail to grasp the nearly unlimited electronic monitoring potential available to any employer.

So the capacity to snoop is there, but is it used? Macworld asked top corporate managers at 301 businesses of all sizes and in a wide range of industries how much they peer at their employees' work on their computers and why. Two of the charts up there explain some of our results.

The survey confirmed that electronic eavesdropping is popular among American employers. Some 22 percent of respondents have engaged in searches of employee computer files, voice mail, electronic mail, or other networking communications. In large companies, that figure actually rises to 30 percent.

Our survey sample directly represents conditions experienced by about one million workers. Extrapolated to all similarly sized companies, these data suggest that some 20 million Americans may be monitored on the job through their computers.

I should add, however, that relatively few employers use electronic surveillance on an everyday basis. While nearly half of the managers in our survey endorsed the concept of electronic surveillance, only about 6 percent of respondents conducted electronic searches 50 or more times in the preceding 2 years. Most employers conducted such searches very few times during that period.

These data strongly suggest, however, that advances in computer-based surveillance technology have outpaced the minimal legal protections for workplace privacy. Some companies argue that self-regulation better serves both employer and employee interests on this issue. But only 18 percent of respondents had a written policy regarding electronic privacy.

Moreover, among executives who acknowledge using electronic surveillance methods, secret monitoring is the norm.

I would like to touch briefly on one other aspect of our investigation which is privacy for individuals in their financial, consumer and legal transactions, and in their efforts to secure a new job.

In recent years, home addresses and phone numbers, marital, salary and employment histories, Social Security numbers, buying habits, business affiliations, vehicle and real estate holdings, civil and criminal court records, and much of the rest of the information trail left by all of us had become readily available from scores of commercial or governmental on-line databases. To explore the impact of those databases, Macworld conducted an on-line experiment.

First, we selected 18 prominent individuals, including Office of Management and Budget Director Leon Panetta; Hollywood producer and friend of President Clinton, Harry Thomason; football star Joe Montana; and Bank of America CEO Richard Rosenberg. We tried to find out everything we could about them with these restrictions. We did not seek legally protected data, and all the information we looked for had to be obtained on-line.

For this modest search, we spent only about \$100 per subject and about an hour per subject. Even so, we unearthed the essential financial, business, legal, marital and residential histories of most of our subjects. In short, we compiled electronic dossiers.

There are good reasons for many records to remain public documents, of course, but easy access has blurred the borders of private life. Our on-line experiment and our survey highlight a daunting challenge: How can society protect the right to personal privacy while preserving the legitimate prerogatives of employers and the vital checks and balances of an open society?

Clearly, Government should take a fresh look at the invasive electronic technologies that offer unprecedented opportunities to pry into private moments or private lives.

I applaud your efforts to tackle this difficult subject. Thank you.

[The prepared statement of Mr. Piller follows, and the extraneous material appears in the appendix:]

PREPARED STATEMENT OF CHARLES PILLER

My name is Charles Piller and I am a senior associate editor at *Macworld* magazine. I am also the author of two books concerning the social and political implications of technology. *Macworld* is a consumer and business magazine that helps readers make buying decisions regarding computer products; we also cover issues that pertain to the social impact of computers.

Macworld is naturally interested in the role computers play in the workplace, and we have closely followed the growing concern expressed by many computer users that computer-based surveillance by managers has undermined personal privacy on the job. Our expertise about the way in which workplace technologies operate gives us a strong basis on which to evaluate those concerns. We recently conducted an wide-ranging investigation into the effects of electronic technologies on employee privacy. Before I explain our findings, which appear in the July issue of *Macworld*, I'd like to offer some context.

HOW AGE IS THE ISSUE?

The 1986 Electronic Communications Privacy Act prohibits phone and data-line taps with two exceptions: law-enforcement agencies and employers. The police or FBI can tap lines—but only as a last resort under court order—to gather evidence on criminal conspirators, drug traffickers, and other serious-crime suspects. The courts permit fewer than 1000 such taps each year, nationwide. Employers suffer from no such limits. They may view employees on closed-circuit TV; tap their phones, e-mail, and network communications; and rummage through their computer files with or without employee knowledge or consent—24 hours a day if they so desire.

We've known for some time that electronic monitoring has become a pervasive employer practice for occupations involving highly repetitive tasks. Millions of times per year telephone operators, airline sales agents, mail sorters, word processors, data-entry clerks, insurance claims adjusters, and even computer technical-support specialists, often working on terminals connected to a mainframe, may be monitored constantly or intermittently for speed, errors, and time spent working.

Numerous national polls have indicated that the general public is extremely concerned about personal privacy. Many people believe that the computers have made their lives less private. Anecdotal reports from individual workers and from a newly established privacy information service in California, as well as informal polls sponsored by labor advocates all suggest that American workers are deeply concerned about workplace privacy.

But as we began our investigation, we found little hard data regarding how easily employers can spy on the various aspects of an employee's computing environment. We also found little information on whether electronic surveillance methods could be used effectively in regard to professional and technical jobs. We also noticed that employers themselves had not been asked how widely or frequently they eavesdrop on employees through their computers.

HOW WE SOUGHT ANSWERS

Macworld then conducted a three-tiered investigation: We looked at the software products that manage the workplace computing environment, conducted a nationwide survey of employers to determine their electronic eavesdropping practices, and spoke to employers about their views of electronic surveillance.

Macworld examined 25 popular network-management, integrated groupware, electronic-mail, and remote-access products to see if they could be used to invade employee privacy, and if so, how easily. The study used only computer software designed for the Apple Macintosh, but similar tools are available for any desktop personal computer, as well as mainframe- and mini-computer based systems.

If an office network uses a full-featured network operating system and is run by a technically sophisticated network manager, then every computer and all data transferred within that network is an open book. Working from a computer across the room or across the country, a network manager—particularly in server-based local area networks (systems that use a dedicated central computer to store and distribute network communications)—can view virtually every aspect of a networked computing environment with or without the approval or knowledge of end users. The manager can see the contents of data files and electronic-mail messages, overwrite private passwords, and audit any employee's time and activities on the network.

All the major groupware products that combine messaging, file management, and scheduling allow network administrators to change passwords at any time, then read, delete, or alter any messages on the server. With few exceptions, network-administration programs allow astute managers to read files transmitted over the net. In short, these tools are only slightly less invasive than others specifically designed for surveillance and used primarily on mainframe systems.

The implications of our tests are clear: Employees who assume that their jobs are too varied or complex to evaluate by machine fail to grasp the nearly unlimited electronic monitoring capability available to any employer.

ACTUAL EMPLOYER PRACTICES

The capacity to snoop is there, but is it used? Old surveys and anecdotal accounts suggest that in some industries—telecommunications, insurance, and banking, for example—telephone or computer-based monitoring runs as high as 80 percent of employees. Such estimates may be inflated, but there is little dispute that many employers monitor routinely. And if the rapid growth of snooping tools is an indication, monitoring is on the rise.

But virtually no rigorous research had been done about how much electronic eavesdropping takes place on the job. Therefore *Macworld* conducted a survey of top corporate managers at 301 businesses of all sizes and in a wide range of industries to find out how much they peer into their employees' work on their computers, and why (see the chart, "Electronic Eavesdropping At Work").

Nearly 22 percent of our survey sample has "engaged in searches of employee computer files, voice mail, electronic mail, or other networking communications." In large companies with 1000 or more employees, the figure rises to 30 percent. Nearly 16 percent of respondents reported having checked computerized employee work files.

The average company in our study employs more than 3,200 people, so the total sample directly represents conditions experienced by about 1 million workers. When extrapolated to all similarly sized companies, these data suggest that some 20 million Americans may be subject to electronic monitoring through their computers (not including telephones) on the job. Moreover, among executives who acknowledge using electronic surveillance methods, fewer than one-third warn employees that such methods are in use.

Our findings about electronic mail were particularly interesting in light of a common myth. Most people believe that electronic-mail messages are secured by their personal password-as private as a letter in the U.S. mail. E-mail is actually more like a postcard. The Electronic Communications Privacy Act treats internal workplace communications as company property. And the *Macworld* survey suggests that many employers agree. About 9 percent of respondents—representing some 375,000 employers—indicated that they sometimes search employee e-mail files.

I should add, however, that relatively few employers use these types of electronic surveillance on an everyday basis. While nearly half of the managers in our survey endorse the concept of electronic surveillance, and more than a fifth actually use such techniques, only about 6 percent of respondents who had searched employee work files, voice mail, electronic mail, or networking communications did so 50 or more times in the preceding two years. About 71 percent of those who conducted such searches did so only live or fewer times during that period.

EMPLOYER PRIVACY POLICIES

For the third piece of our investigation I spoke directly with employers about their policies and practices. Managers who endorse electronic surveillance say that it

helps them gauge productivity and chart the work flow of employees. It can generate statistics on individual or departmental accomplishments and plot future workloads. Computer monitoring can even be used to give employees feedback and reduce the need for personal attention from supervisors, some employers argue. Twelve percent of our survey respondents endorsed monitoring for evaluating performance or productivity.

Monitoring can also increase employee safety or adherence to company rules, according to other employers. Some trucking companies, for example, set on-board monitors to record speed, engine-idling time, and length of stops. Such systems ostensibly ensure that truckers drive safely and take adequate rest breaks.

And companies that deal in sensitive information may understandably feel compelled to protect valuable data against disloyal or merely careless employees who might divulge it to competitors. Four percent of our survey respondents endorsed electronic monitoring "for routinely verifying employee honesty." A much higher number—23 percent—called electronic monitoring a good tool where reasonable evidence of wrongdoing—such as theft or negligence—comes to light.

Many companies recognize growing consumer demand for privacy protections, and they have stepped forward with pioneering consumer privacy policies that go far beyond limited legal requirements. But few company policies go as far to protect employee privacy as the Privacy for Consumers and Workers Act would mandate.

Companies that have led the way on consumer-privacy concerns, such as American Express, Citibank, and Equifax, describe their electronic monitoring of employees as strictly limited. But they would not release internal policies on employee privacy, and they acknowledged surveillance practices beyond what would be allowed by some features of the proposed legislation.

THE MEANING OF OUR DATA

What conclusion can be drawn from our electronic privacy investigation? One can hardly fault employers for trying to guard against ineptitude or criminality. But should they be free to search at will any and all employee computer files, electronic-mail, voice-mail, and data transmissions over a company's local area network?

For about one-third of our survey respondents, the answer is no. They reject electronic surveillance under any circumstances. Many employers recognize that excessive monitoring may have negative side effects—such as increases stress related illness, lowered morale, and ironically, lowered productivity—defeating an often-expressed purpose of electronic surveillance.

We certainly can conclude that technological change in the realm of computer monitoring has outpaced, by a wide margin, the development of laws that protect personal privacy on the job. Some companies argue that self-regulation would better serve both employer and employee interests on this issue. But according to our survey, only 18 percent of respondents' companies had written policies regarding electronic privacy—fewer than the number that actually uses electronic surveillance tools. In effect, many employers have become spies who covertly target their own employees.

A MODEL APPROACH TO EMPLOYEE PRIVACY

After completing my research on electronic privacy I outlined basic features for a good electronic-privacy policy for employers. These principles—which overlap with some basic features of S. 984—are designed to safeguard employee privacy without sacrificing important management interests:

Employees are entitled to reasonable expectations of personal privacy on the job.

Employees know what electronic surveillance tools are used, and how management uses the collected data.

Management uses electronic monitoring or searches of data files, network communications, or electronic mail to the minimum extent possible. Continuous monitoring is not permitted.

Employees participate in decisions about how and when management conducts electronic monitoring or searches.

Data is gathered and used only for clearly defined work-related purposes.

Management will not engage in secret monitoring or searches, except when credible evidence of criminal activity or other serious wrongdoing comes to light.

Monitoring data will not be the sole factor in evaluating employee performance.

Employees can inspect, challenge, and correct electronic records kept on their activities or files captured through electronic means.

Records that have become irrelevant to the purposes they were collected for will be destroyed.

Monitoring data that identifies individual employees will not be released to any third party, except to comply with legal requirements.

Employees or prospective employees cannot waive privacy rights.

Managers who violate these privacy principles are subject to discipline or termination.

MONITORING OF JOB APPLICANTS

I would also like to draw attention briefly to a closely related issue—the growing use of online databases for pre-employment checks of job applicants or to investigate new employees. Managers have become some of the biggest users of online databases. They turn to these tools to investigate job seekers or recent hires. Such managers check online credit and criminal records in a matter of minutes; they often reject applicants whose records show a large debt burden, or who were once convicted of a crime, however old the conviction.

This practice sometimes screens out individuals who may be inappropriate for a given job. But it casts a wide net. Should, for example, a single 10-year-old drunk-driving conviction forever ban a person from work involving precision equipment or the operation of heavy machinery?

When data is not available in electronic form—such as with school transcripts—employers often hire research services to obtain transcripts and deliver their contents to the client's on-line account in a day or two.

And until last summer, many employers searched online data banks to find out whether a job seeker had ever filed a workers-compensation claim—an insurance claim for an on-the-job injury. Some employers refused to hire anyone who had ever filed a comp claim. The Americans with Disabilities Act, signed into law last year, limits the use of such data banks before a firm offer of employment has been made. But if an employer finds a history of compensation claims after making a job offer, the employer can shift the prospective employee to a job classification that reduces risk of reinjury. If in the employer's opinion no appropriately safe job is available, the job offer can be rescinded.

Employers have a responsibility to protect themselves from potential liability. But the increasing use of electronic research tools has the effect of opening all job applicants to a kind of scrutiny that many people consider unwarranted, or even antithetical to basic principles of fairness. It begs the question: Is society well served by a business culture that can blacklist people with the cool efficiency of a high-speed modem?

THE LARGER REALM OF PRIVACY

Finally, *Macworld* looked another closely related issue—privacy for individuals in their financial, consumer, and legal transactions. In recent years, gathering and sharing personal information has become a way of life for business and government. People have kept track of each other for millennia, of course. But vast, accessible computerized databases have made personal data easily available to anyone for a modest price.

Home addresses and phone numbers; marital, salary, and employment histories; social security numbers, buying habits, corporate affiliations; names, addresses and income estimates of neighbors or relatives; vehicle and real estate holdings; civil and criminal court records, and much of the rest of the information trail left by all of us are now available from scores of commercial or governmental sources. Even legally shielded or difficult-to-obtain data—such as credit, medical, and phone records, as well as arrests that do not result in convictions—are routinely revealed to a wide range of qualified or merely determined and savvy requesters. These include private investigators, the press, FBI agents, lawyers, insurance companies, corporate spies, and vindictive ex-spouses.

From a personal computer anywhere in the world, data can be gathered from limitlessly broad and diverse sources. The ability to capture, sort, and analyze that data is often nearly instantaneous. The force of such tools has overwhelmed the capacity of laws and social mores to protect privacy. New records kept by government, corporations, and employers come online all the time. Nearly every quantifiable aspect of our lives—and many a judgment call—finds its way into data banks where it is exchanged, sold and resold, again and again. Easy access to such records has blurred the borders of private life.

The new standards of electronic intrusion upset the balance between two distinctly American values: an open and accountable society, and the right to be left alone. In order to explore the significance and impact of new electronic research tools, *Macworld* conducted an online experiment.

First we selected 18 prominent individuals, including Office of Management and Budget Director Leon Panetta; President Clinton's friend, Hollywood producer Harry Thomason; football star Joe Montana; and Bank of America CEO Richard Rosenberg. Then we tried to find out everything we could about them, with these restrictions: We did not look for legally protected data, and all the information had to be obtained online.

For this modest search we spent a little over \$100 and about one hour per subject. Even so, we unearthed the essential financial, legal, marital, and residential histories of most of our subjects (see the chart, "Shattering the Illusion of Privacy"). In short, we compiled electronic dossiers. As on-line services become increasingly interconnected, affordable, and fast, the ability to build electronic dossiers may become the hottest privacy issue of the next century.

Our online experiment, combined with the rest of Macworld's investigation, highlights a daunting challenge: How can our society protect the right to personal privacy while preserving the legitimate prerogatives of employers and the vital checks and balances of an open society? The answer, in part, is that government must take a fresh look at invasive electronic technologies that offer unprecedented opportunities to pry unnecessarily into our private moments or private lives. Experience has shown that the wholesale erosion of personal privacy in the marketplace and the workplace will continue unabated without such intervention.

Senator SIMON. Thank you.

If I may ask you, Mr. Pillar, when we ask are privacy policies known to employees, and roughly two-thirds respond no—

Mr. PILLER. That's correct, Senator.

Senator SIMON. —as you view business practices—and you are in the private sector—would it hurt those businesses if, when they have surveys, they could let employees know in advance that they are going to have them? What is your off-the-top-of-the-head reaction?

Mr. PILLER. In my discussions with employers in researching this report, I noticed that in the vast majority of cases, employers did not really object to having a stated policy on privacy, but I think the case is more that the technological capabilities that they have obtained have gone faster than their internal ability to regulate those technologies.

Senator SIMON. And if we had some guidelines and rules in the law, this would not impede unnecessarily things that employers need to do from time to time.

Mr. PILLER. I don't think so, sir. I would just point out that I think two of the major criticisms that are made by employers regarding the legislation are, one, that they feel that self-regulation would actually be a more effective means of achieving the same goals. In response to that, I wanted to point out that if indeed that's the case, there is not very much evidence of it out in the private sector right now because so few companies have privacy policies, and of those privacy policies themselves among the few companies who are willing to release them to us—and I might add that it was very few companies who were willing to do so—those policies were very mild and actually went only a short distance along the path that you are travelling with your legislation.

Of course, the other aspect is the question of employee productivity. Many employers feel that it is essential to have the ability to survey employees in order to verify productivity and to monitor work progress. But I might point out that the concerns are based on fear of competition from countries that actually have much more protective privacy policies for employees.

Senator SIMON. And under this legislation, we would not prohibit employers from monitoring productivity. We simply say these are the rules you have to follow as you monitor productivity.

And isn't it also true that there are studies that show that employees who are satisfied are more productive employees, and there is an element of dissatisfaction and unhappiness, as Mr. Ettienne has indicated, when employees discover that they have been monitored without their knowledge?

Mr. PILLER. Yes, sir, and as a matter of fact, there has been some fairly good research recently done on this subject that has identified excessive monitoring to be connected with undue stress in the workplace, which of course leads to both low morale and reduced productivity. And I think many enlightened employers understand that.

As a matter of fact, one of the findings of our survey was that about a third of all employers believe that electronic monitoring is never an acceptable management practice, and I think that speaks strongly toward the enlightened perspective that employees are actually not seeking to be dishonest or otherwise sloughing off on the job.

Senator SIMON. Mr. Ettienne, under this legislation, the video camera that was in your locker room and took pictures of employees dressing and undressing and so forth would be prohibited. If you prohibited that for the Sheraton Hotel where you work, would that in any way do harm to the Sheraton Hotel? Do you understand my question?

Mr. ETTIENNE. Can you repeat that again for me, please?

Senator Simon Under this proposal that we have right now, the Sheraton Hotel could not take the kind of video that you viewed; they would be prohibited from taking videos in a bathroom or in a dressing room.

Do you feel that if we were to make this the law, that would hurt the Sheraton Hotel?

Mr. ETTIENNE. The Sheraton Hotel is wrong; it should be illegal. When you work someplace, the reason they give you that 30-minute break or 45-minute break is to have somewhere that you can rest and mentally be free. So what they did to us is really wrong, and that is why all the workers at Sheraton are very upset, because Sheraton has taken something away from them.

So I believe they are wrong, and the reason that we have come forward is in order to send a clear message to the American people so that they can see that at Sheraton, they don't respect workers' privacy.

Senator SIMON. And under this legislation, if law enforcement officials felt someone was exchanging drugs in a bathroom, then law enforcement officials, with court approval, could monitor, but otherwise you can't take pictures in bathrooms and dressing rooms. Would that be a good thing?

Mr. ETTIENNE. I believe that is why they have security working at the hotel, so that if they know someone is dealing drugs in the hotel, what they are supposed to do is send the security officials to the locker room in order to catch the person who is doing that. When they put the hidden cameras, and did not tell us, we believe that should be illegal. They did not tell anybody, even the union

president, about it. So they know that they have taken something away from us, which is our privacy. They are supposed to have the security who work at that place check often in order to see who is dealing the drugs, because not everybody is dealing drugs at the Sheraton—also, I have never heard of anybody dealing drugs there.

Senator SIMON. All right. We thank you both.

Mr. Piller, I would be interested in receiving copies of any articles you have written in this field, because I think you are onto something that is really very basic in our society.

We thank you both very much for your testimony.

Mr. PILLER. Thank you, Senator Simon.

Mr. ETTIENNE. Thank you, sir.

Senator SIMON. Our next witnesses are Lewis Maltby, director of the National Task Force on Civil Liberties in the Workplace of the American Civil Liberties Union; Barbara Easterling, secretary-treasurer of the Communications Workers of America, and Gwendylon Johnson, a member of the board of directors of the American Nurses Association.

Unless you have any other personal preferences, we'll start with you, Ms. Johnson.

STATEMENTS OF GWENDYLON JOHNSON, BOARD OF DIRECTORS, AMERICAN NURSES ASSOCIATION, WASHINGTON, DC; BARBARA J. EASTERLING, SECRETARY-TREASURER, COMMUNICATIONS WORKERS OF AMERICA, WASHINGTON, DC, AND LEWIS L. MALTBY, DIRECTOR, NATIONAL TASK FORCE ON CIVIL LIBERTIES IN THE WORKPLACE, AMERICAN CIVIL LIBERTIES UNION, NEW YORK, NY

Ms. JOHNSON. Thank you, Senator. Good morning.

I am Gwendylon Johnson, former president of the DC. Nurses Association and member of the board of directors of the American Nurses Association. I appreciate the opportunity to testify today representing American Nurses Association and its 53 State and Territorial nurses associations, on behalf of the Nation's 2 million registered nurses.

ANA supports passage of S. 984, the Privacy for Workers and Consumers Act, with its emphasis on providing protections against electronic monitoring. The bill addresses three factors of particular concern to nurses: the intrusive and basic nature of electronic monitoring; the growth in technology which will continue to make new forms of monitoring available, and the added stress to employees who are subjected to electronic monitoring.

Finally, as consumers of services which could be monitored, and as patient advocates, we support the provisions of the bill which are designed to protect the privacy of consumers.

From childhood, most of us are taught the basic tenets of respect for the privacy of others. We learn not to listen at closed doors, and to immediately put down a telephone if we pick it up and hear voices. We learn that eavesdropping is wrong. We certainly learn not to peek through other people's curtains or observe our friends through cracked doors. Yet the sophisticated technology and workplace production demands have made such practices commonplace, even acceptable, in too many workplaces across the country.

In recent years, we have seen troubling examples of electronic monitoring which unnecessarily invades the privacy of nurses. This committee is aware of the case of nurses at a hospital in Maryland who discovered a hidden video camera in their dressing room, broadcasting their activities to an in-house cable channel.

This is unfortunately not an isolated incident. Nurses at other facilities have found video cameras in their locker rooms. No doubt many other monitoring devices have gone undetected. This practice is discriminatory, invades privacy, raises sexual harassment concerns and is clearly unacceptable.

We fully support the provision that S. 984, which would prohibit the monitoring of locker rooms, bathrooms or dressing rooms. We do not believe such a blatantly intrusive practice should be legal.

ANA believes that workplace privacy issues must be vigilantly monitored. To many times, employees and enforcement officials attempt to use medical testing or technology to address criminal, safety and compliance activities related to employee behavior.

Employers have a responsibility to provide employees adequate orientation to their jobs, education and retraining to maintain competency and appropriate supervision and evaluation. In addition, inappropriate behavior should be properly documented and addressed according to relevant employee/employer procedures.

It is imperative that Federal law protect workers' rights to privacy. Currently, protection for an individual's right to privacy is unevenly reflected in our laws, and sadly absent from laws governing workplace policies and practices. Senator Simon's floor statement upon introduction of S. 984 cites a troubling irony. The Federal Bureau of Investigation cannot wiretap a phone conversation to protect the national security without a court order. Yet employers are permitted to listen to the conversations of their employees at will.

We believe that S. 984 strikes a critical balance in recognizing the employer's need for data and systems to improve productivity and a worker's right to privacy and dignity. We believe it gives employers the latitude needed to manage workplace concerns while protecting workers.

Our Nation has witnessed a tremendous growth in technology. Nurses provide 24-hour health care in a wide range of settings and see daily incredible advances in health care technology. We use equipment that did not exist when we were in nursing school. We work with machines which were unimaginable a few short years ago. We can only begin to imagine what technology will bring tomorrow. These Orwellian technological advances have given rise to the need for regulations and systems to protect the health and safety of health care workers.

Likewise, the ability of employers to monitor the workplace through electronic means will continue to increase with technological advances and computerization. Already, the ability of employers to monitor productivity through computers has raised serious concerns in some work environments.

As information systems are adapted more widely into clinical nursing practice, the temptation to use them for employee monitoring will also spread. Will we soon measure the productivity of nurses through computerized measurements of time spent at the

bedside? Who among us wants our time with a health care provider doled out in computer-measured increments?

ANA supports progress and technological advancement. We also support a workplace which protects the health, safety and privacy of nurses and other workers. Rapid technological advances make it increasingly important to ensure that the ability to monitor is not abused.

We are very troubled by the link between electronic monitoring and increased stress. ANA has long been concerned with the high level of stress associated with nursing. The National Institute for Occupational Safety and Health has found a high level of occupational stress among nurses and other hospital workers. Hospital work requires coping with some of the most stressful situations found anywhere.

Hospital workers must deal with life-threatening injuries and illnesses, and all of this is complicated by overwork, understaffing, tight schedules, paperwork, and intricate or malfunctioning equipment, complex hierarchies of authority and skills, dependent and demanding patients, and patient deaths. All of these contribute to stress.

Senator SIMON. If you could conclude your statement, please.

Ms. JOHNSON. Yes. ANA fully supports the provisions which require that consumers be notified that they are being electronically monitored. Nurses are first and foremost patient advocates, governed by a code of ethics which includes respect for confidentiality. We believe that consumers have a right to know which conversations are private.

We appreciate this opportunity to share our views on electronic monitoring. We look forward to working with you to develop policies to strike a balance between employers' need to know and the workers' need for dignity and privacy. We think S. 984 is a critical step in the right direction.

Thank you.

[The prepared statement of Ms. Johnson follows:]

PREPARED STATEMENT OF GWENDYLON JOHNSON, RN

Good morning, I am Gwendylon Johnson, former president of the DC Nurses Association, and member of the board of directors of the American Nurses Association. I appreciate the opportunity to testify today representing the American Nurses Association (ANA) and its 53 State and territorial nurses associations, on behalf of the Nation's two million registered nurses. ANA is both the largest professional organization of registered nurses and a labor organization, representing nurses for collective bargaining purposes through State Nurses Associations. We commend the committee for holding hearings on workplace privacy and applaud Senator Simon's long commitment to protecting the rights of our nation's workers.

ANA supports passage of S. 984, the Privacy for Workers and Consumers Act with its emphasis on providing protections against electronic monitoring. The bill addresses three factors of particular concern to nurses: 1) the intrusive, invasive nature of electronic monitoring; 2) the growth in technology which will continue to make new forms of monitoring available; and 3) the added stress to employees who are subjected to electronic monitoring. Finally, as consumers of services which could be monitored and as patient advocates, we support the provisions of the bill which are designed to protect the privacy of consumers.

INVASION OF PRIVACY

From childhood most of us are taught the basic tenets of respect for the privacy of others. We learn not to listen at closed doors, and to immediately put down a telephone if we pick it up and hear voices. We learn that eavesdropping is wrong.

We certainly learn not to peek through other peoples' curtains or observe our friends through cracked doors. Yet sophisticated technology and workplace production demands have made such practices commonplace, even acceptable, in too many workplaces across the country.

In recent years we have seen troubling examples of electronic monitoring which unnecessarily invades the privacy of nurses. This committee is aware of the case of nurses at a hospital in Maryland who discovered a hidden video camera in their dressing room—broadcasting their activities to an inhouse cable channel.

This is unfortunately not an isolated incident. Nurses at other facilities have found video cameras in their locker rooms. Nurses in Virginia are considering legal action in a similar case. No doubt many other monitoring devices have gone undetected. Although, the employers defended their actions, citing concerns about illegal behavior, such intrusions are unwarranted.

This practice is discriminatory, invades privacy, raises sexual harassment concerns and is clearly unacceptable.

We fully support the provision in S. 984 which would prohibit the monitoring of locker rooms, bathrooms or dressing rooms. We do not believe such a blatantly intrusive practice should be legal. ANA believes that workplace privacy issues must be vigilantly monitored. Too many times employees and enforcement officials attempt to use medical testing or technology to address criminal, safety and compliance activities related to employee behavior.

ANA has opposed the use of truth testing in long term care and child care settings proposed previously in Congress. ANA submitted extensive comments on the use of truth testing as regulated by the Department of Labor for employees involved in the manufacture and distribution of pharmaceutical agents. As we stated in those instances the use of technology should not be used as a substitute for long established management principles.

Employers have a responsibility to provide employees adequate orientation to their jobs, education and retraining to maintain competency and appropriate supervision and evaluation. In addition, inappropriate behavior should be properly documented and addressed according to relevant employee/employer procedures.

ANA firmly believes that employers have a responsibility to provide appropriate notice to employees regarding workplace environment. This notice should include information on electronic monitoring policies expectations and policies. Without such notice employees cannot be viewed as accepting employment with informed consent.

It is imperative that federal law protect workers' rights to privacy. Currently, protection for an individual's right to privacy is unevenly reflected in our laws, and sadly absent from laws governing workplace policies and practices. Senator Simon's floor statement upon introduction of S. 984 cites a troubling irony. The Federal Bureau of Investigation cannot wiretap a phone conversation to protect the national security without a court order, yet employers are permitted to listen to the conversations of their employees at will.

We believe that S. 984 strikes a critical balance in recognizing the employer's need for data and systems to improve productivity and a worker's rights to privacy and dignity. The bill would not completely prohibit electronic monitoring. However, it protects workers by requiring employers to post a notice advising employees that they may be electronically monitored and to provide written notice describing the forms of monitoring to be used, the data to be collected and similar information.

We believe these provisions give employers the latitude needed to manage workplace concerns while protecting workers.

TECHNOLOGICAL GROWTH

Our Nation has witnessed a tremendous growth in technology. Nurses provide 24 hour health care in a wide range of settings and see daily incredible advances in health care technology. We use equipment that did not exist when we were in nursing school. We work with machines which were unimaginable a few short years ago. We can only begin to imagine what technology will bring tomorrow. These Orwellian technological advances have given rise to the need for regulations and systems to protect the health and safety of health care workers.

Likewise, the ability of employers to monitor the workplace through electronic means will continue to increase with technological advances and computerization—in ways we can only imagine. Already, the ability of employers to monitor productivity through computers has raised serious concerns in some work environments.

As information systems are adapted more widely into clinical nursing practice, the temptation to use them for employee monitoring will also spread. Will we soon measure the productivity of nurses through computerized measurements of time spent at the bedside? Who among us wants our time with a health care provider

doled out in computer measured increments? Unfortunately, consumers already complain about poor bedside manner and insufficient time with their primary providers. Patient contact quotas have resulted in a conveyor belt like provision of care in some facilities.

ANA supports progress and technological advancement. We also support a workplace which protects the health, safety, and privacy of nurses and other workers. Rapid technological advances make it increasingly important to ensure that the ability to monitor is not abused.

In hospital care there are many examples of electronic monitoring which are productive. For example, monitoring in emergency areas and critical care units can greatly enhance patient care and safety. We obviously support such uses of electronic monitoring. Our concern lies only with that which is invasive.

S. 984 maintains a balance, protecting the rights of workers, and acknowledging the demand for and advantages of technological advancement.

ELECTRONIC MONITORING AND STRESS

We are very troubled by the link between electronic monitoring and increased stress. ANA has long been concerned with the high level of stress associated with nursing. The National Institute for Occupational Safety and Health (NIOSH) has found a high level of occupational stress among nurses and other hospital workers. Hospital work requires coping with some of the most stressful situations found in any workplace.

In its 1988 publication, *Guidelines for Protecting the Health and Safety of Health Care Workers*, NIOSH states: "Hospital workers must deal with life-threatening injuries and illnesses complicated by overwork, understaffing, tight schedules, paperwork, intricate or malfunctioning equipment, complex hierarchies of authority and skills, dependent and demanding patients, and patient deaths; all of these contribute to stress."

For nurses, who are working daily under the pressure of providing care in life and death situations, the added stress of wondering who is watching them change clothes, or similar invasions of privacy and is unnecessarily burdensome. We believe that those practices should be illegal.

PROTECTIONS FOR CONSUMERS

ANA fully supports the provisions which require that consumers be notified that they are being electronically monitored. Nurses are aware of the range of health care information which could be divulged in a phone conversation. Nurses in insurance offices and other settings where there may be phone monitoring must know if they are being monitored and should be able to advise their patients and clients.

Nurses are first and foremost patient advocates, governed by a code of ethics which includes respect for confidentiality. We know that the consequences, for consumers, of misuse of information could range from embarrassment to discrimination.

Senator Simon cites an example of a caller discussing a sensitive health care issue, such as an AIDS insurance claim. Given the widespread discrimination against people with AIDS and the complexities of the illness, the conversation might be very different if the consumer is aware the call is being monitored. The same is true of discussions of other health conditions—even though they may be less devastating.

ANA believes that consumers should have the right to choose the information they will divulge in conversations in such situations. They have a right to know which conversations are truly private. We all have a right to know that our conversations are not listened to secretly.

CONCLUSION

The American Nurses Association, appreciates this opportunity to share our views on electronic monitoring. We look forward to working with Senator Simon and other members of this committee as we strive to strike a balance between employers' need to know and workers' need for dignity and privacy. We believe S. 984 is a critical step in the right direction. Thank you.

Senator SIMON. Thank you for an excellent statement.

Barbara Easterling, no stranger to this committee.

Ms. EASTERLING. Good morning, Senator. I am Barbara Easterling, secretary-treasurer of the Communications Workers of America.

In recent years, employers have dramatically expanded their use of concealed electronic surveillance. It has been estimated that each work day, 20 million wage earners are subjected to secret electronic monitoring at job sites across America. Supervisors spy annually on hundreds of millions of telephone calls between workers and the public. A stress epidemic exists at many American workplaces due in part to the marked increase in the use of electronic monitoring.

Thousands of service workers are strung out, bugged, and coming unplugged.

Mr. Chairman, a study issued 2 years ago by the University of Wisconsin and CWA contains striking evidence that workers employed by the American Telephone and Telegraph Company and the seven regional Bell operating companies in jobs that were monitored electronically experienced higher levels of psychological stress and more physical problems than did workers employed by those eight companies in jobs that were not monitored.

With regard to stress, the study revealed that monitored workers suffered more depression, higher levels of extreme anxiety, and more severe fatigue than did nonmonitored workers employed by the same companies.

Looking at physical health, one of the most disturbing findings of the study is that telephone workers who were electronically monitored were more than twice as likely to be plagued by wrist pain as were nonmonitored workers. Of special concern, a recent report disclosed that workplace stress costs employers \$200 billion a year. This is an enormous financial burden that the United States cannot afford if it is to compete successfully in the global marketplace.

Ironically, the stress that is derived from electronic monitoring may diminish the productivity that such surveillance is intended to enhance. Employers claim that secret electronic surveillance is necessary to ensure quality of service, but evidence demonstrates that the absence of concealed electronic surveillance may actually improve the quality of service.

Twelve 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, the Chesapeake and Potomac Telephone Company of West Virginia ranked first in America among Bell System companies in six of 12 customer satisfaction categories. The West Virginia law was overturned during the tenure of the successor to Governor Rockefeller, and this occurred in part because, at a time when West Virginia was enduring a severe recession, and its unemployment rate was then amongst the highest in the Nation, AT&T threatened not to locate a major manufacturing facility in that State unless the monitoring law was changed.

As Ms. Johnson has said, it is disturbing irony that the Federal Bureau of Investigation is required by law to obtain a court order to wiretap a telephone, even in cases that pose a threat to our national security, but that employers are permitted to spy at will on their own personnel and on the public through electronic eavesdropping on their telephone calls.

In order to stop the invasion of privacy, erosion of dignity, and expansion of stress-related illness caused by secret electronic mon-

itoring, CWA supports the enactment of the Privacy for Consumers and Workers Act, S. 984, which you have introduced. The legislation would provide wage earners with the right to know when and under what conditions monitoring will take place. Under the bill, an employer's use of electronic monitoring would diminish as an employee's period of service with the employer increases.

But even under this bill, no matter how long a worker had performed his or her duties in an exemplary manner, the employer would always retain the right to use secret electronic monitoring should management suspect that the worker was engaged in conduct which violated criminal or civil law, or which constituted willful gross misconduct. The legislation would prohibit the abuse of secret electronic monitoring by employers, but it would not stop the legitimate use of secret electronic monitoring by them.

Mr. Chairman, approval of the Privacy for Consumers and Workers Act would permit workers to earn their living without being subjugated to the environment of an electronic sweatshop. Equally significant, enactment of the legislation would strengthen the right to privacy at a time when the growing use of surveillance technologies at the workplace has endangered this most fundamental of American values.

Thank you.

[The prepared statement of Ms. Easterling follows:]

PREPARED STATEMENT OF BARBARA J. EASTERLING

The Communications Workers of America (CWA) appreciates the opportunity to provide testimony in support of legislation that would restrict secret electronic monitoring in the workplace.

By way of background, CWA represents more than 600,000 workers employed in the telecommunications, printing, publishing and broadcasting industries, as well as in the health care field and in State and local government.

Secret electronic monitoring is the merciless whip that drives the rapid pace for workers in the service sector of the economy.

In recent years, employers have dramatically expanded their use of concealed electronic surveillance. It has been estimated that each workday 20 million wage earners are subjected to secret electronic monitoring at jobsites across America. Supervisors spy annually on hundreds of millions of telephone calls between workers and the public businesses covertly count the number of keystrokes employees produce each minute on video display terminals. Management stealthily photographs workers who are honorably carrying out their duties at offices and plants.

A stress epidemic exists at many American workplaces due, in part, to the marked increase in the use of electronic monitoring.

Thousands of service workers are strung out, bugged and coming unplugged! Unremitting job pressure derived from electronic surveillance has corroded their employment environment.

To illustrate the abusive nature of secret electronic monitoring, consider these true labor relations cases.

—A young woman employed as a travel reservation agent was threatened with discipline for not achieving the office productivity standard. She explained that she had been trying to cope with morning sickness (her first pregnancy) and the sudden death of her mother. These reasons were not acceptable to management.

—A middle-age man whose work was subject to telephone service observation was admitted to a hospital after taking a drug overdose. He said that he needed one more "upper" to face the start of another day.

—A computer operator discovered several months after she was hired that a computer was keeping track of her workday activities, including her time in the bathroom. The employee was not notified before she was hired that her employer monitored the workforce in this insidious way.

—A travel 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 for the content of her private conversation.

—A newspaper kept a secret record of every time that the telephone number of the union at represented its workers was dialed and from what extension.

—Nurses in a hospital discovered that management had installed a concealed camera in their locker room. The camera was monitored by male security guards who watched the nurses change clothes into their hospital uniforms and later change back to their non-work attire. The nurses were kept in the dark about this "peeping Tom" invasion of their privacy.

—During contract negotiations in Cleveland, Ohio between the United Auto Workers and Midland Steel Products, members' of the union's bargaining committee became aware that the company was using a video camera to spy on the workers as they planned strategy to discuss wages and working practices.

These and many other examples demonstrate that electronic monitoring is an inhuman system based on lack of trust.

From a related standpoint, concealed electronic surveillance has even invaded the offices of leaders of the Federal Government. The Washington Post reported last November that former Secretary of State James A. Baker III avoided having his telephone calls placed through the Operations Center at the State Department because the Operations Center made a standard practice of eavesdropping illegally on the telephone conversations of Department officials.

When he became secretary of State in 1989, Mr. Baker said, "No way am I going to have my phone conversations routinely monitored," according to one source close to Baker, the Post recounted. Mr. Baker's emphatic statement reflects the desire of thousands of workers whose telephone conversations have been subject to secret surveillance.

The effort to monitor the telephone calls of the former Secretary of State—who was, perhaps, the closest political advisor of President Bush—underscores the need for Congress to take action to restrain this abusive practice.

ELECTRONIC MONITORING AND WORKERS' HEALTH

Management's use of electronic surveillance is taking a devastating toll on the occupational safety and health of wage earners in the form of heightened psychological stress and increased physical strain.

A study issued 2 years ago by the University of Wisconsin and CWA contains striking evidence that electronic monitoring of telephone workers has, at a minimum, the potential to influence conditions that produce ill health.

The study revealed that workers employed by the American Telephone and Telegraph Company (AT&T) and the seven regional Bell operating companies in jobs that were monitored electronically experienced higher levels of psychological and physical problems than did workers employed by those eight companies in jobs that were not monitored electronically.

The research is significant because it is the first major investigation into the relationship between health symptoms and telephone workers who are monitored electronically.

With regard to stress, the University of Wisconsin study disclosed that monitored workers at AT&T and the seven regional Bell operating companies suffered more depression, higher levels of extreme anxiety and more severe fatigue or exhaustion than did nonmonitored workers employed by the same companies.

Specifically, 81 percent of monitored workers who were surveyed complained of depression as compared with 69 percent of workers who were not monitored. Similarly, 72 percent of monitored workers stated that they endured extreme anxiety as contrasted with 57 percent of telephone workers who were not monitored. Also, 79 percent of monitored wage earners reported problems with severe fatigue or exhaustion as compared with 63 percent of nonmonitored wage earners.

Looking at physical health, 51 percent of monitored employees at AT&T and the seven regional Bell operating companies declared that they were plagued by sore wrists. This means that electronically monitored telephone workers were more than twice as likely to suffer wrist pain as were nonmonitored workers! In addition, 81 percent of monitored employees cited problems with neck pressure as contrasted with 60 percent of nonmonitored employees.

Of special concern, it has been estimated that workplace stress costs American employers \$200 billion a year through increased absenteeism, diminished productivity, higher compensation claims, rising health insurance fees and additional medical expense.* This is an enormous cost that the United States cannot afford if it is to compete successfully in the global marketplace. The portion of the \$200 billion cost of stress that is attributable to electronic monitoring is uncertain. Ironically, the

stress that is derived from electronic monitoring may reduce the productivity that such surveillance is intended to increase.

DISTORTED EMPHASIS ON QUANTITATIVE MEASUREMENTS

Many employers in the service sector are using high-tech monitoring to transform their workplaces into electronic assembly lines, reminiscent of 19th century factories.

*World Labor Report 1993, page 7

Just as manufacturers in industrial plants accelerate the pace of production for blue-collar workers, employers of office workers use computers to compress the time allowed for employees to complete their tasks. As a result, unwinking computers have become surrogate supervisors at thousands of jobsites, pushing wage earners to work at top speed.

A graphic illustration of the way in which computers are used to control work routines is seen in the telephone industry. A typical operator handles more than 1,100 calls in a 7½ hour shift. The operator has absolutely no control over when the next call will be routed to her. A central computer determines if the operator receives three calls in a row or 300 in a row.

The operator is required to complete each call in about 30 seconds or less. If the operator fails to handle her calls within the prescribed 30 second average work time (AWT), then the operator can be disciplined or dismissed.

The emphasis on quantitative measurement places operators in the anxiety-producing dilemma of having to choose between performing their duties in a manner that satisfies the needs of the public or attaining the average work time dictated by the company computer.

If an operator receives a call from a customer who suffers from a speech impediment, a hearing problem, a learning handicap, a language barrier, an illiteracy hindrance or any other disability which requires additional time, the operator may be placed in an especially stressful situation.

In such a circumstance, the operator is well aware that it is her duty to provide quality service to the customer. At the same time, the operator is highly cognizant that the clock is running and that the average work time for completing the call forms an integral part of her performance evaluation. In addition to confronting the difficult choice between serving the customer or preserving her employment, the operator may fear that the call is subject to telephone service observation by Ma Bell's intrusive sibling, Big Brother.

All of this can combine to produce a cauldron of stress for the operator that boils over.

To illustrate the distorted priorities that management's emphasis on 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 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 30 seconds.

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, [sic] 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 popped 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 manager 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,

THE FALSE CLAIM THAT MONITORING ENSURES SERVICE QUALITY

Employers claim that the use of secret electronic monitoring is necessary to ensure quality of service. Evidence demonstrate, however, that the absence of concealed electronic surveillance may actually improve quality of service.

Twelve years ago, legislation that prohibited secret telephone monitoring was signed into law in West Virginia by then-Governor Jay Rockefeller. Despite the absence of such surveillance, the Chesapeake and Potomac Telephone Company of West Virginia ranked first in America among Bell System companies in 6 of 12 "customer satisfaction" categories, according to the company's official journal C and 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 operators from Washington, DC, where monitoring was permissible, to West Virginia after monitoring there was prevented.

The West Virginia law was subsequently overturned during the tenure of the successor to Governor Rockefeller. This occurred in part because—at a time when West Virginia was enduring 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 electronic monitoring has been eliminated in several telephone company workites without any reported diminution in quality of service. In such cases, the absence of monitoring reduced accompanying financial costs for supervisory personnel and for monitoring equipment, allowing the potential for higher profits.

LEGISLATIVE REMEDY

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 did not foresee the onrush of technology that would foster the use of electronic eavesdropping devices more insidious than any enemy soldier they faced on the battlefield.

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

Congress must take steps to ensure that employers do not destroy our nation's basic freedoms through the abusive practice of secret electronic monitoring.

It is a disturbing irony that the Federal Bureau of Investigation (FBI) is required by law to obtain a court order to wiretap a telephone—even in cases that pose a threat to our national security—but that employers are free to spy at will on their own personnel and on the public through electronic eavesdropping on their telephone calls.

In order to stop the invasion of privacy, erosion of dignity and expansion of stress-related illnesses caused by secret electronic monitoring, CWA supports enactment of the Privacy for Consumers and Workers Act, S. 984, introduced by Senator Paul Simon (D-IL).

The legislation would provide wage earners for the first time with the "right to know" when and under what conditions monitoring will take place. The bill would require employers to give workers advance notice of the types of electronic surveillance that will be used and the purposes for which they will be used.

Under the bill, an employer's use of electronic monitoring would diminish as an employee's period of service with the employer increases.

But no matter how long an employee had performed his or her job duties in an exemplary manner, the employer would always retain the right to use secret electronic monitoring should management suspect that the employee is engaged in conduct which violated criminal or civil law or constituted willful gross misconduct.

Therefore, the legislation would prohibit the abuse of secret electronic monitoring by employers but it would not stop the legitimate use of secret electronic monitoring by employers.

Enactment of the Privacy for Consumers and Workers Act would permit workers to earn their living without being subjugated to the environment of an electronic

sweatshop. Equally significant, passage of the legislation would strengthen the right to privacy of every citizen at a time when the growing use of surveillance technologies at the workplace has endangered this most fundamental of American values.

Senator SIMON. Thank you very much.

Mr. Maltby.

Mr. MALTBY. Good morning, Mr. Chairman.

Our first response to stories like Mr. Ettienne's and the nurses that Ms. Johnson described is shock. The second is confusion. Isn't there a right to privacy in this country, we ask. The answer in this situation, unfortunately, is no.

When most people think about the right to privacy, what they really have in mind is the right to privacy found in the Federal Constitution. This right is real and very important. But like all constitutional rights, it applies only to the Government. The Constitution and Bill of Rights do not apply in any way to any private corporation in this country.

When most workers go to work in the morning, they might just as well be going into a foreign country. They are equally beyond the reach of the Constitution in both cases.

Unfortunately, Federal law does very little to fill the void here. When it comes to electronic surveillance on the job, we have only the Electronic Communications Privacy Act of 1986 to protect us. ECPA is an amendment to the old 1968 Omnibus Crime Control Act.

From the standpoint of consumers and employees, ECPA is a lot like many consumer contracts. The big print gives it to you, and the small print takes it away.

Section 2511 of ECPA does generally prohibit the interception of electronic communications. However, the section also contains an exception for interceptions "in the ordinary course of business."

What this has come to mean through the defining process of Federal litigation is that employers cannot deliberately monitor personal communications that someone might make at work. If an employer has separate telephone phones that employees can use for personal calls, those phones cannot be monitored. When there is only one set of phones, and an employer is monitoring for quality control purposes and accidentally picks up a personal call, under ECPA, they are obliged to hang up as soon as they realize the call is personal.

But if the communication is work-related in any way at all, the employer can do anything it wants. Your employer can intercept your electronic mail without your knowledge, tap your telephone, watch you with a hidden video camera, and bug your office, all without violating any Federal or State law.

Where business-related communication is concerned, the employer has all the rights; the employee has none.

State law is no better. No State legislature in this country has ever passed a law protecting people's privacy from electronic surveillance at work, and to the best of our knowledge, not State legislature is even contemplating doing it now.

The end result is that we have no real right to privacy on the job. The Federal Constitution does not apply. The only Federal statute is a very limited application, and there is no State law at all.

If we are to have a meaningful right to privacy on the job in this country, we must have a new law to create it. Senator Simon, you and your subcommittee and the staff have done an excellent job of creating a bill that will protect the right of workers and consumers to privacy and do it in a way that does not impede the legitimate needs and interests of employers. The American Civil Liberties Union supports S. 984, and we hope the committee will as well.

Thank you.

[The prepared statement of Mr. Maltby follows:]

PREPARED STATEMENT OF LEWIS L. MALTBY

Mr. Chairman and members of the subcommittee, thank you for inviting the American Civil Liberties Union (ACLU) to testify before you today in support of S. 984, The Privacy for Consumers and Workers Act. The ACLU is a private, non-profit organization of over 275,000 members dedicated to the protection of civil rights and civil liberties. I direct the ACLU's National Task Force on Civil Liberties in the Workplace.

We believe that S. 984, if enacted, will be an important step forward in protecting the privacy of Americans at work.

The ACLU is deeply concerned about the state of privacy in the workplace today. The use of computers and other electronic equipment is exploding. It is estimated that almost so million Americans will use computers at work by the turn of the century.

While this holds the promise of multiplying our productivity, it also poses threats to our privacy. Computer screens can be read without the user's knowledge. Telephone calls can be secretly monitored and recorded. Electronic mail can be covertly intercepted. Hidden microphones and video cameras can record our every move without our knowledge. Not only are these practices technically feasible, but the rapidly declining cost of electronic technology also makes them very affordable. Unfortunately, many companies are taking advantage of these conditions to violate the privacy of their employees. The ACLU receives over 50,000 complaints every year. The majority of those complaints do not involve any government agency; they are complaints about the workplace. Privacy violations are the most common workplace complaint. We have had nurses discover hidden video cameras in their shower room. We have had employees whose offices have been bugged. We have had employees whose phones have been tapped.

Despite this the ACLU is not opposed to electronic surveillance. We recognize that managers need to monitor the quality and quantity of employees' work; and that, in an electronic age, some of that monitoring will be electronic.

A balance needs to be struck, however. Employees are human beings. They have—or at least ought to have—a right to privacy. That right should not disappear when people go to work. Employers need information about job performance, but that need must be balanced against employees' reasonable expectations of privacy.

Unfortunately, current law does not strike such a balance. In fact, it does not even attempt to strike a balance. The ACLU supports S. 984 because it provides needed protection for personal privacy that current law does not provide.

The principal law in this area is the Electronic Communications Privacy Act (ECPA), a 1986 amendment to the 1968 Wiretap Law. Section 2511 of the ECPA prohibits the interception or disclosure of electronic communications. However, the section creates an exception for interception done in "the ordinary course of business."

What this has come to mean, through the defining process of federal litigation, is that employers cannot deliberately monitor an employee's personal communications which are made at work. For example, if an employer provides separate telephones for employees to make personal telephone calls, those telephones may not be monitored. Where separate telephones do not exist, and employees must make their personal calls on their business phones, the employer must hang up once it realizes it is monitoring a personal call. But if the electronic communication is work related, the employer can do anything it wants. While the ECPA takes the valuable step of protecting personal communications from employer monitoring, it does not even attempt to balance the rights of employers and employees where business communications are concerned. For business communications, the employer has all the rights, the employee has none.

State law also fails to protect our privacy. There are no State statutes regulating the use of electronic surveillance on the job. There is a common law right to privacy

in virtually every State, which frequently applies to employees. This right, however, covers only the few indefensible abuses that no sensible employer would engage in anyway—such as strip searches. It offers no protection in the more common cases where the rights of employers and employees must be balanced.

We believe the current state of the law is unconstitutional and unfair. As members of Congress, you need to know what your staffs are doing. You might sit in on an important meeting to see how your staff handled it. But you would not bug the room, so you could listen in without their knowledge.

"Knowledge" is the essence of S. 984. The bill does not restrict an employer's ability to monitor the work of its employees, but it requires that the employer tell the employees when they are being watched or listened to.

Eliminating covert surveillance is not only fair, but it improves employee performance in the long run. The technocrats who design these workplace surveillance systems have forgotten that employees are people. You can slice them up into tiny pieces and scrutinize them under a microscope, but in the process their spirit is destroyed. An employee who does not care is not a productive employee.

The report on electronic surveillance by the Congressional Office of Technology Assessment discusses several real world situations that illustrate this. The most well-known is the Hotel Billing Information System (HOBIS) office in Tempe, AZ. Under an arrangement worked out by AT&T and the Communications Workers of America (CWA), all 100 operators were organized into an autonomous work group. Covert monitoring was eliminated. The results are eye-opening. Quality of service improved. Customer complaints went down. Absenteeism decreased. Grievances declined. Management costs went down. Training costs went down. From everyone's perspective: employees', managements', and the customers', the office worked better without covert surveillance.

The same lesson emerges from the West Virginia experience. For several years, West Virginia had a statute forbidding covert 5 electronic surveillance at work. During that time, West Virginia Bell's operators were rated better than most of their secretly monitored counterparts in other States.

Most Americans cherish deeply their right to privacy. No one should have to spend years of their working life never knowing when they are being secretly photographed or when their employer is listening to their telephone conversations. S. 984 is a modest step towards constructing a balanced law of workplace privacy. We urge you to support it. We look forward to working with you on this important matter.

Senator SIMON. We thank you for your testimony.

Ms. JOHNSON, you are a nurse. When you mentioned instances in Maryland and Virginia of nurses being monitored in their dressing rooms, if an individual does that, we have a name for that, don't we? What do we call that?

Ms. JOHNSON. Voyeurism.

Senator SIMON. Yes, voyeurism, but I was looking for another phrase—"peeping Tom." We do not permit an individual to do that. We call that person a "peeping Tom," and that person can be arrested and prosecuted, and properly so.

Does there seem to be some analogy between a camera—incidentally, we are being videotaped here today—does there seem to be some analogy between the "peeping Tom" and a hospital or a corporation doing the same thing?

Ms. JOHNSON. Senator, every nurse that I have spoken with feels exactly that way. They feel that it is absolutely unallowable, unacceptable for that kind of behavior to take place, and they have referred to it in terms from "peeping Tom" to voyeurism, in terms of the observation of nurses.

I as an obstetrical nurse have to change clothes every day when I go to work. I would find it terribly offensive to think that someone would be monitoring the dressing or undressing of anyone, particularly of nurses.

Senator SIMON. Ms. Easterling, you talked about the West Virginia company that received high marks. What is your overall observation, not just in West Virginia, but overall? How many of the

Bell companies do you know follow policies of monitoring with warning their employees, and how many do it in a way that is offensive without warning?

Ms. EASTERLING. We do have some agreements with the Bell Operating Companies as well as with AT&T on monitoring procedures. I would like to tell you that they are adhering to those policies, but at the same time I must tell you that we have several incidents in the grievance procedure that they are not abiding by the policies.

I would say probably 50 percent have some type of agreement with us on the issue. However, we are not at a point where we can say to you that the agreement is there to treat the employees fairly, to notify them in advance, and then to live up to that agreement. There is always the feeling somehow, some way, that the employee is going to try to do something that they should not be doing and that the easiest way for the company to handle it is by monitoring them. The employees do indeed suffer a great deal of stress because of this, and I can personally speak to that, having been a telephone operator, that the very thought that you never knew when or at what time someone was going to be monitoring you kept you under a great deal of stress for 8 hours a day.

Also, something that you might say to a coworker and would be picked up by the monitoring on them at the time was often used against you. So even though that was what you might call a personal comment, those comments were entered in your record and held against you just as well.

Senator SIMON. And in terms of productivity, those who enter into agreement and those who don't enter into agreement with you, is there any difference in productivity in these companies?

Ms. EASTERLING. Our contracts were just renegotiated last year, and we have not had an opportunity to track that, but we intend to do so.

Senator SIMON. And what about—I mentioned the Bell companies, but you have GTE and a lot of smaller companies.

Ms. EASTERLING. I don't believe we have any agreements in any of the smaller companies or in GTE.

Senator SIMON. And the reality is that the employees who are not covered by any kind of union agreement, there is just virtually unlimited access, then?

Ms. EASTERLING. That is one of our major reasons for being here. We find, for example, that in the telemarketing areas, or in small companies, that the employees who are using the telephone, working on the telephone, are usually very low paid women. So consequently, it is a very abusive activity, we feel, against those individuals, and as always, we are concerned about people we represent, but also those who don't have anybody to represent them as well.

Senator SIMON. Mr. Maltby, if I could ask you to put on a different hat, and imagine that you are an employer. What harm comes to the employer if we pass this and we require notification, with rare exceptions, when we think the law may be violated?

Mr. MALTBY. Senator, it is really not such a hard hat to put on, because for most of my adult life, I was a senior manager in the private sector.

Senator SIMON. In what field? What did you do?

Mr. MALTBY. Do you remember the horrible tragedy on Bhopal, India several years ago, Senator, when a toxic chemical tank overflowed and killed and entire town? It is not well-known, but Union Carbide has the same sorts of tanks with the same sorts of chemicals in the United States. And the reason that those chemical tanks and many others do not overflow is because the company to which I was formerly executive vice president made very reliable electronic control systems to keep those tanks under control. So I was in a very, very safety-sensitive business where the quality of the product literally was protecting many people's lives. And we did not do electronic surveillance of this type. Our feeling was that it would have made the products much more dangerous.

There was an interesting Harris poll that was done several years ago that showed that a majority of American employees consciously and deliberately do less than their best work, and it is clearly related to the way they feel about their companies and the way they feel their companies are treating them.

If we are going to have the kind of competitiveness and productivity we need in the future, we have to get employees more committed to their companies and more committed to their jobs than they are right now. There may be many things we have to do to create that, but clearly, treating people with dignity and respect on the job is an absolutely indispensable part of that solution.

Senator SIMON. I could not agree more. I think we have to improve labor-management relations in this country, and we have to improve productivity—but that means the small gestures on both sides that can be so meaningful both to labor and to management.

We are pleased to be joined by Senator Thurmond.

OPENING STATEMENT OF SENATOR THURMOND

Senator THURMOND. Thank you very much, Mr. Chairman.

I regret I had to be in another committee meeting this morning and could not be here sooner, but I will take pleasure in reading the record.

To save time, Mr. Chairman, I ask unanimous consent that my opening statement appear in the record following your statement.

Senator SIMON. It will be entered in the record.

Senator THURMOND. Thank you.

[The prepared statement of Senator Thurmond follows:]

PREPARED STATEMENT OF SENATOR THURMOND

Mr. Chairman, it is a pleasure to be here this morning to receive testimony concerning S. 984, the "Privacy for Consumers and Workers Act of 1993". I would like to join you and the other members of the committee in welcoming our witnesses here today.

Mr. Chairman, businesses are constantly seeking ways to increase the quality and efficiency of their services and work product by using the advances in electronic and telecommunication technology. As the volume and value of these services and work products increases, businesses are finding it essential to use electronic monitoring as a means of staying competitive in the 1990's and into the next century.

The bill before us today¹ S. 984, 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 electronic devices to monitor employees. While employee privacy should be protected in certain situations, that privacy must be balanced against the need of businesses to maintain quality services in a competitive market.

On the whole, I believe that most employers use monitoring to increase their productivity and to ensure a quality product and a quality workplace. I realize that these are a few who have been abusive in their actions. However, I must question whether a Federal mandate in this area fully takes into account the varying needs and circumstances of the employers involved with this issue. I am also concerned that the definitions in this legislation are so broad and ambiguous that businesses will have difficulty applying them.

In addition, I have concerns about the breadth of section 10(c) of the bill and its practical meaning. That section prohibits the collection or use of data "obtained by electronic monitoring of an employee when the employee is exercising First Amendment Rights."

Mr. Chairman, some type of notice or restrictions may be reasonable. However, we should question whether to mandate these actions, and if so, exactly what form and manner that should take.

Again, I would like to welcome our witnesses here today and I look forward to reviewing their testimony.

Senator SIMON. Do you have any questions of this panel, Senator Thurmond?

Senator THURMOND. We are going to have a vote in just a minute. If you don't mind, I'll submit some written questions.

Senator SIMON. Yes, we will have written questions, and we may have written questions for other witnesses, also.

We thank all of you very, very much for your testimony.

Our next panel includes Richard J. Barry, a member of Security Companies Organized for Legislative Action—and my staff tells me that in 1988 when I was on the presidential campaign, he was one of those who provided security at that point. John Gerdelman is senior vice president of customer markets for MCI, in Arlington, VA. And Michael Tamer is president of Teknekron Infoswitch Corporation of Fort Worth, TX.

We are very pleased to have all three of you here, and unless you have any special wishes, we will just start with you, Mr. Gerdelman.

STATEMENTS OF JOHN GERDELMAN, SENIOR VICE PRESIDENT, CUSTOMER MARKETS, MCI, ARLINGTON, VA; MICHAEL J. TAMER, PRESIDENT, TEKNEKRON INFOSWITCH CORPORATION, FORT WORTH, TX, AND RICHARD J. BARRY, MEMBER, SECURITY COMPANIES ORGANIZED FOR LEGISLATIVE ACTION, BOSTON, MA

Mr. GERDELMAN. Thank you, Mr. Chairman. I want to thank you for inviting me to appear here today on behalf of MCI Communications Corporation to discuss S. 984.

I am responsible for all customer service and sales operations for MCI consumer markets, serving residential customers.

In its broad scope, this legislation addresses many different forms of electronic monitoring of employees in the workplace, including "telephone service observation." This kind of monitoring, which involves listening to calls being made or received by an employee to monitor the quality of service provided by the employee, is an essential part of MCI's customer service program.

For that reason, we would like Congress to understand why and how such activities serve our customer interests. We would also like Congress to understand what it would mean to our customers and to our employees if our present telephone service monitoring practices were restricted or prohibited, as S. 984 currently proposes.

Unlike other marketplaces, our marketplace was not competitive. It was controlled by an entrenched monopoly which for years was the only available source of the services we wanted to offer.

MCI knew that there was a demand for an alternative source for such services. But we also understood that just being an alternative source would not be enough to make it a successful competitor. In order to overcome the inertia and numerous other advantages which favored the incumbent, we would have to fight for market share, which we did on all fronts, such as price, innovation, and the one factor which directly touches consumers, quality of customer service.

MCI's commitment to assuring quality customer service is one of the things new employees learn about their new employer. Employees are well-trained and given ample time to gain experience in fulfilling their own responsibilities toward attaining this quality commitment. It is clear they understand and support this commitment not only as a sound competitive corporate policy, but also as an employment policy that offers personal challenges and opportunities for advancement.

Our customer service professionals who handle inbound calls from MCI customers constitute the front-line testing ground for the sincerity of MCI's commitment to customer service. These employees understand that the telephone service monitoring process is a key practical ingredient of their training and evaluation and that these programs are designed to directly benefit them as well as the company by guiding and improving their workplace.

New service trainees are monitored periodically during a 5 to 7-week training period by trainers, supervisors, and managers who use the monitoring to coach them in developing their call-handling performance levels. The frequency and amount of monitoring will vary according to the trainee's learning and performance capabilities. Typically, a trainee is monitored five to ten times a month. The feedback is immediate and promptly applied by the employee in subsequent calls to the customers.

Experienced customer service professionals are monitored periodically to assess the quality of their interactions with customers. This practice results in the completion of a "quality monitoring summary." This standardized form evaluates the employee's performance and includes observations concerning the employee's handling of the call. Completed summaries are shared with employees so they better understand how to improve their skills.

Let me emphasize, please, that our employees are neither disciplined nor penalized on the basis of the monitoring. But they do receive rewards for positive actions, such as awards for savings accounts that would have canceled, or demonstrating high quality or other productive call abilities.

Apart from customer service, telephone monitoring also plays several important roles in our sales activities. Although we don't formally use monitoring information as marketing information, monitoring in both sales and customer service allows us to quickly discern trends and developments in the concerns and interests of our customers. The more we learn about the ways people respond to our sales call, the more sensitive our people will be in responding to the concerns of our prospective customers.

An important point is MCI's monitoring of its telephone sales personnel is also designed to help ensure compliance with the "do not call" requirements of the Telephone Consumer Protection Act.

The company's monitoring practices are not designed or implemented to play games of "Gotcha" with employees. We do not monitor to trap unwary employees in misdeeds or in personal matters, and we do not use monitoring as a whip or a prod for punishment. So we are greatly troubled by the current provisions of S. 984, because they seem to reflect these very worst assumptions about how and why telephone service observation is performed by companies like MCI.

In its present form, the bill puts telephone service observation on the same restrictive footing with video surveillance and other very different forms of electronic monitoring, despite the complete lack of evidence of comparable abuse. It simply does not acknowledge that telephone monitoring does benefit employees and consumers.

By virtually banning unannounced monitoring for all but new employees, it has lost sight of two very fundamental facts. First, it must be remembered that telephone service monitoring is limited to calls which are conducted by the employee acting on behalf of the employer, within the scope of performing his or her job responsibilities. MCI employees are provided with unmonitored phones to make personal calls, both inbound and outbound, and there are no personal privacy interests of the employee at stake in monitoring the business calls.

Second, to a large extent, the benefits of telephone monitoring for purposes I described earlier will only be obtained if the monitoring is unannounced, that is, performed without letting the employee know when it will occur.

So in conclusion, MCI strongly believes that responsible telephone monitoring of customer service and sales representatives is an essential part of our training and performance evaluation programs. S. 984 fails to give adequate consideration to the experience of companies like MCI in proposing to place unreasonable restrictions on monitoring and thereby threatening to eliminate our ability to live up to our commitment to our customers.

Thank you very much, Mr. Chairman.

[The prepared statement of Mr. Gerdelman follows:]

PREPARED STATEMENT OF JOHN GERDELMAN

Mr. Chairman and members of the subcommittee, I want to thank you for inviting me to appear here today on behalf of the MCI Communications Corporation to discuss S. 984, the proposed "Protection for Consumers and Workers Act." I am John Gerdelman and am responsible for the management of all customer service and sales operations for MCI Consumer Markets, which serve residential customers.

In its broad scope, S. 984 addresses many different forms of "electronic monitoring" of employees in the workplace, including "telephone service observation." This kind of monitoring, which involves listening to calls being made or received by an employee to monitor the quality of service provided by the employee, is an essential part of MCI's customer service program.

For that reason, we want Congress to understand why and how such activities serve our customer's interests. We also want Congress to understand what it would mean to our customers and our employees if our present telephone service monitoring practices were restricted or prohibited as S. 984 currently proposes.

MCI'S FOCUS ON CUSTOMER SERVICE

Unlike other marketplaces, our marketplace was not competitive. It was controlled by an entrenched monopoly which for years was the only available source of the services we wanted to offer.

MCI knew that there was a demand for an alternative source for these services. But MCI understood that just being an alternative source would not be enough to make it a formidable and successful competitor. In order to overcome the familiarity, inertia, and numerous other advantages which favored the incumbent in this market, MCI would have to fight for its market share on all fronts: price, innovation, and the one factor which directly touches consumers, quality of customer service.

For 25 years, MCI has worked and thrived on its commitment to provide its customers with the finest quality service available. As the global telecommunications marketplace has rapidly opened to ever-increasing competition over a continually-expanding range of services, our commitment to customer service has helped us not only to attract new customers but to hold onto our old ones as well.

TELEPHONE SERVICE MONITORING AND "CONSISTENT CALL HANDLING"

MCI's commitment to assuring quality customer service is one of the First things new employees learn about their new employer. Employees are well trained and given ample time to gain experience in fulfilling their own responsibilities toward attaining this quality commitment. It is clear they understand and support this commitment not only as a sound competitive corporate policy but also as an employment policy that offers personal challenges and opportunities for advancement.

Our customer service professionals who handle in-bound calls from MCI customers constitute the front-line testing ground for the sincerity of MCI's commitment to customer service. These employees understand that the telephone service monitoring process is a key practical ingredient of their training and evaluation. These programs are designed and implemented to directly benefit them as well as the company in guiding and improving their work.

MCI's telephone monitoring practices for customer service can best be understood in the context of its "Consistent Call Handling" program. The call handling program provides service professionals guidelines and procedures to follow in responding to certain types of customer calls, such as those involving billing, credit card accounts, or other service arrangements.

New customer service professional are monitored periodically through a 5-7 week training period by supervisors, managers and trainers who use the monitoring to "coach" them in developing their call handling performance level. The frequency and amount of monitoring will vary according to the learning and performance capabilities and responses demonstrated by the new employees. Typically, this involves 5 to 10 instances of monitoring per month, performed on the basis of 1 to 3 call intervals which are interspersed with "coaching" feedback. For this kind of monitoring, the feedback is immediate and promptly applied by the employee in subsequent calls.

Even experienced customer service professionals are monitored periodically to assess the quality of their interactions with MCI customers. Such monitoring results in the completion of a "quality monitoring Summary" which evaluates the employee's performance by reference to the call handling guidelines and procedure and "customer care" categories. The latter include observations concerning the employee's handling of the monitored call, including how the employee initially responds

to the call, verifies account information, and offers assistance, as well as whether the employee identifies and satisfies customer needs. In addition, observations are made about the employee's communications skills and use of systems and resources.

The completed summaries are shown to and discussed with monitored employees. Employees are not disciplined or penalized in any way on the basis of such monitoring, but they may receive rewards for Positive actions, such as "saving" accounts, or for demonstrating high quality or other productive call abilities. Sometimes, the customer with whom the employee was speaking will subsequently be called by MCI Quality Management and asked to participate in a brief "customer satisfaction survey" regarding their earlier call to MCI customer service.

TELEPHONE MONITORING AND TELEPHONE SALES

Apart from customer service, telephone monitoring also plays several important roles in MCI's telephone sales activities.

As with customer service personnel, monitoring of telephone sales personnel is an important training and evaluation tool. MCI uses certain quantitative measures for sales and productivity. In sales, as in customer service, it is the nonquantifiable quality of the interaction between the MCI employee and the customer that is the key to success. This is the most revealing element in assessing the effort and skill in the employee's performance.

Although MCI does not formally use any monitoring information as marketing information, monitoring in both the sales and customer service areas allows us to quickly discern trends and development in the concerns and interests of our customers. The more we know about why people call us, the more able we are to provide precisely the customer service they need. Similarly, the more we learn about the ways in which people respond to our sales calls, the more agile and sensitive will our people be in gauging the receptivity of the prospective customers we contact by telephone. With regard to the latter interest, MCI's monitoring of its telephone sales personnel is also designed to help ensure their compliance with the "Do-Not-Call" requirements of the Telephone Consumer Protection Act.

TELEPHONE SERVICE OBSERVATION AND S. 984

MCI's monitoring practices are not designed or implemented to be games of "Gotcha!" with our employees. We do not monitor to trap unwary employees in misdeeds or personal matters, and we do not use monitoring as a whip or prod for punishment, production or control.

But we are greatly troubled by the current provisions of S. 984 because they seem to reflect these very worst assumptions about why and how "telephone service observation" is performed by companies like MCI.

In its present form, S. 984 puts telephone service observation on the same restricted footing as video surveillance and other very different forms of "electronic monitoring," despite the complete absence of evidence of abuse. There is no recognition that telephone monitoring greatly benefits employees and consumers as well as employers.

Under the bill's proviso, MCI would no longer be able to engage in its current practice of unannounced telephone monitoring with respect to any customer service or telephone sales personnel who has been a company employee for more than 60 working days. It would be prohibited from doing even announced telephone monitoring in connection with such employees once they have been with MCI for a cumulative period of 5 years. For personnel who have been MCI employees for more than 60 working days but less than 5 years, we would be permitted to conduct monitoring for up to 2 hours per week, but only if we give the individual employee 24 hours advance written notice of the date and hours during which the monitoring will occur.

Restricting or, worse yet, prohibiting monitoring solely on the basis of how long an employee has worked for the employer is wholly irrational. This standard fails to consider that the person who has been an employee for 10 years may only have been a customer service representative for 10 days. Even if the provision were rewritten in terms of more than 5 years performing a specific kind of job, there simply is no reliable correlation between how long a person has spent doing a particular job and how well the job is being done.

On the other hand, even if you could prove a reliable correlation between length of service and current quality of service, this would not justify exempting veteran employees from monitoring for customer service and consumer protection purposes. Experienced employees may still require monitoring for training purposes, since they are the ones most likely to be given new or more complex assignments. In addition, the justification for monitoring as a performance evaluation tool does not di-

minish, especially with respect to customer service and consumer protection concerns, based on how long the employee has been on the job.

In virtually banning unannounced monitoring for all but new employees, the bill has lost sight of two very fundamental facts about telephone monitoring:

First, it must be remembered that telephone service monitoring is limited to telephone calls which are conducted by the employee acting on behalf of the employer and within the scope of performing his or her job responsibilities. MCI and others who responsibly use telephone monitoring for training and evaluation in the context of customer service and consumer protection interests fully recognize that employees should have access to unmonitored phones for the purpose of making or receiving personal calls. S. 984 fails to address the issue that there are no personal privacy interests of the employee at stake in the monitoring of business calls.

Second, it must be understood that, to a large extent, the benefits of telephone monitoring for the purposes described above will only be obtained if the monitoring is unannounced; that is, performed without letting the employee know when it will occur. The monitoring must be unannounced because this is the only way to ensure that the employer obtains a representative sampling of the employee's typical telephone performance, rather than one which has been affected by knowledge of the monitoring.

MCI fully explains its telephone monitoring practices to its employees and prospective employees before monitoring occurs, so that they will understand the reasons for such monitoring. We also share the results of monitoring promptly with the employee, so that an evaluation and discussion of the results can help the employee to improve his or her performance.

CONCLUSION

MCI strongly believes that responsible monitoring of telephone service representatives is an essential part of any training or performance evaluation program where customer service and consumer protection are important interests to be served. S. 984 fails to give adequate consideration to the experience of companies like MCI in proposing to place unreasonable restrictions on such monitoring and thereby threatening to eliminate the benefits of such programs for employees and consumers as well as employers.

Senator SIMON. We thank you, Mr. Gerdelman.

Mr. Tamer.

Mr. TAMER. Mr. Chairman, Senator Thurmond, I appreciate the opportunity to speak before this committee on legislation that may have a profound effect on my company, Teknekron Infoswitch Corporation, and the industry it serves, the call center marketplace.

Teknekron has been in the call center marketplace in excess of 15 years as a provider of telecommunications technology and services to call centers. Call centers are integral parts of businesses that provide customer service to predominantly inbound telephone callers. Examples would be airline reservation centers, public utilities, and catalog companies. For these businesses, the ability to evaluate the effectiveness and competitiveness of their call center operations is largely dependent upon obtaining reliable, quantitative and qualitative data through electronic monitoring.

We believe S. 984, if not substantially revised, will not only harm businesses, but ultimately and most importantly, their employees and customers.

This is not to say portions of the legislation are not good. In fact, some sections are very well-done. Specifically, Section 4 of the legislation detailing the contents of notice to employees is by and large a needed element in the workplace.

However, we believe that the definitions in the legislation are too broad and ambiguous and that Sections 5, 6, and 8 are largely unworkable. These sections construct artificial parameters without regard to the uniqueness of different industries and the complexities involved.

First, this legislation impacts work products. In the call center environment, an agent's handling of a customer's call for placing an order or inquiring about service is that agent's work product. This basic premise is disclosed upon hiring.

Second, a fundamental concept of business is the need to quantify and qualify an employee's work product.

And third, our industry has just begun to explore the potential of quality measurement through statistical process control. This legislation may impair the industry's initiatives focusing on true total quality management.

We appreciate that an employee needs to be protected from excessive intrusive monitoring. We also believe employers need to be protected from overzealous monitoring by supervisors, which ultimately contributes to a decline in morale and productivity.

The legislation as drafted protects neither. We suggest there are alternative methods for providing this protection, developed by harnessing available technology to assure fair and objective treatment of employees, while providing immensely improved data and information collection to employers.

Technology currently exists and is used by our customers to establish a process which enhances the work product and protects the employee, the employer, and the customer. Examples are for accuracy and consistency in monitoring, parameters and constraints may be automatically established, such as by length of call, time of day, type of product. For more efficient evaluation, a supervisor may pre-record a session and, together with an employee, review it at a more convenient time with an opportunity for playback. For use as an employee training tool, a supervisor's notes and comments may be input to be considered later by the employee. For accuracy in performance evaluations, an employee may review the results of monitoring in comparison to the supervisor's comments. For self-training, an employee may pre-select and experiment with self-selected parameters.

And, perhaps most importantly, the monitor may be monitored. This means that any evaluation system used for an employee may also include a similar system for the monitor. The monitor's actual scoring trends can be reviewed in relationship to their peers and the company's standards. And the monitoring can also include the ability to decipher any discriminatory practices of the reviewing supervisor, such as between the sexes, the aging, the disabled, or minorities. This can ensure not only fair recording of the data, but strong confidence by the employee that the people monitoring cannot abuse their employees.

The telephone center for inbound calling is a rising area of employment in this country. There are estimated to be over 40,000 call centers in existence today. New job market opportunities, such as telecommuting, which is the performance of the telephone service representative functions at home, have opened up tremendous opportunities for the disabled, the elderly, and the working parent. Telecommuting jobs are expected to increase dramatically for the rest of this decade. Also benefited are those who, for one reason or another, cannot physically go to a place of business and yet can receive virtually any service over the phone. This legislation, if not significantly modified, will adversely affect these job markets.

We offer the following recommendations. First and most importantly, the monitors must be monitored. Second, monitoring may only be used for business purposes. Third, data or information in whatever form must be recorded, stored, and made available for the protection of the employee and employer for a reasonable period of time.

Four, all similarly situated employees must be monitored consistently. In other words, one group may not be monitored only in the morning, while they are well-rested, and the other only late in the day.

And five, monitoring must be disclosed, but restraints, especially time restraints, if any, must be created with enough flexibility to avoid destroying the accuracy and reliability of the information collected.

Finally, Mr. Chairman, I believe it would be enormously beneficial for this committee if the technology currently utilized by our customers could be demonstrated. This could provide Senators and their staff with an understanding of how technology protects workers from abuse while providing businesses with the information vital to their competitiveness and successful service to their customers.

Mr. Chairman, I cannot overemphasize how proud you would be of the impressive service America's leading companies provide to the ultimate and most important customer—the American people.

Thank you for the opportunity to provide you with the information on this very important subject. We look forward to working with the committee on this matter.

[The prepared statement of Mr. Tamer follows:]

PREPARED STATEMENT OF MICHAEL J. TAMER

Mr. Chairman and members of the subcommittee, I appreciate the opportunity to speak before this committee on legislation that may have a profound affect on my company, Teknekron Infoswitch Corporation, and the industry it serves, the Call Center marketplace.

Teknekron has been in the Call Center marketplace in excess of 15 years as a provider of telecommunications technology and services to Call Centers. Call Centers are integral parts of businesses that provide customer service to predominantly in-bound callers over the telephone. Businesses utilize Call Centers either for revenue generation such as airlines sales, insurance transactions, or catalogue sales; or for revenue protection such as banking transactions (credit management), public utility services or computer support activities. For these businesses, the ability to evaluate the effectiveness and competitiveness of their Call Center operations is absolutely critical and this ability is largely dependent upon obtaining reliable quantitative and qualitative data through electronic monitoring. We believe S. 984, if not substantially revised, not only will harm businesses but ultimately, and most importantly, their employees, and customers.

This is not to say portions of the legislation are not good, in fact some Sections are very well done. Specifically, section 4 of the legislation, detailing the contents of notice to employees is by and large a needed element in the workplace. Nor, obviously, would we object to the legislation's privacy protections for locations such as bathrooms and locker rooms. This type of intrusive monitoring is patently offensive. But frankly, we believe that the definitions in the legislation are too broad and ambiguous, and that sections 5, 6, and 8 are largely unworkable. These Sections construct artificial parameters without regard to the uniqueness of different industries and the complexities involved. While we may be submitting more specific legislative comments later to the committee staff on these and other matters, let me address our chief concerns now:

1. This legislation impacts work products. In the Call Center environment, an agent's handling of a customer's call for placing an order, or inquiring about service, is that agent's work product.

2. A fundamental concept of business is the need to quantify and qualify an employees' work product. The ability to manage a business depends on the ability to review employees' work product (in the Call Center service business, this includes such areas as verification that proper etiquette was followed, appropriate pricing and product information was disclosed, and that an adequate number of transactions are processed).

3. Employees understand that their work product is serving the customer by telephone. Every employee, in whatever capacity, is subject to performance evaluation. In the Call Center environment, it is simply that this evaluation involves successfully processing telephone related transactions.

4. This legislation will adversely affect industry initiatives focusing on the Total Quality Management (TQM). U.S. companies have found it increasingly important to perform qualitative and quantitative evaluations in their efforts to compete in a global marketplace. While the legislation recognizes distinctions in continuous monitoring and random access monitoring, the restrictions contained in sections 5, 6 and 8, along with the broadly based definitions, may ultimately preclude initiatives in TQM.

Monitoring inbound calls in a Call Center environment protects a company, its employees and its customers, as it allows for an accurate and effective evaluation of the quality or quantity of services provided by an employee to a company's customers. Quantitative measurements are not new (quantum measurements have frequently been an element of the workplace in job positions ranging from salespeople to assembly line workers). Nor, obviously, are qualitative measurements. What is new is the evolution of technology in making such measurements. We appreciate that an employee needs to be protected from excessive intrusive monitoring. We also believe employers need to be protected from over-zealous monitoring by supervisors, which ultimately contributes to a decline in morale and productivity. The legislation, as drafted, protects neither. We suggest there are alternative methods for providing this protection other than that proposed in the legislation (specifically the tenure caps, and notice windows). These methods are developed by harnessing available technology to assure fair and objective treatment of employees, while providing immensely improved data and information collection to employers.

Technology currently exists and is used by our customers to establish a process which enhances the work product and protects the employee, the employer, and the customer. For instance, to assure accuracy and consistency in monitoring, parameters and constraints may be automatically established (by length of call, by time of day, by type of product); for more efficient evaluation, a supervisor may prerecord a session and review it at a more convenient time with an opportunity for playback; for use as an employee training tool, a supervisor's notes and comments may be input to be considered later by the employee; for accuracy in performance evaluations, an employee may review the results of monitoring in comparison to the supervisor's comments; for self-training, an employee may pre-select and experiment with self-selected parameters; and perhaps most importantly, the monitor may be monitored. This means that any evaluation system used for an employee may also include a similar system for the monitor (the supervisor). The monitors' actual scoring trends can be reviewed in relationship to their peers and the company's standards, and the monitoring can also include the ability to decipher any discriminatory practices of the reviewing supervisor such as between the sexes, the aging, the disabled or minorities. This can insure not only fair recording of the data but strong confidence by the employee that the people monitoring cannot abuse their employees.

The telephone center for in-bound calling is a rising area of employment in this country. There are estimated to be over 40,008 Call Centers in existence today. Companies are increasingly recognizing that customers can be served over the phone with high quality of service and at a reduced cost compared to face-to-face communication. New job market opportunities such as telecommuting, which is the performance of the telephone service representative functions at home, have opened up tremendous opportunities for the disabled, the elderly and the working parent. Telecommuting jobs are expected to increase dramatically for the rest of this decade. Equally benefited are those who, for one reason or another, cannot physically go to a place of business, and yet can receive virtually any service over the phone. The legislation, if not significantly modified, will adversely affect these job-markets.

In conclusion, Teknekron Infoswitch believes that when used fairly and ethically, monitoring in the Call Center environment can benefit the employer, the employee, and the customer. As mentioned before, we believe that this protection cannot be ensured by artificial constraints, but instead by an equitable process. In this regard Teknekron Infoswitch has the following recommendations for any electronic monitoring legislation that this Committee and the Senate may consider:

1. First and most importantly, the monitors must be monitored.

2. Monitoring may only be used for business purposes.

3. Data or information in whatever form (visual, audio, etc.) must be recorded, stored, and made available for the protection of the employee and employer for a reasonable period of time.

4. All similarly situated employees must be monitored consistently (in other words, one group may not be monitored only in the morning when they are well rested and another only late in the day).

5. Disclosure must be made to employees of the substance of the monitoring (in other words, what quantitative and qualitative factors are being evaluated and how are those factors interrelated).

6. Monitoring must be disclosed (but restraints, especially time restraints, if any, must be created with enough flexibility to avoid destroying the accuracy and reliability of the information collected).

Finally, Mr. Chairman and members of the subcommittee, I believe it would be enormously beneficial to this committee if the technology currently utilized by our customers could be demonstrated. This could provide Senators and their staffs with an understanding of how technology protects workers from abuse while providing businesses with information vital to their competitiveness and successful service to their customers. Mr. Chairman, I cannot overemphasize how proud you would be of the impressive service America's leading companies provide to the ultimate and most important customer, the American people.

Thank you for the opportunity to provide you with information on this very important subject. We look forward to working with the committee on this matter.

Senator SIMON. We thank you, Mr. Tamer.

Mr. Barry.

Mr. BARRY. Thank you, Mr. Chairman, Senator Thurmond.

My name is Richard J. Barry. I am the co-founder, owner and executive vice president of First Security Services Corporation in Boston, MA. We are a 22-year-old, privately-held company providing security alarm, security officer and investigative services in the Northeast. We presently employ approximately 3,000 people and deliver over 80,000 hours of private security services weekly.

I am also speaking today on behalf of the Security Companies Organized for Legislative Action, known as SCOLA, a coalition of five trade associations representing the guard, alarm, armored car, and investigative service industries. Together, our organization represents more than 3,000 firms in the private security industry, and more than one million employees. The firms represented by our group range from small, family-owned concerns to major corporations with international operations.

We appreciate this opportunity to share our views on S. 984, the Privacy for Consumers and Workers Act. As you know, Mr. Chairman, Mr. Vincent Ruffolo, of Blue Island, IL, SCOLA's chairman, had the privilege of testifying before your subcommittee in 1991 on this same subject, and I bring his thanks and appreciation for our appearance here today.

We were concerned then by overly-broad language that would have seriously impaired the ability of business to safeguard patrons, employees, personnel and business assets from criminal activity and other threats in and about the business premises.

S. 984 represents a significant response to many of the security concerns presented by Mr. Ruffolo at that time. Nevertheless, our industry still has serious reservations about the day-to-day impact on employees who implement security programs.

S. 984 is administratively complex and burdensome for employers, and we have many questions about its application to specific situations. We hope that its scope can be narrowed to address more precisely the privacy interests of those in the workplace without

sacrificing the legitimate and needed electronic technology security applications.

We also ask, since the bill was only recently introduced, that the hearing record be kept open to allow additional statements to be submitted.

We agree that protecting consumer and worker privacy in the workplace is important. We also believe, however, that those interests must be in balance with the appropriate use of electronic security and safety systems to protect consumers' and workers' safety and to preserve company assets.

The key word is "appropriate." We do not condone abusive or capricious use of security equipment or procedures. We know from our own experience, however, that workers and the general public expect and demand electronic security systems in many workplace environments. An example that comes to my mind is a large, nationally-recognized hospital in Boston. The sheer size of that facility makes it impossible to provide a secure and safe environment for workers, patients, visitors, without the use of electronic systems.

In hundreds of thousands of other workplaces, electronic technology is accepted as a key component in eliminating crime and other unacceptable behavior by and toward employees and others on the employer's premises.

Mr. Chairman, we recognize that striking the appropriate balance between an atmosphere of adequate safety and security on the one hand and individuals' privacy rights on the other is quite a challenge, and it deserves a thoughtful approach. It is impossible, however, to contemplate all the situations which may be covered under this bill and to be confident about how its provisions would be applied.

A number of the concepts in the bill, such as continuous electronic monitoring, periodic inspection, random monitoring, and the provisions concerning work groups and persons with cumulative employment for 5 years, are extremely difficult to imagine in their practical applications without wondering if they would effectively prohibit commonly used types of safety and security systems.

It seems unlikely that this bill is intended to expose employers to liability for using measures that make the workplace safer; yet we are concerned that just such an unintended result may be dictated by S. 984.

It is important to note that many premises' protection systems are activated by a person's entry into a secured area—for example, hospital pharmacies, Department of Defense record rooms, or bank money rooms. As we read S. 984, such systems would be random or periodic and subject to Section 5. However, an employee or trespasser whose mission is to steal or tamper with information or materials, or to harass a coworker, may also enter a secured area where he or she can today be electronically monitored, engaging in whatever his or her nefarious mission may be.

Under S. 984, however, monitoring systems activated by the motion of a person's approach and entry into a secured area would become practically unusable until the employer had reasonable suspicion that an employee had broken or was about to break a law

and that the misconduct would involve significant economic loss to the employer or other employees.

Even with this exception, there may be little an employer can do as a practical matter, since mechanical systems do not distinguish between authorized and unauthorized persons.

I would conclude, Mr. Chairman, by stating that with crime and violence in the workplace an ever growing concern, we sincerely hope that S. 984 and its companion bill in the House will be amended to authorize legitimate security-focused monitoring in the workplace to deter activities that diminish productivity. Such monitoring is important to deter both conduct that is actually criminal, such as physical assaults and battery, pilferage, thefts against employees themselves, and inappropriate behavior by employees toward coworkers that impairs the psychological quality of the work environment.

I conclude by thanking you again, Mr. Chairman.
[The prepared statement of Mr. Barry follows:]

PREPARED STATEMENT OF RICHARD J. BARRY

Mr. Chairman, my name is Richard J. Barry. I am the co-founder, owner, and executive vice president of First Security Services Corporation, headquartered in Boston, Massachusetts. We are a privately owned business, providing security alarm, security officer, and investigative services in the Northeast. My firm currently employs 3,000 people and provides in excess of 80,000 hours of security services per week.

I am also speaking today on behalf of Security Companies Organized for Legislative Action, known as SCOLA, a coalition of five trade associations representing the guard, alarm, armored car, and investigative services industries. Together, our organization represents more than 3,000 firms in the private security industry, and more than one million employees. The firms represented by our group range from small, family-owned concerns to major corporations with international operations.

We appreciate this opportunity to share our views on S. 984, the Privacy for Consumers and Workers Act. As you know, Mr. Chairman, Mr. Vincent Ruffolo, of Blue Island, Illinois, had the privilege of testifying before your subcommittee in 1991 on behalf of SCOLA concerning this same subject. You may recall our concern at that time with what we believed to be overly broad language that would have seriously impaired the ability of business to safeguard its patrons and employees, and to protect personal and business assets located in and about the business premises. We believed the language in that bill would have also made it difficult to document premises fraud, theft, and sabotage.

Mr. Chairman, while S. 984 represents a significant response to many of the security concerns presented by Mr. Ruffolo at that time, our industry still has serious reservations about the day-to-day application of this bill and its impact on the ability of an employer to implement security measures. I'm sure you would agree that businesses shouldn't be placed in the position of having to consult a lawyer for every specific use of legitimate security technology. As it stands now, S. 984 appears to be administratively complex, with questionable interpretations on how it applies to specific situations, and seems to be unnecessarily burdensome especially for small business.

The security industry is understandably interested in this issue, Mr. Chairman, and believes the committee would benefit from a thorough analysis by security professionals out in the field. Since the bill was only recently introduced, we hope the hearing record will be kept open long enough to allow additional time for statements to be submitted from businesses which will be affected by its provisions.

Mr. Chairman, we agree that protecting consumer and worker privacy in the workplace is wholly appropriate and important. We also believe, however, that these interests must be in balance with the appropriate use of security to protect consumer's and worker's safety and to safeguard company assets. The overriding word here, Mr. Chairman, is the word "appropriate". SCOLA does not condone abusive or capricious use of security equipment or procedures, such as using cameras in a locker room without legal cause. Yet both workers and the general public expect, even demand, reliable security in many workplace situations, such as cameras in elevators, remote areas, or parking facilities.

Striking the appropriate balance between legitimate security and the right to privacy is the concern, of course, and deserving of a thoughtful approach. It is impossible, however, to contemplate all the business situations which may be covered under this bill and be confident about the application of its provisions.

In our business, we ask a lot of questions; that's the nature of our work. For instance, if there is theft, how do you identify the perpetrator? If there are security problems, how do you expose the situation? If drugs are being abused or deal transacted in the workplace, how can you document the activity? If there is industrial espionage, how do you confirm your suspicions? If there is a charge of sexual harassment, how might you document the allegation? Mr. Chairman, we would ask those same questions regarding the application of this bill. Technology in the security business is advancing rapidly, and newer, more innovative ways are being developed to address the solution of those security questions. We need to know how those methods could be applied under the provisions of this bill.

Imagine, for example, a large building with a bank of video monitors that continuously afford the opportunity to view each of the areas monitored for security purposes. If the images presented rotate from one area to another; in a sequence, with a manual override that can be controlled from the control center, is this "continuous monitoring", or is it "random", or "periodic"? The definition of "continuous electronic monitoring" may contemplate such a situation, but "periodic inspection of continuous video monitoring from an off-site location . . . to deter crime and provide evidence to law enforcement personnel" [Section 1(1)] does not clearly answer this question, as we read it.

This inquiry becomes particularly significant in light of the section 5(b) (3) prohibition on random or periodic monitoring of any employee who has a cumulative employment of 5 years, although it appears that random or periodic monitoring is permitted without restriction only within an employee's first 60 working days with an employer. While we wonder about the practical applicability of the "working group" concept to random or periodic monitoring, subject to notification of those employees, we are greatly troubled by the prohibition against intermittent monitoring of 5-year veteran employees. Random monitoring undertaken for security purposes—the multiple video monitoring system described previously¹ for example—would probably be unable to avoid picking up the images of these veteran employees if they happened to pass through any of the areas in which security cameras were in place. It seems unlikely that the intent is to expose the employer to liability under this act for using measures that make the workplace a safer environment, yet we are concerned that just such an anomaly may be created by the current language of the bill.

There are other questions in our mind also, Mr. Chairman. For instance, could a picket line be monitored if there is the threat of violence? Some retail establishments and or restaurants with bars, for example, have a high rate of employee turnover and a constant problem with theft. How would the provisions of this bill apply in those workplaces? What effective methods of security could be utilized? Under what conditions and subject to what prerequisites?

Mr. Chairman, as you know, a companion bill has been introduced in the House by Mr. Williams, H.R. 1900, which addresses this same issue. In comparing the two bills, we noticed some differences which need clarification. For instance, in the sections addressing the review of continuous electronic monitoring, H.R. 1900 provides an exception for the review of electronic data obtained from video monitoring which is used to deter crime by persons and to provide evidence to law enforcement personnel. The Senate bill does not seem to contain that direct exception. We would like to know how that legitimate exception would be treated under the Senate bill.

In another example that needs clarification, the Privacy Protection sections of both S. 984 and H.R. 1900 would not allow electronic monitoring in bathrooms, locker rooms, or dressing rooms. However, the House bill provides a exception in the case of a reasonable suspicion of criminal activity. Again, S. 984 does not seem to address this specific exemption.

In one last example concerning workers compensation, the Senate imposes a threshold of \$25,000, where no threshold exists in the House version. To a small business, Mr. Chairman, a \$5,000 claim can represent a truly significant level.

Mr. Chairman, given the challenges before your committee on this important issue, we would respectfully urge that the use of legitimate security measures be provided with a specific, but workable exemption regarding the application of S. 984. All workers and citizens have a right to a safe, prosperous work environment, and the legitimate use of security adds greatly to that goal. Employers are diligent and sincere in their efforts to provide security and safety to employees; this is supported by the Nation's cost figures for security and systems. We believe employees could be protected from indiscriminate and unfair use of electronic security and safety sys-

tems by having the burden of proof on the employer to ensure that the system's use was only for security and safety of the employees and the general public.

Thank you, Mr. Chairman.

Senator SIMON. I thank you. You used the word "balance," and I think that is what we are trying to find. I think the evidence is fairly clear from the first witness, Mr. Piller, that things have gotten out of balance.

You mentioned the hospital. You heard a representative of the American Nurses Association testify about videos in dressing rooms, wash rooms and bathrooms, and Mr. Ettienne testified to the same. If there is no suspicion of the laws being violated and under S. 984 if you had suspicion you then could get a court order, and then there could be unannounced, secret monitoring, is there any justification for just video tapping bathrooms?

Mr. BARRY. I would not say that there is any justification in some of the examples that were used. However, in the case of the situation in the hotel locker room, I believe that it had been published that the investigation was initiated by complaints from other employees who were disturbed with some of the conditions that existed in the locker room.

The monitoring of the locker room was done, according to the reports that we read in the paper, under legitimate and legal procedures.

Senator SIMON. Under what are now legitimate and legal procedures.

Mr. BARRY. Correct, and the letter of the law, according to those who did it, was followed. They have no way of knowing if they are accurate or right in their assumption.

However, usually, they are initiated by complaints from coworkers who are disturbed by some type of conduct that is taking place in these areas that we speak about.

Very seldom is the video that is taken in that type of an atmosphere subjected to the public viewing that this particular film did. And it is generally, in the times that I am familiar with, restricted to use for the strict evidence for the purpose that it was installed.

Senator SIMON. But if there is no suspicion that the law is being violated, is there any justification for that kind of video?

Mr. BARRY. I would say no.

Senator SIMON. All right. Mr. Gerdelman, in your business at MCI, you mentioned first of all people who are starting out, that they need to be monitored.

Mr. GERDELMAN. Yes.

Senator SIMON. Can't they be notified that they are going to be monitored, and you live within the law?

Mr. GERDELMAN. All our employees are notified at the time they start employment that we do randomly monitor. In fact, they do sign a statement acknowledging that we monitor. We feel that the highest quality that we can achieve is via unannounced, so that we truly see an average call. And actually, some employees prefer not to know when because they don't feel the stress when it is routine and random.

Senator SIMON. What if the CEO of MCI were to say to you, "You had a phone conversation with Senator Simon, and you should have handled it better. You said this and this, and you should have

said something else." Would you welcome such a phone call from your CEO and that kind of monitoring?

Mr. GERDELMAN. Well, actually, most of our calls are not personal in nature. They are between a customer for business reasons.

Senator SIMON. Well, this is for business reasons. You are calling me about this legislation.

Mr. GERDELMAN. Well, telephone service observations are healthy, and it does improve the quality, if that would help my quality. But most of the time, when we listen to employees, it is for coaching, and it helps them, and they appreciate the feedback. And I learn from my CEO. He helps me in presentations.

Senator SIMON. And if your CEO wants to coach you, you would not resent that?

Mr. GERDELMAN. I don't resent coaching, no. Coaching is good. It helps you be a winning team. And in fact, recently, we were notified that Fortune Magazine mentioned that we are rated one of the best in the telecommunications industry, which is part of the quality monitoring that we do.

Senator SIMON. Mr. Tamer, how would what your company does violate S. 984 right now? I am not real clear.

Mr. TAMER. Our company provides technologies that allow call centers to run their businesses, and our technology covers two areas. It covers continuous electronic monitoring of the telephone system and the statistics that come from the technology. Then we also provide software products that allow companies to analyze and evaluate the productivity and quality of their call centers, which allows them to chart and plot the distinction between the two so that the companies can address both of those issues, because it is very difficult for them, because they have to make a decision between how many, how often, and how well do I do it.

So we bring technology forward and solutions forward that allow companies to get a better understanding of what their employees are doing, what sort of service levels they want to provide to their customers, and finally, how efficiently and how cost-effectively can they do it for them.

Senator SIMON. OK. Let's just say Mrs. Smith is disabled and is taking care of telephone business. You mentioned that this is one of the things, that people who are disabled can do this in their homes. And she is notified that she is going to be monitored for the next week on how she handles things. And that complies with this law. What, beyond that, should be necessary for Mrs. Smith in that situation?

Mr. TAMER. Under the law as I understand it, Mr. Chairman, she would only be monitored if she were under 5 years. If Mrs. Smith were working out of her home in a telecommuting environment, and she was over 5 years, you would not be able to get any sort of data whatsoever on her performance of her work out of her home. So under 5 years, you could get the data associated with her, and it could be used, but over 5 years, as I understand the legislation, she would not be able to be monitored.

Senator SIMON. And let me just add, this legislation is not written in stone; we want to be fair to business.

Mr. TAMER. I understand.

Senator SIMON. And as you mentioned, Mr. Barry, we have made modifications. But generally, after 5 years, you know whether you have a good employee or whether you don't have a good employee, and it seems to me it would be rare that you would need to monitor someone after 5 years. And then there can be—unless my staff corrects me—if there is notification, that employee, Mrs. Smith, could be monitored.

Mr. TAMER. Mr. Chairman, I have two responses to that. First, for the most part, monitoring in our industry is used for training, and the number of years that you are employed may directly affect your knowledge of that particular application or it may not. Actually, the more years you are employed, you may find that your tasks switch from handling this type of service call to that type of service call to that type of service call, so your requirement for training would continue above and beyond the 5 years. And as you move more and more people out into the home, which we want to occur, because it provides tremendous opportunity, we have to be able to get to that person to provide extensive training, probably, and monitoring is an excellent way to do that.

Senator SIMON. And the bill permits that at-home monitoring. In fact, it says that it permits the discharge of an employee solely on the basis of monitoring—of course, which happens now, anyway, if it is at an at-home facility.

Mr. TAMER. Mr. Chairman, parts of the bill, I do not know the correct interpretation. If I have taken that section wrong—my understanding of that section was that it only discussed the reviewing of the material and that you could review continuous monitoring of someone who was outside the standard billing. I did not see the connection between reviewing continuous monitoring and the exemption from anybody over 5 years being able to be monitored at all. I did not, and if that is so, then you could monitor them out of their home.

Senator SIMON. Let me ask all three of you to do this—because frankly, I don't want to have another hearing 2 years from now; I want to move this legislation and get something done. I would be interested if in the next 30 days, you could get me specific language suggestions for changing the legislation that you think would be helpful. Obviously, some, I am likely to accept, some I am not likely to accept. But we want this to be a practical bill. We also believe there should be greater protection for employees than there is now—in terms of their basic civil liberties and the ability to communicate without fear. We think that is in the interest of employers, and we think it is in the interest of employees. We don't want to hurt MCI; we don't want to hurt your business, Mr. Tamer; we don't want to hurt your business, Mr. Barry. We do want to protect people. We are interested in security, but we are also interested in civil liberties.

It does seem to me that people of good will ought to be able to fashion something that is constructive in this area.

Mr. BARRY. Mr. Chairman, I would like to speak to a point that you made, if I might, in regard to the suspicion by law enforcement that would support the initiation of electronic monitoring.

Senator SIMON. Yes.

Mr. BARRY. That ties into a portion of the statement that I did not get to, and it deals with directly how private security firms interface with law enforcement. And today, unfortunately, we are all familiar with the cutbacks in public law enforcement, both at the Federal and State levels. And the private businesses that we serve find themselves unable to obtain the services of public law enforcement because of the constraints on their manpower. So most of the investigations that companies begin are initiated by private investigative services, who then at some point work with the law enforcement to provide them whatever evidence they have to support law enforcement procedure.

So quite often, the evidence that is gained is gained by a private investigative firm before it goes to the police department, and the interface with police departments is very good in the public and private security. And it became very apparent recently in the electronic surveillance of the garage at the World Trade Center, when hours and hours of surveillance of vehicles coming and going from that garage, unknown to those people that were in it, be they employees, delivery, or whatever. However, with the advent of the explosion, that videotape was reviewed, and miles and miles of useless videotape happened to contain some evidence that became significant as an investigative tool to assist in the solving of that bombing.

So quite often the evidence that is gathered by electronic surveillance cameras is not known to be valuable until some time, as in that example.

So there is a good working relationship between law enforcement and private investigators. However, much of the work that is done is done by private investigators before the law enforcement has the time to commit manpower to a criminal or sexual harassment or whatever the investigation might be. I would just want the committee to be aware of that.

Senator SIMON. Well, we understand there is that cooperation, and we want that cooperation to continue. The bill does differentiate, however, between a dressing room, a bathroom, and a garage. And I am not ready, frankly, to say—and meaning no disrespect to your company—that a private security agency can go in and videotape a bathroom or a dressing room in any private business.

Mr. BARRY. Nor do we ask for that.

Senator SIMON. This legislation says if that is going to be done, then it has to be not your company, but it has to be law enforcement people who do that.

We thank you for your testimony here today, and we thank all the witnesses. Again, not just the witnesses, but any others who have any suggestions for changes in the legislation if you can get that to us within the next 30 days, frankly, I want to get this bill moving. Thank you very much.

[The following prepared statement was submitted for the record:]

PREPARED STATEMENT OF DIANE K. BOWERS, PRESIDENT, COUNCIL FOR MARKETING AND OPINION RESEARCH

Mr. Chairman and members of the subcommittee, my name is Diane K. Bowers. I am president of the Council for Marketing and Opinion Research (CMOR). We appreciate the opportunity to submit this statement addressing S. 984, the "Privacy for Consumers and Workers Act."

CMOR is a coalition of research associations, survey and polling organizations, and manufacturers representing all segments of the research industry from research providers to research buyers. CMOR was established in the fall of 1992 to speak on behalf of the entire marketing and opinion research industry on issues of respondent cooperation and government affairs.

Mr. Chairman, we applaud you for addressing workplace privacy issues. You and Representative Williams have identified problems that clearly warrant attention. As drafted, however, S. 984 would undermine the ability of government, university and private researchers to ensure the accuracy and quality of survey research data. We strongly oppose the bill in its current form.

Public opinion polling and other survey research relies heavily on telephone interviews. Supervisory monitoring of telephone interviews enables the companies conducting the research to ensure the accuracy and quality of their data. This function cannot be served if supervisory monitoring must be limited to a few hours a week, if interviewers must be told when their calls will be monitored, and if respondents must be told that the interviews are being monitored.

This is precisely what S. 984, in its current form, would do:

Section 5 would prohibit a research organization from monitoring interviewers (other than the newest employees) through "telephone service observation" or other electronic monitoring for more than 2 hours per week, and long-time employees could not be monitored at all.

Section 4 would require that interviewers be given advance notice of the hours and days that any monitoring would occur. Sec. 4(b). It also would require that respondents be informed that the call is being monitored. Sec. 4(e). Additionally, anyone conducting telephone research for a Federal agency would have to offer respondents the opportunity not to participate in view of the fact that the call might be monitored. Sec. 4(f).

Dr. J. Ann Selzer, the former Director of the Iowa Poll, has stated that these requirements would make it impossible for researchers to maintain the "stringent quality control" that is indispensable to "first-rate survey research." Frank Brown, the president of MarketSearch Corporation in Columbia, SC, spoke for survey research organizations around the country when he stated that S. 984 "would seriously jeopardize telephone survey research." The reasons are obvious:

If survey research organizations are unable to monitor interviewers whenever they are conducting research, they cannot ensure that questions are being asked properly and that answers are being properly recorded, or evaluate the study as a whole, including the general tone of the responses to the questionnaire.

If interviewers must be told when monitoring is being conducted, they inevitably will be more cautious and conscientious at those times than at others, thus defeating the control function of the monitoring. We are aware of no comparable requirement that employees in other contexts be given such specific notice that they are being observed.

If respondents are told that the calls are being monitored, this information—which is wholly gratuitous and amounts to "static"—is bound to make at least some respondents less willing to participate and thereby compromise the quality of the population sample.

The additional requirement that Federal agencies affirmatively invite respondents to "opt out" of a survey would cripple the ability of the Labor Department, the Commerce Department, the Federal Trade Commission and other agencies to collect important research.

Eminent academic researchers also have expressed their strong opposition to S. 984. Dr. Stanley Presser of the University of Maryland, who is the President of the American Association for Public Opinion Research, has stated that S. 984 would "impair the ability of both public and private decisionmakers to obtain high-quality information" about public attitudes and opinions "on a wide range of subjects."

Dr. Norman N. Bradburn, the director of research for the National Opinion Research Center at the University of Chicago, and Dr. John M. Kennedy, director of the Center for Survey Research at the University of Indiana, have expressed similar concerns. Dr. Bradburn has warned that S. 984 threatens many government surveys and "would do great harm to the fundamental statistics upon which the Congress and the Administration rely for policy information."

Four leading public opinion researchers—Field Research Corporation, The Gallup Organization, Louis Harris & Associates, Inc., and The Roper Organization—have sent each Member of this subcommittee a joint communication stating their strong opposition to the bill as drafted. (See Attachment A). Indeed, letters opposing the bill have been sent to individual members of the subcommittee by a wide variety

of public opinion polling and survey research organizations and professionals, including some identified above. (See Attachment B).

Mr. Chairman, survey research organizations and other employers should provide their employees with general notice that they may be subject to electronic monitoring, and they should describe the purposes for which the monitoring may be conducted. But it is unreasonable to address the privacy concerns that underlie S. 984 in a manner that would severely impair government and private survey research, which the bill as currently drafted would do.

Thank you.

ATTACHMENT A

TEXT OF WESTERN UNION OPINIONGRAM BY LEADING PUBLIC OPINION RESEARCHERS OPPOSING S. 984

June 21, 1993

To the members of the Subcommittee on Employment and Productivity:

As leading public opinion researchers in the United States, we strongly oppose S. 984, the "Privacy for Consumers and Workers Act," scheduled to be heard by the subcommittee on June 22. As drafted, S. 984 would impose restrictions on supervisory monitoring of telephone interviews that would cripple our ability to ensure the accuracy and quality of polling and other survey data relied upon by government and private decisionmakers alike. S. 984 should be rejected unless these unnecessary and unwarranted restrictions are eliminated.

Field Research Corporation, Mervin D. Field, chairman The Gallup Organization, James K. Clifton, President Louis Harris & Associates, Inc., Humphrey Taylor, President, COO The Roper Organization, Harry W. O'Neill, Vice Chairman

ATTACHMENT B

Illinois

Dr. Norman M. Bradburn, Director of Research, National Opinion Research Center (NORC) at the University of Chicago

John A. Bunge, President, LEGAL MARKETING RESEARCH INC.

Verne B. Churchill, Chairman and CEO, MARKET FACTS

Wesley R. Peters, President, DIMENSION RESEARCH, INC.

Indiana

Dr. John M. Kennedy, Director of the Center for Survey Research at the University of Indiana

Iowa

Dr. J. Ann Selzer, SELZER BODDY, INC., formerly Director of the Iowa Poll

Maryland

Dr. Stanley Presser, Director of the University of Maryland Survey Research Center and the Joint University of Maryland/University of Michigan Program in Survey Methodology, and President of the American Association for Public Opinion Research

Joseph A. Hunt, President, WESTAT

New Hampshire

Michael Kenyon, President, PROJECTIONS INC.

Pennsylvania

John Berrigan, President, National Analysts, Inc.

Paul A. Frattaroli, President, JRP Marketing Research Services, Inc.

B.J. McKenzie, President, Market Dimensions Inc.

Fred B. Soulas, President, ICR Survey Research Group

South Carolina

Frank K. Brown, President, MarketSearch Corporation

Utah

Ron Lindorf, President, Western Wats Center

Senator SIMON. The hearing stands adjourned.

[The appendix follows:]

APPENDIX

SPECIAL REPORT

o n e l e c t r o n i c p r i v a c y

BOSSSES WITH X-RAY EYES

*Your employer
may be using
computers to keep
tabs on you*

BY CHARLES PILLER

Each and every day, Gayle Grant and her colleagues were electronically monitored down to the second as they did their jobs. Unplugging themselves from their job monitors could lead to dismissal. "We punch in and out of three units: the time clock, the VDT [computer terminal], and the telephone keypad known as Collins. We plug a phone jack into Collins that is attached to our headset and [we] receive telephone calls. The VDT and Collins track every second of our day," says Grant (a pseudonym), an airline reservations agent in California. She and her colleagues were allowed 11 seconds between calls and 12 minutes of personal breaks daily. Two episodes of unauthorized unplugged time in a week were cause for disciplinary action. She eventually cracked under the pressure. Grant suffered a nervous breakdown.

Grant's reaction may have been extreme, but her employer merely followed standard practice in many industries, and acted consistently with both the letter and intent of U.S. federal law. The 1986 Electronic Communications Privacy Act (ECPA) prohibits phone and data-line taps with two exceptions: law-enforcement agencies and employers.

The police or FBI can tap lines—but only as a last

resort under court order—to crack criminal conspirators, drug traffickers, and other serious-crime suspects. The courts permit fewer than 1000 such taps each year, nationwide.

Employers have no such limits. They may view employees on closed-circuit TV; tap their phones, E-mail, and network communications; and rummage through their computer files with or without employee knowledge or consent—24 hours a day.

The most pervasive use of monitoring takes place in occupations where tasks are highly repetitive, so productivity can be easily measured. The Communications Workers of America, the union that represents most telecommunications workers, estimates that employers eavesdrop on phone calls between workers and consumers 400 million times per year—more than 750 calls every minute. Mail sorters, word processors, data entry clerks, insurance adjusters, and even computer tech-support specialists, often working on terminals connected to a mainframe, may be monitored constantly or intermittently for speed, errors, and time spent working.

Working in Glass Offices

MOST PROFESSIONAL AND TECHNICAL EMPLOYEES assume that they have nothing to fear. Their privacy is protected by the nature of their jobs—too complex to evaluate by machine, right? To test that assumption, *Macworld* examined 25 popular network-management, integrated groupware, electronic-mail, and remote-access products to see if they could be used to invade employee privacy, and if so, how easily. The study used only Macintosh software, but similar tools are available on other platforms.

If your office network runs on a full-featured network operating system, like Novell NetWare or Microsoft LAN Manager, and is run by a technically astute manager, then your Macintosh and all data transferred from it is an open book. Working from an office across the room or across the country, a network manager—particularly in server-based local area networks—can eavesdrop on virtually every aspect of your networked computing environment with or without your approval or even knowledge. The manager can view the contents of data files and electronic-mail messages, overwrite private pass-

Job Seeker Beware: Electronic Hurdles to Employment

As Pat Perot's eager campaign volunteers were stunned last year when they discovered that agents of the billionaire politician may have looked into some of their backgrounds. The news stimulated an FBI probe into allegations that the Perot campaign organization illegally obtained volunteers' confidential credit reports. The allegations made Perot seem paranoid and sleazy. Actually, he may just have been following the standard practice of many prudent managers, who have become some of the biggest users of electronic tools to investigate job seekers or recent hires.

These managers verify prior-employment claims carefully, of course. Nothing new there. Then they check credit and criminal records online in a matter of minutes. If data is not available in electronic form—for example, college transcripts—they hire research services to get transcripts and deliver their contents to the client's online account in a day or so.

These efforts fit right into a corporate culture that leads a growing number of employers to require drug tests and, leaving nothing to chance, so-called personality profiles. Such profiles may contain hundreds of true-false questions, such as these typical examples: "I have read little or none of the Bible," "My sex life is satisfactory," and "I am very seldom troubled by constipation." They may be used to predict laziness, poor work habits, or psychological problems, or merely to verify whether the job seeker has mainstream values or an outlook consistent with company goals.

"Management is very pragmatic," says Alan F. Westin, a professor at Columbia University who is an expert on electronic privacy issues and an industry consultant. "Management will do whatever the social system and the legal system says, with a special emphasis on whether it helps get the work done to make a better product."

This pragmatic approach derives, in part, from skyrocketing health-insurance and legal bills. The cost of medical care has led many employers to screen out applicants who smoke or are overweight.

And until last summer, many employers searched online data banks to find out whether a job seeker had ever filed a workers'-compensation claim—an insurance claim for an on-the-job injury. Some employers refused to offer a job to anyone who had ever filed a comp claim. The Americans With Disabilities Act, signed into law last year, limits the use of such data banks before a firm offer of employment has been made. But if an employer finds a history of compensation claims after making a job offer, the employer can shift the prospective employee to a job classification that reduces risk of reinjury. If in the employer's opinion no appropriately safe job is available, the offer can be rescinded.

And a rash of lawsuits in the 1980s accusing employers of "negligent hiring" has also pushed employer vigilance to a new standard. You hire a man to do maintenance at your hotel, giving him a passkey to all the rooms, of course. That man rapes a guest. Because you failed to check his criminal history online, you didn't know that he served time for assault six years earlier. Welcome to court. Employers are caught in a dilemma, says Westin. "Do they stay with the hands-off, respect-the-privacy, that's-not-our-business view, or do they respond to their lawyers' warnings to protect themselves against liability, and then bean-counters' warnings that health-benefit costs are going to be out of sight?"

Employers have a responsibility to protect themselves from potential liability and their customers from undue danger. But privacy advocates ask whether society is well served by a business culture that can blacklist people with the cool efficiency of a 9600-bps modem.



Tam O'Neil, a New Jersey business consultant and onetime chairperson of the Perot campaign in his state, claims he was confronted by representatives of Perot's Dallas headquarters who had obtained error-ridden versions of his personal data.

over the net. In short, these tools are only slightly less invasive than others specifically designed for surveillance and used primarily on mainframe systems.

They Like to Watch

NETWORK ADMINISTRATION AND COMMUNICATION tools were designed for valid reasons, not to invade employees' privacy. Like any technology, they are value-neutral. Some vendors even include strongly worded privacy warnings and a few offer options that allow a client Mac to shut out network managers.

The capacity to snoop is there, but is it used? Old surveys and anecdotal accounts suggest that in some industries—telecommunications, insurance, and banking, for example—as many as 80 percent of employees are the subjects of telephone or computer-based monitoring. Such estimates may be inflated, but there is little dispute that many employers monitor routinely. And if the rapid sales and market growth of snooping tools is an indication, monitoring is on the rise. But virtually no rigorous research has been done about how much electronic eavesdropping takes place on the job.

Until now, *Macworld* conducted a survey of CEOs and MIS directors at 301 large, medium, and small businesses in a wide range of industries to find out how much they peek at their employees' work on their computers, and why (see the "Electronic Eavesdropping at Work" charts). About 22 percent of our sample have engaged in searches of employee computer files, voice mail, electronic mail, or other networking communications. In companies with 1000 or more employees, the figure rises to 30 percent. Nearly 16 percent of respondents report that they have checked employees' computerized work files.

The average company in our study employs 3240 people, so the total sample represents the conditions experienced by nearly 1 million workers. This data suggests that some 20 million Americans may be subject to electronic monitoring through their computers (not including telephones) on the job. Meanwhile, only 18 percent of respondents' companies have a written policy regarding electronic privacy for employees.

Managers who endorse electronic surveillance argue that it helps them gauge productivity and chart the work flow of a group of employees. It can generate statistics on individual or departmental accomplishments and plot future work loads. Computer monitoring can even be used to give employees managerial feedback and reduce the need for personal attention from supervisors. In the

words, and audit your time and activities on the network.

All the major electronic-mail and groupware products that combine messaging, file management, and scheduling (such as WordPerfect Office) allow the network administrator to change pass-

words at any time, then read, delete, or alter any messages on the server. With few exceptions, network-monitor programs, such as AG Group's LocalPeek, Farallon Computing's Traffic Watch II, and Neon Software's NetMinder, allow astute managers to read files transmitted



Privacy advocate Mares Rotenberg: "Contrary to what many people believe, 'E-mail is more like a postcard than a sealed letter.'"



Senator Paul Simon: "Employees should not be forced to give up their freedom, dignity, or sacrifice their health when they go to work."



Privacy expert Alan F. Westin: "Monitoring that creates feelings of surveillance and stress is antithetical to the new cultures of management."

Macworld survey, 12 percent of responding employers endorse monitoring for evaluating performance or productivity.

Monitoring can also increase safety or adherence to company rules, some employers contend. Some trucking companies, for example, set on-board monitors to record speed, engine-idling time, and length of stops. The system ostensibly tries to ensure that truckers drive safely and take adequate rest breaks.

Companies that deal in sensitive data may feel compelled to guard against disloyal or merely careless employees who might divulge it to competitors (see the sidebar "To Catch a Spy: Is Workplace E-Mail Private?"). And 4 percent of our survey respondents endorse electronic monitoring "for routinely verifying employee honesty." A much higher number—23 percent—feel electronic monitoring is a good tool where reasonable evidence of wrongdoing, such as theft or negligence, comes to light.

While nearly half of the managers in our survey endorse the concept of electronic monitoring, and nearly a fourth actually conduct electronic monitoring, most of those don't do it often. About 71 percent of those who conducted such searches did so only five or fewer times in the preceding two years. Only two companies had searched employees' work files, voice mail, electronic mail, or networking communications more than 100 times during that period.

From Watching to Intruding

THE MACWORLD SURVEY INDICATES THAT many employers may recognize that excessive monitoring has possible negative side effects. "Technology now allows employers to cross the line from monitoring the work to monitoring the worker," Cindis Cameron, a field organizer for 9 to 5, National Association of Work-

A Model Employment-Privacy Policy

Macworld's privacy survey suggests that less than one-fifth of U.S. employers have electronic privacy policies. So in most cases, employees may have no idea whether or how employers monitor their everyday activities and work files. The following points represent what many privacy advocates consider basic features for a good electronic-privacy policy for employers:

- Employees are entitled to reasonable expectations of personal privacy on the job.
- Employees know what electronic surveillance tools are used, and how management uses the collected data.
- Management uses electronic monitoring or searches of data files, network communications, or electronic mail to the minimum extent possible. Continuous monitoring is not permitted.
- Employees participate in decisions about how and when electronic monitoring or searches take place.
- Data is gathered and used only for clearly defined work-related purposes.
- Management will not engage in secret monitoring or searches, except when credible evidence of criminal activity or other serious wrongdoing comes to light.
- Monitoring data will not be the sole factor in evaluating employee performance.
- Employees can inspect, challenge, and correct electronic records kept on their activities or files captured through electronic means.
- Records no longer relevant to the purposes they were collected for will be destroyed.
- Monitoring data that identifies individual employees will not be released to any third party, except to comply with legal requirements.
- Employees or prospective employees cannot waive privacy rights.
- Managers who violate these privacy principles are subject to discipline or termination.

ing Women, told a Senate committee. She cites the case of an express-mail company employee whose computer logs the length and frequency of her trips to the bathroom. The woman was reprimanded for using the bathroom four times in a single day.

Some employers use monitoring data in efforts to boost productivity through competition—by posting data publicly. One enterprising Florida company, Thomas Powell Associates, found a way to automate the process. "I got the idea watching the [Miami] Dolphins [football team]," says a company founder. "Those athletes play their hearts out. Why? Certainly the money helps, but it's not the real reason. They play at 100 percent

because everything they do is seen by hundreds of thousands of people—instantly." The company produces and sells software that instantaneously puts every telephone operator or telemarketer's productivity statistics on a computer screen, visible to all employees.

Do such schemes pay off? "Monitoring that creates feelings of surveillance and stress is antithetical to the new cultures of management that our society is moving toward," says Alan F. Westin, a professor at Columbia University and consultant to the data-gathering giant Equifax. Westin practically invented the idea of "electronic privacy" and has written on the subject for three decades. "[If management] doesn't motivate employ-

To Catch a Spy: Is Workplace E-Mail Private?

Most people believe that electronic-mail messages are secured by a personal password—as private as a letter in the U.S. mail. "They are finding out," says Marc Rotenberg, Washington, D.C., director of Computer Professionals for Social Responsibility, "that E-mail is more like a postcard than a sealed letter."

Test case for privacy Employers have ready means to read E-mail messages, and many do just that, as computer executive Eugene Wang found out recently. His case, involving two Silicon Valley companies, could break new ground in electronic-privacy law.

Wang, who was Borland International's vice president for computer languages, defected to a direct competitor, Symantec Corporation, last September. Court documents filed by Borland attorneys state that shortly after Wang announced his departure, Borland execs found E-mail addressed from Wang to Symantec CEO Gordon Eubanks. The messages allegedly revealed top-secret corporate data, including marketing plans, product-release dates, and detailed information on Borland's game plan against Symantec. The police and FBI were called in shortly thereafter, and seized other documents at Eubanks' and Wang's homes.

Because Wang used MCI Mail—a commercial E-mail service—allegedly to transfer data to Eubanks, electronic privacy has become a key issue in the case. Wang and Eubanks, who have been indicted on criminal felony charges involving theft of trade secrets, deny that they violated trade secrecy laws. They also argue that when Borland viewed Wang's MCI Mail messages, the company may have violated federal law. If so, the confiscated E-mail messages might not be admissible in court. The 1986 Electronic Communications Privacy Act (ECPA) protects messages sent on commercial E-mail, such as MCI Mail, from outside or unauthorized users. "Even if Borland had gathered evidence in a legitimate and legal way regarding privacy, [Eubanks and Wang] would still be innocent," says Symantec attorney James McManis. "But if after reviewing all the data, it appears to us that there has been a violation of the (ECPA) statute, we will raise that."

Borland counters that it paid for Wang's MCI Mail account, and therefore had every right to inspect the messages. "New employees at Borland are given an MCI [Mail] password that is on file with a Borland administrator," says Borland spokesperson Steve Grady. "You do not have a reasonable expectation of privacy in an E-mail system that is given to you for company business by your employer." If the privacy issue is litigated, it could set new standards on the privacy of commercial E-mail.

California challenges Federal rules regarding in-house electronic mail are less ambiguous than those governing commercial E-mail. ECPA treats internal company communications as company property. And a *Macworld* survey suggests that some 375,000 employers agree. About 9 percent of respondents—CEOs and MIS directors of U.S. companies of all sizes—indicate that they sometimes search employee E-mail files. This prerogative is being challenged in California, where the state constitution specifically protects privacy, unlike the U.S. Constitution. Court documents indicate that Alana Shoars, formerly E-mail director of Epson America, claims she was fired in 1990 for questioning her boss's right to read hundreds of E-mail messages sent between other employees. Shoars filed wrongful-termination and class-action lawsuits against Epson. Her attorney, Noel Shipman, claims that by reading employee E-mail messages, Epson violated both the state constitution's privacy provision as well as a California eavesdropping statute.

Shipman also represents two employees of Nissan Motor Corporation embroiled in an E-mail controversy. Rhonda Hall and Bonita Bourke were allegedly fired from their jobs installing software and training other employees. A legal brief filed by Shipman claims that the two were fired or forced to resign after complaining about managers printing and reviewing printouts of personal messages from the company's E-mail system—messages they assumed were private. The two sued for invasion of privacy and wrongful termination.

Both the Nissan and Epson cases were dismissed by lower courts, but are now on appeal. If the plaintiffs prevail in either situation, the legal status of personal E-mail messages on internal company systems will be thrown open, perhaps resulting in greater privacy rights.



Symantec's Eugene Wang, who stands accused of theft of trade secrets, is at the center of a bitter debate over the privacy of commercial E-mail services that are used for company business.

ees to be more participative, to be more committed to the workplace, then the chances of producing the kind of quality work that will compete with the Japanese and the Germans are very low."

And managers concerned with both productivity and containing health-insurance costs may find electronic monitoring to be self-defeating. Electronic monitoring increases employee "boredom, tension, anxiety, depression, anger, and fatigue," according to a recent study of 745 employees of telecommunications companies, jointly conducted by researchers from the University of Wisconsin and the Communications Workers of America. These findings confirm earlier studies that implicate electronic monitoring as a major workplace stress factor—linked, in part, to the sense of powerlessness that monitored employees feel.

Possible Legislative Relief

SUCH CONCERNS HAVE STIMULATED some members of Congress to ask what constitutes fair and appropriate monitoring. The proposed Privacy for Consumers and Workers Act failed in the last Congress, but Capitol insiders have high hopes for it in this session. The proposed law would limit how monitoring could take place in these ways:

- Employers would have to tell new hires how they might be monitored and how the collected data would be used.
- Employers would be required to give advance warning that monitoring will take place (except for employees on probation)—possibly including a signal light or beep tone during monitoring.
- The total time that an employee could be monitored would be capped at two hours per week.
- Secret, periodic, or random monitoring of long-term employees would be prohibited.

Macworld's survey shows that the law would force policy changes for many businesses. We found that only 31 percent of companies that conduct electronic monitoring or searches of employee computers, voice mail, electronic mail, or networking communications give employees advance warning.

Many companies recognize consumer demand for privacy protections, and they have stepped forward with pioneering consumer-privacy policies that go far beyond the limited legal requirements. But few companies have policies in place that go as far to protect employee privacy as the Privacy for Consumers and Workers Act would mandate.

Companies that have led the way on consumer-privacy concerns, such as American Express, Citibank, and Equifax,

describe their electronic monitoring of employees as strictly limited. But they would not release internal policies on employee privacy, and they acknowledged surveillance practices beyond what would be allowed by some features of the congressional proposal.

One reason that employers may give less weight to employee privacy is that they feel countervailing pressure: legal requirements to monitor or audit employee activities, particularly in information-intensive industries. So most employers comply with employee-monitoring laws and regulations as they see fit, rather than breaking new ground by minimizing monitoring and using the least-invasive approach, says privacy expert Vestin.

Industry groups also castigate the Privacy for Consumers and Workers Act. "An employer would be put in the awkward position of having to advise suspected thieves when they are being observed," Vincent Ruffolo, president of Security Companies Organized for Legislative Action, told a Senate hearing.

If the proposal is enacted, says Lawrence Fineran of the National Association of Manufacturers (NAM), customer service will erode, and manufacturers might have to abandon certain kinds of computer-aided manufacturing. "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," Fineran says. "Otherwise the United States may as well let the information age pass it by." Yet Japan and most of Europe already impose much tighter restrictions on employee surveillance than the U.S. proposal would mandate.

Few privacy advocates argue that monitoring should be eliminated. But they say industry ignores a critical factor: most employees are hardworking and honest. "The problem with the business community," says Louis Maltbe, director of the American Civil Liberties Union's Workers Rights Project, "is that they are trying to make the rules with the assumption that every employee is a goldbrick."

Maltbe and other advocates see reasonable privacy protection going far beyond the provisions of the proposed law, to the point where employees have some control over monitoring practices and data collected (see the sidebar "A Model Employment-Privacy Policy").

"There has been kind of a reflex reaction, automatically resisting things that ultimately have been very helpful to industry," says Senator Paul Simon, D-Ill., principal sponsor of the Senate version of the privacy bill. "The banking industry resisted having—believe it or

MACWORLD POLL

Electronic Eavesdropping at Work

Workers are routinely monitored in some industries, but how pervasive is the practice? To find out, Macworld conducted the first national survey designed to find out how and why businesses monitor employees. Top corporate managers from 301 businesses of all sizes and in a wide range of industries participated.

More than 21 percent of respondents—30 percent in large companies—have "engaged in searches of employee computer files, voice mail, electronic mail, or other networking communications." Nearly 18 percent report having

checked computerized employee work files, and 9 percent having searched employee e-mail.

These data suggest that some 20 million Americans are subject to electronic monitoring, in its own right or as a byproduct of network searches. Better ask your boss directly. Only 13 percent of respondents' companies had a written policy regarding electronic privacy. And only 31 percent of companies that conduct electronic monitoring or searches of employee computers, voice mail, e-mail, or networking communications give employees advance warning.

Electronic Search Practices

Are employee files searched?  Yes 21.6%

If yes:

Which files?

Electronic work files	73.8
E-mail	41.5
Network messages	27.7
Voice mail	15.4

On whose authority?

Executives	66.2
Middle managers	16.9
Personal managers	10.8
MIS director	44.6

Why?

Monitor work flow	29.2
Investigate thefts	29.2
Investigate espionage	21.5
Review performance	2.2
Prevent harassment	5.2
Seek missing data	2.1
Seek illegal software	2.1
Prevent personal use	3.1

How often? (last 3 years)

More than 100	2.1
30 to 100	2.1
20 to 49	0.0
10 to 24	7.7
8 to 9	5.2
1 to 5	70.8
None	4.8

Are employees warned?

Yes	30.9
No	66.7

Company Privacy Policies

Do you have a written policy on privacy?  Yes 35.9%

Do you have a policy on electronic privacy?

 Yes 18.3%

Are privacy policies known to employees?

 Yes 33.6%

Company Personnel-Record Policies

Are personnel records kept electronically?  Yes 82.2%

Do employees have access to records on any medium?

 Yes 51.8%

Who has unrestricted access?

Executives	51.8
Middle managers	14.0
Personal managers	66.1
Payroll managers	2.0

Who has need-to-know access?

Executives	61.1
Middle managers	41.9
Personal managers	52.2
Payroll managers	7.3

Management Philosophy on Electronic Monitoring

Never acceptable	34.6
Usually or always counterproductive	16.3
Good tool to verify evidence of wrongdoing	22.6
Good tool to routinely monitor performance	12.0
Good tool to enhance performance	7.3
Good tool to routinely verify honesty	4.0

Totals may not equal 100 percent, due to non-responses or multiple responses.

Margin of error for responses is ± 2.9 percent.

not—federal insurance for banks. Now no bank would want to do without it," he adds. "Some companies are [giving prior notice of monitoring] right now and having no difficulties. I think it improves employee "relationships," Simon says. In

any case, he argues, "employees should not be forced to give up their freedom, dignity, or sacrifice their health when they go to work." ■

Research assistance by JIM CARR.

PRIVACY IN PERIL

*How computers
are making
private life a
thing of the past*

BY CHARLES PILLER

In recent years, gathering and sharing personal information has become a way of life for business and government. People have kept track of one another for millennia, of course. But the advent of telecommunications, the growth of centralized government, and the rise of massive credit and insurance industries that manage vast computerized databases have turned the modest records of an insular society into a bazaar of data available to nearly anyone for a price.

The U.S. Constitution carries no explicit guarantee of personal privacy. But most Americans consider the ability to conduct one's personal affairs relatively free from unwanted intrusions to lie an inherent human right. A year-long *Starworld* investigation shows that such a right stands little chance against new electronic technologies that make most people's lives as clear as glass.

From a personal computer anywhere in the world, data can be gathered from limitlessly broad and diverse sources. The ability to capture, sort, and analyze that data is often nearly instantaneous. The force of such tools has overwhelmed the capacity of laws and social mores to protect privacy.

Until the last few years, if you wanted to find out,

if anyone had sued Roger Heinen, the former Apple vice president who defected to Microsoft in January, you had to laboriously check, in person, at various county courthouses. I spent about two minutes doing the same thing online.

"As technology becomes ever more penetrating and intrusive, it becomes possible to gather information with laserlike specificity and spongelike absorptency," says Gary T. Maza, a privacy expert who teaches at the University of Colorado. "Information leakage becomes rampant; indeed, it is hemorrhaging. Barriers and boundaries—be they distance, darkness, time, walls, windows, even skin—that have been fundamental to our conceptions of privacy, liberty, and individuality give way. Actions, feelings, thoughts, acts, even futures are increasingly visible." Easy access has blurred the borders of private life.

The public views these developments with growing alarm. In a 1992 poll conducted by Louis Harris and Associates, 78 percent of Americans expressed concern about their personal privacy, up from about a third of those polled in 1970, and up from 64 percent in 1978. Perceived threats to personal privacy from computers rose from 38 percent in 1974 to 68 percent last year.

In a 1991 *Time/CNN* poll, 93 percent of respondents asserted that companies that sell personal data should be required to ask permission from individuals in advance. The 1990 census showed the highest rates of noncooperation ever—the result of fears that participation could place personal information in jeopardy, contend some privacy advocates. And California's Privacy Rights Clearinghouse—the first privacy hotline in the nation—logged more than 5400 calls within three months of its inception last November.

What They Have on You

PUBLIC CONCERNS HAVE RISEN IN TANDEM WITH the proliferation of personal records kept by government, corporations, and employers. New forms of data are coming online all the time. Nearly every quantifiable aspect of our lives—and many a judgment call—finds its way into data banks where it is exchanged, sold, and resold, again and again.

The sheer volume of available data is stunning. In 1990, the U.S. General Accounting Office, an arm of Congress, conducted a survey of federal data banks that contain health, financial, Social Security, and a wide range of other personal data. That incomplete tally included 910 major data banks with billions of individual records. Much of the information

A Model Consumer-Privacy Code

Feeling the sting of consumer anger at the deluge of direct-marketing solicitations and credit-report problems, many companies have voluntarily established privacy codes of conduct. The following model code combines high points from corporate and trade-association policies with the views of privacy advocates. This model is based on reasonable expectations for business practices in today's world. Therefore, it does not address three ideas that could prove critical to protecting privacy in the long term:

- An opt-in system for direct marketing, in which the personal data would be collected only on consumers who request that their names be placed on marketing lists.
- Mandatory updates, audits, and correction of public records data.
- The option to replace credit cards that have an electronic bill for every consumer transaction with anonymous debit cards, as some nations now do (see photo below). But for now, the following measures would go a long way toward protecting consumer privacy in electronic transactions.

Data Collection

- Fully disclose to consumers the nature of the data collected.
- Collect only data necessary to your business purpose.
- Contact consumers yearly to disclose current and anticipated secondary uses of their personal data, and to offer an opt-out option.

Direct Marketing

- For small companies: Don't sell detailed personal data that can be tracked to specific individuals. Do require customers to certify that list data will not be resold.
- For large companies: Don't sell personal data at all. Instead, charge customers to distribute marketing materials relevant to their interests.

Data Accuracy

- Conduct systematic and regular audits to catch data entry errors.
- Disclose the source of data on request from individual consumers.
- Provide easy and free methods for consumers to challenge records that concern them and if needed, to correct those records.

Data Security

- Limit access to personal data on a "need to know" basis—available only for legitimate business purposes.
- Train employees to prevent unauthorized disclosure, and audit their compliance at regular intervals.

Credit and Medical Data Bureaus

- Provide free yearly complete reports to consumers.
- Create a speedy appeal process for consumers to challenge their data.

Sunset Provisions

- Follow all laws in expunging incriminating records such as criminal convictions or bankruptcies.
- Periodically check for and purge all obsolete data.



Phone debit cards, such as this one from France, work like computer transit tickets. Each call's cost is deducted from the prepaid card, obviating detailed billing records.

from these computerized systems is open to other government agencies and corporations, or sold to thousands of commercial data banks that trade on records about your home, possessions, stock transactions, family characteristics, and buying habits.

And once created, a record rarely disappears. "In our society, there is a tendency to collect data without a clear purpose. And it stays around for years," says Alan Brill, head of the information-security practice for Kroll Associates, the largest and most successful private-investigation firm in the country. "It's like

vampire data. It rises up from the dead to bite you," he says.

Obsolete information can mislead. Out of context, a single incriminating element in someone's personal history can become a defining characteristic. Suppose you were guilty of possessing a small quantity of marijuana in 1985, but haven't taken a toke since 1986. Should that conviction affect your employment prospects in 1993?

The problems grow when the data is wrong. If data banks contain millions or billions of records, it's hardly surprising that they sometimes slip a digit or two.

Consider the Big Three credit bureaus—TRW, Equifax, and Trans Union—which are among the largest and most closely monitored purveyors of personal data. These agencies compile and sell the records of key economic transactions for a large majority of American consumers.

Early this year, TRW agreed to pay \$1000 each to about 1200 residents of Norwich, Vermont, whom the company erroneously designated as deadbeats due to a coding error. A 1988 survey of 1500 credit reports found that 43 percent contained errors. And a 1991 survey by Consumers Union found errors in 48 percent of reports requested from the Big Three, including 19 percent with inaccuracies that could cause a denial of credit, such as a delinquent debt. The Federal Trade Commission receives more complaints about credit bureaus than about any other industry.

Errors are not always the fault of the credit bureau—it might lie from one of its sources. "In many cases the [credit bureaus'] responsibility to their customers is to give an accurate reflection of what's in the public record, and that public record may itself be inaccurate," explains Steve Metalitz, general counsel of the Information Industries Association, which represents about 500 companies that gather and resell data.

Regardless of the origin of such errors, there are no clear lines of responsibility for correcting the record. Meanwhile, the victim's life may descend into a Kafka-esque nightmare.

Values in Conflict

THE NEW STANDARDS OF ELECTRONIC intrusion upset the balance between two distinctly American values: an open and accountable society, and the right to be left alone.

There are many reasons to keep public records open and easily accessible. Society has the responsibility, for example, to monitor illegal activities, to capture criminals, and to preserve public safety. If electronic privacy rights were absolute, we would never have learned about Oliver North's E-mail messages, which helped unravel the Iran-Contra scandal. And organized-crime kingpin John Gotti might never have been convicted had for the tap on his phone.

Yet data collection has a dark side. In the 1960s and 1970s, J. Edgar Hoover's FBI gathered personal data by any means possible and often used it to blackmail innocent people, sometimes destroying their lives.

Employers have a right to guard against ineptitude, criminality, and cor-



Trade association spokesman Steve Metallitz: "In many cases, the [credit bureaus'] responsibility is to give an accurate reflection of what's in the public record, and that record may itself be inaccurate."



Privacy advocate Evan Handrick: "To me, junk mail is not the most burning privacy issue, but I can see it annoys the hell out of a lot of people." He receives hundreds of letters that prove the point.



Information industry lawyer Ronald Plesser: "Is the use of information compatible with the purpose for which it was collected?" If not, misinterpretation or cross exploitation usually follows.

porate spies. But should employers be free to search at will any and all employee computer files, E-mail, voice-mail, and data transmissions over a company's local area network? (See "Bosses with X-Ray Eyes," in this issue.)

Government investigators, members of the press, and the public at large may have a legitimate interest, for example, in knowing whether U.S. Transportation Secretary Federico Peña has ever been tagged for drunk driving. (We have no reason to believe he has.) But when the driving records of millions of people are sold to mass marketers of automobile insurance or alcohol-treatment programs, has the public trust been violated?

Beyond Junk Mail

THE ISSUE TRANSCENDS ELECTRONIC-list sales and the invasive micro-marketing tactics they stimulate. Personal data itself has become a commodity for sale on the open electronic market to anyone who owns a personal computer.

Take the case of Marketplace: Households, an ill-fated joint venture of Lotus Development Corporation, a software developer, and the Equifax credit bureau. Marketplace would have placed the names, estimated incomes, purchasing habits, marital status, and other data on 120 million consumers on a CD-ROM—the nation on a disc for only \$700. Few consumers were persuaded by the project's privacy protections. And they let it be known: 30,000 angry letters killed Marketplace. Shortly thereafter, in the face of mounting consumer pressure, Equifax agreed to quit selling any consumer credit data to direct-marketing vendors.

In the space of a year Equifax went from promoting one of the most far-reaching incursions into privacy ever con-

templated to opting out of the credit-data marketing business altogether. Early this year, TRW (but not Trans Union) followed suit.

But the personal-information market hardly depends on Equifax or TRW. Thousands of other data resellers—*Macworld* among them—offer lists of likely buyers. This wealth of sources has spawned a sprawling information-reselling industry. The Burwell Directory of Information Brokers describes 1253 commercial services with names like Disclosure, Access Information, and Answer Associates.

Many of these services provide only data on companies, economic trends, or sociopolitical issues. But personal information—address, marital, salary, driving, and employment history; corporate affiliations; who your neighbors are; vehicle and real estate holdings; civil and criminal court records—and much of the rest of the trail of bytes left by all of us is now available from scores of commercial sources. And to make their lives easier, the data-hungry turn to supermarkets of online information.

Down in the Data Mines

SO-CALLED SUPERBUREAUS BUY ACCESS to the major credit bureaus, state and federal agencies, and just about any other private or public-record repository they can find. They provide one-stop shopping for online data. The data-reselling trade is the electronic equivalent of the gold rush—few legal restrictions apply, and there is lots of money to be made if you own the mine.

Standards vary widely, but some information brokers are less than scrupulous in screening their clients. Even legally shielded data, such as credit and phone records, as well as arrests that do not

result in convictions, frequently are revealed to a wide range of qualified or merely determined and savvy requesters. These include private investigators, direct marketers, the press, FBI agents, lawyers,

The U.S. is
a laughingstock among
privacy experts
because we protect video-
tape-rental records,
but not medical records

insurance companies, corporate spies, and vindictive ex-spouses.

For data mining to be worthwhile, the information has to be difficult or impractical to obtain using conventional methods, but worth the cost of electronic extraction. It is.

Consider the results of an online experiment my colleague Galen Grunson and I conducted during research for this article. First we selected prominent individuals from the entertainment industry,

Shattering the Illusion of Privacy

THE GOAL

How easy is it to obtain someone's home address? Social Security number? Real estate holdings? Macworld investigated 18 business leaders, politicians, Hollywood celebrities, and sports figures. We primarily targeted residents of California, where most public records are online, and sought all legally accessible data available from four commercial and two governmental data

suppliers. We exhausted the systems' resources after spending about \$112 per subject. In addition to the records shown below, we searched public records for criminal court filings, fictitious business names, and records of bankruptcies, insider trading transactions, trusts, deeds, powers of attorney, and other legal matters.

THE SUBJECTS

In addition to the pictured subjects, we obtained similar data on U.S. Attorney General Janet Reno, U.S. Representative Robert K. Dornan, actor Clint Eastwood, Microsoft executive Roger Hahn, former U.S. Attorney General Edwin Meese III, restaurateur Wolfgang Puck, San Francisco Mayor Frank Jordan, and several others.

George Lucas
Movie producer

Joe Montana
Football star

Lion Panetta
Director, U.S. Office of
Management/Budget

William H. Hearst III
Publisher,
San Francisco Examiner

Richard M. Rosenberg
CEO, Bank of America



WHAT WE FOUND

Personal Data

Birth date

Home address

Home phone

Social Security number

Neighbors' address/phone

Driver record*

Marriage record

Voter registration

Biography

Legal/financial data

Tax liens

Campaign contributions**

Vehicles owned

Real estate owned

Commercial loans/debts

Civil court filings

Corporate ties***

*Includes physical characteristics. **\$200 or greater contributions, federal offices only. ***CEO or registered agent of a corporation. Macworld does not guarantee the completeness or accuracy of the records we obtained.

business, politics, the Macintosh industry, and sports, including Hollywood producer (and friend of President Bill Clinton) Harry Thomson, former San Francisco 49ers quarterback Joe Montana, and Bank of America CEO Richard Rosenberg. Then we tried to find out everything we could on them, with the following restrictions: we did not seek legally protected data, and all the information had to be obtained online.

For this modest search we spent an average of only \$112 and 75 minutes per subject. Even so, we unearthed the essential financial, legal, marital, and residential histories of nearly all of our subjects (see the chart "Shattering the Illusion of Privacy"). In short, we compiled elec-

tronic dossiers. And these were the efforts of data-mining neophytes.

As online services become increasingly interconnected, affordable, and fast, the ability to build electronic dossiers may quickly become the hottest privacy issue of the next century. Then again, there are so many pressing privacy issues and such widely divergent sensibilities about personal privacy, even professional privacy advocates have trouble deciding what's most important.

A Question of Priorities

"TO ME, JUNK MAIL IS NOT THE MOST burning privacy issue," says Evan Hendricks, editor of the *Privacy Times* newsletter. "But I can see it annoys the

hell out of a lot of people." To illustrate the point, he pulled out a box of 100 recent letters from consumers apoplectic over a deluge of unwanted letters flowing into their mailboxes. Financial interests and personal sensibilities about electronic privacy cover an enormously broad spectrum. This makes it hard to separate trivial problems from real invasions that damage people.

"You have to choose a certain bundle of records, prioritize those records, and create a trustee situation around them," argues Jerry Berman, Washington, D.C., director of the Electronic Frontier Foundation, an advocacy group for computer users. "You cannot protect all data, bit by bit, byte by byte."

What should be in the bundle? Medical records are a top priority "due to the sensitivity of the data and the lack of any existing legislation to protect it," says Ronald Plesser, a lawyer who represents the Information Industry and headed President Clinton's transition team for the Federal Communications Commission. Tighter privacy controls for banking, tax, and credit records are also near the top of every privacy advocate's list.

"Around the world, the U.S. is a laughingstock among privacy experts because we have a law protecting video-tape-rental records, but not medical records," Hendricks adds. (The release of individual video-rental records was sharply restricted after a reporter singled the details of Judge Robert Bork's viewing habits during his confirmation hearings for a seat on the U.S. Supreme Court two years ago.)

Outcry over Credit Records

PUBLIC OUTCRY AND POLITICAL PRESSURE have already reformed the major credit bureaus: all three bureaus now permit consumers to view and correct credit reports, although the reports released to consumers may not be as detailed as those given to, say, prospective employers or landlords. What's missing is usually information like an assessment of the person's credit risk.

TRW makes reports available free to individual consumers. Equifax has opened a toll-free line (800/685-1111) to respond to consumer questions. Rad publicity has prompted credit agencies—particularly Equifax—to more strictly screen companies and information brokers who seek access to credit reports. And in February, federal legislation was introduced that would force credit bureaus to correct errors within 30 days, and would hold banks and retailers accountable for the quality of the information they turn over to credit bureaus.

But credit records represent only a small fraction of online personal data. The far broader category of public records—real estate ownership, court records, tax liens, bankruptcy filings, voter registration data, auto and driver records, marriage records, and the like—should be on the table, argues Jan-Lori Goldman of the American Civil Liberties Union's Privacy Project.

"We're now asking a question that hasn't been asked before: What is the public's interest in accessing this information?" she says. Should the price of a driver's license be that you give up your detailed personal description to anyone who wants to buy it? Privacy advocates call for a close look at online data mining

and they recommend limits on the collection of unduly detailed electronic dossiers.

Plesser, the Clinton transition team adviser, suggests using this test: "Is the use of the information compatible with the purpose for which it was collected?" When the answer is no, the prospect of misinterpretation or crass exploitation usually follows.

De Access and Privacy Conflict

MANY LAWYERS, DIRECT MARKETERS, and reporters say that radical restrictions on public-records data would give them electronic migraines, and could even make their jobs impossible. But Marc Rotenberg, Washington, D.C., director of Computer Professionals for Social Responsibility, warns against believing arguments that access and privacy rights are inherently incompatible. Such conflicts are often promoted by those who stand to profit by expanding access to private data, he argues.

Take the case of caller ID. Such systems instantly reveal a caller's number on a display attached to the phone of the party receiving the call. Caller ID has often been portrayed in the media as a simple case of competing consumer interests—some people advocate the system as a way to apprehend heavy breathers; others fear caller ID as an open invitation for businesses to surreptitiously pad marketing lists and for hollies to find battered spouses hiding in shelters.

But there is a third factor. "With the advent of caller ID, the telephone companies stood at the fulcrum of this information transfer and stood to benefit from the proposed sale of personal telephone numbers," Rotenberg says. How? They can charge businesses for using the caller ID service and then charge consumers for being listed or not listed, depending on the local laws' requirements.

Managing Electronic Privacy

HOW SHOULD SUCH CONFLICTS BE resolved? In the U.S., a wide range of federal and state agencies grapple with privacy issues. Sometimes they have exemplary tools to work with, such as the Electronic Communications Privacy Act, which bans most electronic eavesdropping over phone or data lines.

More often, there is little or no legal protection of personal data. Part of the reason may be that no government agency reviews privacy issues comprehensively or tries to map a coherent overall policy on the wide range of consumer, commercial, and workplace privacy issues.

Canada and many European nations use privacy commissions or data-protec-

tion agencies to advise their governments on privacy policy, protect consumer rights, or regulate corporations. Most privacy advocates in this country see some kind of privacy board—staffed with specialists equipped to evaluate emerging

O ur society

*collects and stores data
without a clear purpose.*

It's like vampire

*data. It rises up from the
dead to bite you.*

privacy issues—as a key to timely and effective regulation.

"The U.S. is an embarrassment to the privacy movement overseas," says Simon Davies, director of the Australian Privacy Foundation. "The U.S. stands alone as an example of what a superpower should not do in privacy."

A U.S. data-protection board with advisory powers was proposed in Congress in 1991. Proponents believe that such a board could sort out the privacy implications of new services or technologies before they saturate the marketplace or are unnecessarily quashed by consumer outrage.

The developers of Lotus Marketplace might have averted years of fruitless development if a privacy board had offered feedback on the idea in advance. The National Research and Education Network (NREN), promoted by the Clinton administration, would be a prime candidate for advance evaluation by a privacy board. This multibillion-dollar "data superhighway" would theoretically allow tens of millions of Americans to communicate data, voice, video, and other forms of media at many times the speed of current networks. Protecting personal information on NREN is "the privacy issue of the twenty-first century," says the Elec-

11 Easy Ways to Safeguard Your Electronic Privacy

Other than a few hermits living on remote mountain peaks, few of us can realistically give up insurance, credit cards, and electronic banking. Sacrificing some personal privacy is the price of admission to our consumer society. But the following steps can curb some of the worst invasions of privacy in the lives of today's consumers.

Personal Identification

- Give only the minimum data required for commercial transactions. Leave all Social Security, home phone, driver's license, and credit card numbers off checks whenever possible. And don't give such numbers for credit card purchases; in most cases they are not needed by merchants.

Credit

- Obtain your credit report yearly from one or more of the big three credit bureaus (Equifax, Trans Union, and TRW); to contact these companies check for an office in your area, and try to correct any errors you detect.
- When rejected for credit, ask why; then verify the accuracy of the data used to reject you.

Insurance

- Obtain a free copy of your medical record from the Medical Information Bureau (617/476-3660), an agency used by more than 750 insurance companies to calculate financial risk. If (in consultation with your doctor) you detect errors, contact the bureau and demand that the record be corrected promptly.
- When rejected for insurance, ask why; then verify the accuracy of the data used to reject your policy application.

Marketing

- When offered "free" premiums, rebates, or other incentives in return for giving personal data for a marketing list, find out who will use the data and for what purpose. Ask if you can participate by giving minimal information, such as name and address.
- When you return warranty cards, provide only information essential to the warranty service. Ignore personal questions used only for marketing.
- To pare back junk mail, calls, and faxes, check the "opt-out" box many companies offer on warranty forms and subscription cards. Ask solicitors to take your name off their lists, and get the Direct Marketing Association (212/689-4977, ext. 369) to remove your name from its members' lists.
- If you participate in marketing or public opinion surveys, verify that answers will be used only in conjunction with those of other respondents, and that no personal information can be traced back to you.

Telecommunications

- Some states allow caller ID services—a way to view a caller's phone number on a monitor attached to your phone before answering. In most such states, the phone company must provide callers with an option to block viewing of their number. Ask your phone company to set up that blocking ability.

Banking

- Ask your bank to agree in writing to disclose your personal financial records only to legally authorized requesters, and to notify you when such requests are granted.



Charles Hamel, a critic of the Alyeska Pipeline Service Company, which operates the trans-Alaska oil pipeline, was the subject of an elaborate spying operation initiated by the company. Alyeska, through a third-party investigator, gained access to Hamel's credit and phone records, as well as personal financial data.

and complaint-resolution responsibilities that privacy advocates see as minimum requirements to safeguard consumer and worker rights.

For now at least, the privacy implications of new technologies are likely to be confronted by government on an ad hoc basis, and only after the public has cried out for relief.

The Role of Technology

PRIVACY ADVOCATES ARE FOND OF SAYING that the United States is "first in technology, last in privacy protection." And while technology has made our personal lives more transparent, privacy and technology are not inherently antagonistic. In the absence of a privacy board, new technologies may prove one of the most potent forces driving what *Privacy Times's* Hendricks calls "the right to informational self-determination."

Technology has already alleviated many everyday intrusions: Airport X-ray units have made hand searches of luggage rare. With magnetic markers in books and clothing, searches of purses or briefcases in libraries and stores are quickly becoming obsolete. And encryption software makes computer files infinitely more secure than paper documents in locked cabinets.

A California company has even developed a "video game" to replace drug testing for truck drivers and other workers. Before each shift, employees go through a short hand-eye coordination exercise at a computer terminal. If they fail this simple test, they skip the shift or are moved to less demanding work that day. The technique not only screens out drug or alcohol intoxication, but also seems to identify workers who are excessively fatigued or preoccupied. One trucking company reports a dramatic decrease in accidents and worker errors after a year using the system.

Such stories are encouraging, but so far they are rare. Industry and society face a daunting challenge: to develop technologies that protect personal privacy faster than those that threaten privacy.

The stakes are high. "Privacy allows us to move freely between the public world and private world, to form smaller communities within the larger community, to share our concerns, dreams, and beliefs with our close friends. To have secrets," Rotenberg commented in an online forum sponsored last year by the *Wall Street Journal*. "There is a close tie between privacy and pluralism. . . . This is what I suspect is at risk in the current rush to record and exchange personal data. Global Village in theory. Surveillance State in practice." ■

tronic Frontier Foundation's Berman, yet so far the government has ignored the privacy implications of the project.

With powerful industry interests arrayed against it, privacy-board legislation has gone nowhere. "American consumers have more choice than any other consumers in the world. Part of the reason is that we are an open information

society," says Lorna Christi of the Direct Marketing Association, echoing the industry's general fear of government regulation. "Self-regulation is working."

John Baker, senior vice president of Equifax, supports the idea of a board that conducts research and gives confidential advice to industry. But he objects to giving a privacy board the very investigative

My name is Sarah Ann Vasco, I work for Southern California Gas Company.

I have been employed for 12 years.

I am a customer service rep.

During my employment I have been monitored everyday in one form

or another. In the early part of of my employment I was told that

I would be monitored sometime during that week. This was done

in one of two ways: A lead person sitting next to you plugged into

your calls, or a lead person sitting in another room taping on a tape

recorder. Later with computers and sophisticated monitoring devices

great emphasis was put on using this equipment to check for

Quality, Quantity and safety. Recording of calls 24 hours a day as

well as keeping count of calls were but two ways of reaching this goal.

Monitoring can occur at anytime of any day. We were assured that only

10 consecutive calls would assured be taped

ensuring the customer service rep that tapes (favorable or unfavorable)

would not be created. Adding to this you are sitting eight to ten

hours per day at a computer terminal. One 30 min break in the morning and a

30 min break in the afternoon. You are given 1/2 to 1 hr lunch. You also have

a constant beep in your ear. You now have a basis for a stressful environment.

I was upgraded to the position of Lead for 1 1/2 years. My main

duties were monitoring of department personnel. During this period

I did most of the monitoring for two supervisors who shared the

position of Cust Ser Supervisor. As the Lead I recorded, scored

and reviewed the audit. It became apparent as time went on that

one of the supervisors was taking monitoring to an extreme. The employees were divided among both supervisors. One did her monitoring and had no real problems. The second supervisor reviewed every audit over and over again and 90% of the time scores were brought down. This caused friction in department. Employees asked to be assigned to other supervisor but were told no. Three employees left work due to stress, another bid out and two were fired. We were told that monitoring was a teaching tool but instead it became a tool of intimidation. I have included a copy of a seniority list with arrows indicating those most heavily monitored.

I now would like to share with you my own personal experience. Around October 1990 I had a misunderstanding with fellow employee - it was resolved outside of work - or so I thought. The employee decided to bring the issue to work - I tried to ignore it but the backbiting comments she was giving to supervisors as well as fellow co-workers could not be ignored. I received calls from the FBI I notified my supervisor who called a company special agent to check it out. Mr. Dale expressed his concern about this other employee possibly being apart of this. My ability to work was disrupted by this person to the point that in March or April 1990 I spoke to my supervisor I was told company could not get involved. After I followed all internal procedures to remedy situation I chose to use "Open Door Policy" within days I was demoted, told no more funds to pay my upgrade. I returned to the telephones. One week later I was monitored and given a low score. I protested

but signed the reviewed. 2 weeks later I^{was} called into supervisors office told my recording was going to be reviewed again. I asked if everyone's

review being gone over. She said "No, just you." I asked why just me - she became angry and said because I had 2 complaints about your work. She would not allow me to read the complaints or hear the complaints as they were ~~placed~~. I was only able to hear the original call.

Approx October 7 was given a monitor from late September. This time the tape appeared to have been doctored. I called the General Manager and said if this was the result of using his "Open Door Policy" He said for me to file a grievance. October 10 called into supervisor's office and told I have poor attendance poor production and overall poor performance and that this was going to affect my ~~score~~ being upgraded again in the future.

On or around October 20 I requested that a grievance be filed

On November 6 I was asked to report to map room. I asked why? ^{supervisor} she said to go over my tape. I told her I had a grievance pending. She said I know this meeting was arranged by your union rep. I had not been notified I had the union rep paged and ~~she~~ stated I did not want to do this. He urged me to give the company every opportunity to make things right. I did so against my better judgment. After we went over the tape I was given a higher score, but at the end the supervisor told me I had better watch it, because I was getting a reputation of being a trouble maker and this was going to follow me anywhere I went in the company.

Approx. around October 15, 1991
 I developed numbness and
 tingling on left side, I have
 had since about 1991.
 On July 5, 1992 I filed a workers
 compensation claim. I have qualified
 for state disability as well as
 I just this month qualified for
 social security, but my employer
 still refuses to release my long
 term disability benefits.

I hope that in these few minutes I
 have impressed upon you the
 importance of passing S. 984
 Employees need to be protected.
 Let us not create electronic
 sweatshops as we go into a new
 age of technology.



DIRECT MARKETING ASSOCIATION, INC.

1101 17th Street, N.W., Washington, D.C. 20036-4111 • (202) 317-1222 • Fax: (202) 295-2231

25 June 1993

RICHARD A. BARTON
 SENIOR VICE PRESIDENT, GENERAL COUNSEL

Dear Senator Simon:

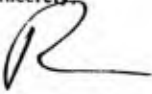
On behalf of the Direct Marketing Association (DMA), I submit this letter and attached DMA Fact Sheet and request that they be included in the record of the hearing held by the Subcommittee on June 22, 1993, regarding S. 984, the Proposed "Privacy for Consumers and Workers Act."

As you may know, the DMA is a national trade association which represents more than 3,000 companies and organizations that use the telephone, mail and other electronic and print media to communicate directly with consumers. DMA membership reflects a wide variety of businesses that use inbound and outbound telephone calls as their primary means of contact with customers and perspective customers for the advertisement and sale of goods and services. In addition, DMA members include or provide telephone services for many of the charitable, religious, educational, and political organizations that use the telephone for fund-raising, membership and other non-profit support activities.

DMA members who use the telephone for these purposes share a desire and obligation to maintain high standards of customer service and compliance with consumer protection requirements. Telephone service monitoring is essential for achieving these goals, but would prove unavailing if restricted as proposed in S. 984.

We will continue to work with the Subcommittee and its staff in an effort to produce a revised bill which addresses abusive monitoring practices without placing unjustified restrictions on the ability of DMA members to perform necessary telephone service monitoring.

Sincerely,



Richard A. Barton

RAB:jwb
Enclosures

**DMA Fact Sheet Concerning
Telephone Service Monitoring and S.984
("Privacy for Consumers and Workers Act")**

TSR Monitoring Benefits Customers and Protects Consumers

Businesses and nonprofit groups that primarily use the telephone to advertise and sell goods and services, or to raise support for charitable and political causes, monitor their telephone service representatives ("TSRs") as an essential part of their effort to provide quality customer service and comply with relevant consumer protection laws and regulations.

TSR monitoring allows these employers to determine how well their employees are communicating with current or prospective customers, whether they are adequately responding to customer needs, concerns or questions, and what, if any, problems are occurring that may be remedied through discussion with the employees. Moreover, in light of new laws and regulations that prohibit deceptive telemarketing practices and certain kinds of unsolicited telephone calls, TSR monitoring is an indispensable means for employers to promote and comply with a variety of consumer protection requirements.

TSR Monitoring Benefits Employees As Well As Employers

Proper training, supervision and evaluation of employees whose work consists primarily of handling inbound or outbound telephone calls on behalf of their employer requires periodic monitoring of such telephone calls by the employer. New TSRs receive helpful reviews and coaching in post-monitoring discussions with supervisors, and benefit from monitoring calls handled by their more experienced colleagues. In addition, veteran TSRs who are chosen to handle new, multiple, or more complex projects appreciate monitoring feedback, and monitoring helps maintain the quality of scripts and other TSR resources.

Monitoring helps employers make fair job performance evaluations that acknowledge the quality of a TSR's development and efforts, as well the quantity of the TSR's sales, calls or other "bottom line" figures. Such monitoring not only helps the employer to make decisions regarding training and assignments, but provides the TSR with better opportunities to obtain a raise, bonus or promotion.

TSR Monitoring Does Not Violate An Employee's Personal Privacy

The personal privacy interests of TSRs should be protected by ensuring that all employees have access to unmonitored telephones for the purpose of making and receiving personal calls. Because TSR monitoring is limited to telephone calls which are conducted by the employee acting on behalf of the employer and within the scope of performance of the employee's job responsibilities, such monitoring need not raise personal privacy concerns for employees...

TSR Monitoring Should Be "Unannounced" to Achieve Its Objectives

To a large extent, the beneficial purposes of TSR monitoring will be achieved only if the monitoring is performed without notice to the employee that it is occurring, since this is the only way to ensure that the monitoring obtains a representative sampling of the employee's usual performance, rather than one that is affected by knowledge of the monitoring.

Although some TSRs apparently find it stressful to be subject to "unannounced" monitoring, others prefer not to know when they are being monitored for fear that their performance will not be as good as usual due to nervousness brought on by knowing that monitoring is occurring.

In any event, all employers should fully explain their telephone monitoring practices to employees and prospective employees before any monitoring occurs, so that the employees will understand how and why the monitoring is conducted. Moreover, monitored employees should have a right of access to any information which the employer obtains through monitoring and uses to make decisions affecting them.

Why DMA Opposes S.984 As Introduced

1. The bill's "one size fits all" approach fails to distinguish among different types of "electronic monitoring" in terms of their purposes, benefits and susceptibility to abuse. It puts "telephone service observation" under the same restrictions as other distinct forms of "electronic monitoring," without evidence of comparable abuse and without understanding how the restrictions would deny the benefits of TSR monitoring to customers, employees and consumers.

2. The bill assumes that all forms of "electronic monitoring" are oppressive and violate employees' personal privacy, despite the fact that TSR monitoring only applies to calls which are handled by employees acting on behalf of their employer and in the scope of the performance of their job responsibilities, rather than on their own personal behalf.

3. The bill would bar or restrict TSR monitoring based solely on how long an employee has worked for an employer. Banning monitoring of employees who have worked for their employer for more than five years, imposing a 2-hour per week restriction on monitoring of all employees who have worked for the employer for more than sixty days but less than five years, and allowing unrestricted monitoring of employees who have worked for their employer for less than sixty working days, are wholly arbitrary policies because the length of employment with the employer does not reliably determine the quality of the employee's job performance.

4. Through enactment of the Telephone Consumer Protection Act of 1991 and its anticipated passage of the proposed "Telemarketing and Consumer Fraud and Abuse Prevention Act" (S.568/H.R.868) sometime this year, Congress is serving notice to TSRs that their telephone conduct must conform to certain standards of federal law. The only effective technique for ensuring full compliance with such laws and their implementing regulations is TSR monitoring.

The bill's "consumer protection compliance" exemption permits TSR monitoring "only to the extent necessary to ensure an employee provides the notices required" by various consumer protection laws and regulations. This standard is not adequate to ensure compliance with requirements imposed by federal and State laws because many of the requirements of such laws (e.g., those prohibiting deceptive telemarketing practices) do not involve giving required notices.

[Whereupon, at 11:00 a.m., the subcommittee was adjourned.]

O