TELEPHONE MONITORING PRACTICES BY FEDERAL AGENCIES

HEARINGS

BEFORE A

SUBCOMMITTEE OF THE COMMITTEE ON GOVERNMENT OPERATIONS, HOUSE OF REPRESENTATIVES

NINETY-THIRD CONGRESS

SECOND SESSION

JUNE 11 AND 13, 1974

Printed for the use of the Committee on Government Operations

U.S. GOVERNMENT PRINTING OFFICE
37-871 O WASHINGTON : 1974

For sale by the Superintendent of Documents, U.S. Government Printing Office
Washington, D.C. 20402 - Price $2.70

CONTENTS

TELEPHONE MONITORING PRACTICES BY FEDERAL AGENCIES

TUESDAY, JUNE 11, 1974

HOUSE OF REPRESENTATIVES,
FOREIGN OPERATIONS AND
GOVERNMENT INFORMATION SUBCOMMITTEE
OF THE COMMITTEE ON GOVERNMENT OPERATIONS,
Washington, D.C.

The subcommittee met, pursuant to notice, at 10 a.m., in room 2203, Rayburn House Office Building, Hon. William S. Moorhead (chairman of the subcommittee) presiding.

Present: Representatives William S. Moorhead, Bill Alexander, John N. Erlenborn, and Gilbert Gude.

Also present: William G. Phillips, staff director; Norman G. Cornish, deputy staff director; L. James Kronfield, counsel; and Stephen M. Daniels, minority professional staff, Committee on Government Operations.

Mr. MOORHEAD. The Subcommittee on Foreign Operations and Government Information will be in order.

Today's and Thursday's public hearings by the Foreign Operations and Government Information Subcommittee of the House Committee on Government Operations are part of a longstanding and continuing investigation by Congress into the problem of invasion of privacy.

At these particular sessions, we are focusing on the use of telephone monitoring and surveillance devices by the Federal Government, especially as they affect the people of the United States.

This subcommittee has long been concerned with individual privacy. In the early 1960's, it pioneered inquiries looking into the use of so-called lie-detector machines, which it found did not distinguish between truth and falsity at all. At that time, it also raised serious questions over telephone monitoring by Government agencies.

Since then, it has conducted in-depth investigations into the use of advanced information technology by Federal agencies through computers and other systems, and their implications on the possible invasion of privacy of American citizens. As a matter of fact, the subcommittee is currently writing landmark legislation to guarantee the right of every American to know what files and records our Government keeps on him and his family, and the right to examine those documents. Similarly, he should know what our Government has done, in terms of making that information available to others, and who those others are.

Subcommittee members also are fighting the establishment of any national data center which could put into the hands of Government officials complete dossiers on individual law-abiding Americans.

The Senate Watergate hearings, which disclosed the brief existence of a domestic security intelligence system and "political enemies" lists, have strengthened the determination of Congress to do two things:

First, every Government practice which has invasion of privacy implications must be thoroughly examined by Congress and put to the test of fire. "Big Brother" systems must be halted now before they grow from monkeylike creatures into gorillas.

Second, Congress—in every way that it can—must take action through investigation and passing new laws to implement the full letter and spirit of the Constitution in the protection of the right of privacy.

This does not mean that we want to coddle criminals, spies, and other wrongdoers. But even they should be brought to justice within the Constitution and not outside of it.

The subcommittee shares with a number of other committees in the House and Senate a deep concern with the reported excesses of warrantless wiretapping and electronic surveillance by law-enforcement and intelligence-gathering agencies.

These hearings, however, are not aimed primarily at the consideration of third-party interception of telephone conversations, or so-called wiretapping.

This subcommittee will consider mainly the magnitude and propriety of the monitoring of the day-to-day exchange of information among Government agencies and between those agencies and the public.

We firmly believe that when a citizen contacts a Federal agency by telephone, that citizen should know whether his call is being monitored or recorded, and if so, why. The spirit, if not the letter, of one of the greatest documents ever written—the Bill of Rights—requires no less.

Do you have any comments, Mr. Alexander?

Mr. ALEXANDER. Thank you, Mr. Chairman.

I continue to be concerned with the increasing preoccupation of Government with spying on our citizens. This is an alarming tendency of Government. There is almost a propensity to forget its purpose, to forget that it is the servant of our people and for it to assume the role of an authoritarian master.

Mr. Chairman, I, too, look forward to these hearings.

Mr. MOORHEAD. Thank you, Mr. Alexander.

The subcommittee would now like to hear from Mr. Glenn E. Watts, secretary-treasurer, Communications Workers of America.

Mr. Watts.

If you would like to have our good friend, Mr. Morgan, join you at the table, we will be pleased to have him.

Would you gentlemen please rise so I can administer the oath?

Do you swear to tell the truth, the whole truth and nothing but the truth, so help you God?

Mr. WATTS. I do.

Mr. MORGAN. I do.

STATEMENT OF GLENN E. WATTS, SECRETARY-TREASURER, COMMUNICATIONS WORKERS OF AMERICA; ACCOMPANIED BY JOHN MORGAN

Mr. WATTS. Thank you very much, sir.

I am Glenn E. Watts, the secretary-treasurer of the Communications Workers of America, a labor union representing more than 575,000 American men and women, most of them employed in the telephone industry.

At your suggestion, a very lengthy statement that we have prepared has been provided to you, and I will summarize it this morning.

Mr. MOORHEAD. I have read the statement. It is an excellent one; and without objection, the full statement, together with the appendixes, will be made a part of the record.

[Mr. Watt's prepared statement follows:]

PREPARED STATEMENT OF GLENN E. WATTS, SECRETARY-TREASURER, COMMUNICATIONS WORKERS OF AMERICA

Mr. Chairman, if we all are not to succumb to the evils of a totalitarian superstate --- or "snooperstate"--- the privacy of the ordinary citizen must be made to follow the intent of the writers of the Bill of Rights.

For the record, I am Glenn E. Watts, Secretary-Treasurer of the Communications Workers of America, a labor union representing more than 575,000 American men and women, most of them employed in the telephone industry. On behalf of President Joseph A. Beirne and the CWA Executive Board, we wish to thank you for asking the Union's views on the important subject of telephone monitoring.

This Subcommittee, of the Committee on Government Operations, is studying the abuses, actual and potential, of telephone monitoring and eavesdropping, by which a large portion of a citizen's personal life may be jeopardized. We hope that the Congress soon will write very stringent legislation to stamp out the abuses which we all know exist, and of which some of us have learned in addition. Your Committee's charter, Mr. Chairman, includes "... studying the operation of Government activities at all levels with a view to determining its economy and efficiency."

The Federal Government for many years has been the largest single user of telephone and related telecommunications services, spending

several billion dollars each year. Some of that money and the related work effort, we are learning each day, goes into the practices of wiretapping and eavesdropping. These practices are costly. We cannot see how th se practices can lead to any kind of efficiency in Government.

However, it is not necessary to spend large sums of money for the equipment necessary to eavesdrop. Some of the most common items are tariffed by the telephone companies. For example, the transmitter cutoff switch, by which a person may listen in on an extension telephone without detection, is available at around 25¢ a month. The "push-to-talk" telephone handset, available at a nominal monthly rental, allows listening without detection. When a person wants to talk, he or she depresses a button in the handle of the set.

These two items, Mr. Chairman, were designed to aid in providing telephone service in normally noisy areas, such as automobile body shops; the original purposes were innocent, morally neutral. Even these simple devices have been subject to abuse.

And while on the subject of low-budget invasions of privacy, I will display the "telephone pickup," available at the Radio Shack stores for $1.19 plus sales tax. A member of the CWA staff recently purchased this device, which uses a suction cup to attach to a telephone handset for surreptitious recording. We note that the Federal Communications Commission tariff governing the use of recording devices calls for a "beep" tone. This $1.19 device does not have any warning as to the restrictions set by the FCC pursuant to Federal law.

The Communications Workers of America has for years been concerned

about wiretapping and eavesdropping practices, because of the abuses. CWA orginally became interested and involved in the classical labor-management relations arena, because the union's members were being subjected to discipline on the basis of "service observing" or "monitoring" by telephone company management personnel. It is not the union's intention to turn this hearing into a labor-management grievance session, Mr. Chairman. However, in the course of following the employee monitoring, CWA has become concerned over the privacy problems of the individual citizen who has no connection with a telephone company other than that of subscriber-user.

Currently a highly disturbing motion picture, "The Conversation," is being shown at theaters in this area. The film, produced by Francis Ford Coppola, depicts some of the many actual techniques of destroying one's privacy. We understand that Harold K. Lipset of San Francisco gave the technical advice to producer Coppola. We recommend a review of his testimony, given February 18, 1965, before the Senate Judiciary Committee's Subcommittee on Administrative Practice and Procedure. Mr. Lipset came to Washington to demonstrate many of the devices and techniques that he and other private detectives use to gather information for their clients.

Mr. Chairman, you did the Nation a great service in late October 1972, when you "blew the cover" on the White House's "Big Brother" study. This was the study assembled for the President's Domestic Council, headed at that time by the well-known John D. Ehrlichman. Unfortunately, at that time the 1972 Presidential election was at its climax, with the result that the public may not have had sufficient information about

the meaning of that Domestic Council study. From what we have seen of the study, every bit of the technology necessary to provide for the massive invasion of privacy existed at that time. The key consideration in putting the plan into effect appears to have been whether to get the money to start operations. The text of the report gave some lip service <u>at best</u> to the ethical and moral consequences of that program.

Your Subcommittee's hearings in 1973 on information technology adequately exposed the ramifications of that "Big Brother" plan.

The machinery of our Federal Government either in the Legislative or Executive Branches is not adequate to cope with the problems of privacy. The CWA staff has found scanty unified jurisdictions in either branch.

For example, these House Committees would or could have jurisdiction over privacy matters:

Government Operations, for agency monitoring/eavesdropping/snooping.

Commerce, for its normal oversight of telecommunications.

Judiciary, for Constitutional reasons.

Post Office and Civil Service, for "mail cover."

Ways and Means, for abuse of the Social Security number as a kind of "universal standard identifier."

Armed Services, for surveillance on civilians.

Internal Security, for building dossiers.

Banking and Currency, for snooping into bank accounts.

Science and Astronautics, for scientific development.

Appropriations, for whatever oversight it exerts over CIA and other intelligence entities.

Mr. Chairman, the Senate Committees which correspond to those of the House named above would have the same jurisdictions.

In the Executive Branch, many Departments and Agencies exercise power over areas in which privacy questions must emerge. We would include the Departments of Justice, Defense, Health, Education and Welfare, Commerce and Treasury. We also would include the Federal Communications Commission, the Office of Telecommunications Policy, the Central Intelligence Agency, the National Security Agency, and the now-defunct Office of Science and Technology.

The CWA Convention of 1973, held at Miami Beach, Florida, addressed the jurisdictional chaos in matters of privacy in its Resolution 35A-73-8, entitled "The Abuse of Technology: Freedom's Enemy, Corruption's Ally." I include a copy of that resolution and a CWA staff paper on that topic as Appendix A.

The 1973 Convention resolution noted some of the abuses of our communications and related technology, called for a comprehensive review of those matters, and asked the Congress to establish standing committees on individual privacy in both Houses. If standing committees are not established, we believe the Committee on Government Operations of both House and Senate would be the logical focus for privacy oversight of the entire Executive Branch.

These hearings are to discuss the subject of "telephone monitoring," a term that has a specific meaning. The ordinary telephone can be "tapped" or "monitored," in various ways. An ordinary telephone also can become a "bug," as that term is now understood. The Coppola film mentioned earlier, "The Conversation," included a demonstration of one way an ordinary telephone, while not in use and lying in its cradle, becomes a "bug." Mr. Lipset should be able to demonstrate that technique. A device of that sort to allow a

hung up telephone to become a "bug" was described by Ronald Kessler, staff writer for the Washington Post, in a story in September 1971. We will return to the subject further along.

While discussing monitoring, we should look at the role of the nation's telephone industry. The Bell Telephone Laboratories, jointly owned by AT&T and Western Electric Co., have given us much of the pioneering work in communications technology, including lasers, communications satellites, microwave, and waveguide. Other major developers of the technology are Kellogg and ITT's Federal Laboratories. From the trade journal, Telephony, and other sources, we note many smaller firms develop, produce, and market equipment that tends to be capable of surreptitious use --- or misuse. In most instances, the telephone companies must tariff their service offerings, including equipment. Non-operating companies do not face this requirement.

At the time of the preparation of the "Big Brother" study, the President's science adviser was Dr. Edward E. David, who came to the White House from Bell Telephone Laboratories. Dr. David signed the White House response of December 29, 1972, to Chairman Moorhead's inquiries on the "Big Brother" study. Dr. David's letter concluded thus: "Furthermore, I know of no tests now under way or even contemplated which would in any way infringe on either the rights or privacy of the citizens of this country. Any such possibility is abhorrent to this Administration."

While we hope this is the case, every possible suggestion in the "Big Brother" study is so vulnerable to abuse as to frighten one even to contemplate.

The telephone industry is a key to any inquiry into the use of the telephone for monitoring. Appendix B is a CWA staff paper, with attachments, giving a few reasons why the Bell System should be questioned. The CWA staff paper briefly reviews the following matters:

a. Early in 1970, the telephone of an employee of the Federal Communications Commission who was suspected of leaking FCC agenda matters was tapped for about 5 weeks. The local AT&T company, Chesapeake & Potomac Telephone Company, assigned management personnel to do the necessary wiring after hours, without written work orders. The Department of Justice, after some Congressional hearings, stated that the 1970 wiretap incident was illegal.

A more complete description of this matter is given in Appendix C, which is a CWA staff paper headed "Monitoring of FCC Employees." As a result of the wholly illegal manner of tapping that employee's telephone lines, CWA President Beirne directed each of the Union's District Vice Presidents to make contact with responsible Bell System company officials to determine individual company policy in parallel circumstances. Included is a copy of the CWA President's letter to Chairman Harley Staggers of the Committee on Interstate and Foreign Commerce, who conducted some rigorous hearings in 1972 on the 1970 incident.

b. In his testimony of June 25, 1973, before the Senate Watergate Committee, John W. Dean III, the ex-White House Counsel, said that a 28-year ex-Bell System employee who went to the White

House staff utilized his associations at C&P Telephone Company to learn the "pair numbers" of the telephone lines syndicated columnist Joseph Kraft, in order to install wiretaps. Dean identified the ex-Bell System employee as John S. Davies, who had been associated with three Nixon campaigns as a communications expert-coordinator. In the wake of Dean's testimony, C&P said company policy bars release of "pair numbers" except on court order or a written request from the Attorney General or FBI Director, who must cite "national security" grounds. In addition to the Washington Post story of June 26, 1973, we refer to pp. 919-922, Part 3, of the printed record of the Watergate hearings. Dean's testimony was at the point exploring the White House concern about information leaks. The Post story is in Appendix B.

c. The AT&T Management Report of August 9, 1973, in Appendix C, outlines the policies and procedures on the method for Bell System employees to treat wiretaps they discover while at work. The CWA position is that a Union-represented craftsman could be placed in violation of criminal law. Under the subheading "Discovery of Wiretaps," the AT&T bulletin gives the instructions as to checking for wiretaps. CWA sees a "Catch-22" type situation facing the employee who discovers the existence of a tap on a line. If an illegal wiretap is found, removal is not accomplished forthwith. Therefore, the damage being done by the illegal wiretap continues for an indeterminate period, while various people are "going through channels."

d. Bell System employs "remote observing" systems, by which a person with a push-button telephone who knows the proper access codes may listen in on conversations without detection. CWA knows of at least two "remote observing" or "REMOBS" systems, marketed through normal telephone industry supply channels. We will discuss these further along.

Mr. Chairman, four weeks ago, the United States Supreme Court handed down an opinion which voided the convictions of a number of accused narcotics sellers. The Court unanimously ruled that the convictions must be voided because the Department of Justice had committed serious error in the wiretaps leading to the prosecution and conviction of the ones accused. (Appendix D)

We are alarmed for several reasons. First, the Department of Justice should have known better, because it is specifically charged with enforcement of the wiretap provisions of the Omnibus Safe Streets and Crime Control Act of 1968. Second, the errors have lead to the release of charges against persons who very probably were and are engaged in the drug traffic. Now they will be back on the streets, ready to resume business. Third, the resort to illegal wiretaps has been somehow relied on by the Department of Justice as a kind of procedural shortcut to evidence-gathering.

Only 10 days ago, the New York Times reported that the New York City police department had acknowledged using illegal wiretaps in 33 narcotics cases between 1969 and 1971. The Times story was based on intra-departmental testimony in disciplinary cases of high-ranking

police officers. Currently the police department is investigating the 33 cases, in light of the tainted evidence. The Times story also is in Appendix D.

The Department of Justice has come under sharp criticism to the degree that public confidence is shaken, because of events of the last few years, which we would term ominous. In July 1973, two FBI agents were discoverd in the telephone wireroom of the Federal Courthouse in Gainesville, Florida. In the agents' possession was a briefcase containing various items of electronic gear. The wireroom was reported to be adjacent to the room being used by lawyers defending 7 anti-war Vietnam veterans who were being prosecuted at that time. The FBI agents are reported to have explained that they were checking out FBI telephone lines, even though the nearest FBI office is 60 miles away, in Jacksonville.

Because there is some question as to whether aid is extended for government eavesdropping efforts by the telephone companies, the companies should be queried directly. Appendix E, "FBI and Other Snoopers in the Wireroom and Elsewhere," is a CWA staff paper on the Gainesville incident and others. Included with that paper are news stories from 1973 and 1974 indicating FBI interest in the use of communications technology.

Mr. Chairman, the Omnibus Crime Control and Safe Streets Act of 1968 included a mandate, in Section 804, to establish the "National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance." The Commission has begun its work with a final report due in a year. On behalf of CWA, I urge your Subcommittee to provide information on the practice of wiretapping and other invasions of privacy to the Commission, so that it might make sound recommendations for corrective legislation. The 15 members of the Wiretap Law Review Commission appear to include proponents and opponents of the practice.

On January 30, 1974, Robert D. Lilley, President of American Telephone and Telegraph Company gave a speech at the National Press Club dealing with the problems and challenges of the Bell System, which had produced a successful telecommunications network. At the end of his speech, Mr. Lilley addressed a topic of overriding interest to the Nation's press: the company policy of providing toll telephone records of newspaper offices and reporters to Federal investigators, who were trying to find the sources of news "leaks." Appendix F consists of photocopies of the final 2 pages of Mr. Lilley's prepared Press Club speech text. However, several points must be made in comments to the remarks:

1. Although company policy is expressed as protective of privacy of users, Bell and other companies let customers use monitoring equipment. The customers can include government, hotels, department stores, airlines, and other service businesses.

2. The speaker cited toll records as the only ones in which specific information as to calling and called numbers is available and retrievable. However, that passage in Mr. Lilley's speech ingnores the existence of the "pen register" and other devices, by which the outgoing calls --- of Jack Anderson, the New York Times, of anyone --- can be recorded. We refer to the Alston Subscriber Dial Service Measuring System, Models 370/389, which includes a visual display and tape recording, and the Tel-Tone N-240 system. Mr. Chairman, the number being called appears on the visual display, from which it can be read. The tape recorder will record the dial pulses or tones being actuated by the user. Retrieval of the data necessary to determine whom the user is calling --- either on a <u>local</u> or <u>toll call</u> basis--- is thus routine. Further on, we will go into more detail.

3. The use of the adjectives, in the Lilley speech, "appropriate" and "lawful" needs to be questioned in the light of the current scandals in government. Congressional proceedings in the last year have certainly established that the FBI, Central Intelligence Agency, the National Security Agency, the Secret Service, Internal Revenue Service, and others have been or could be used for political espionage purposes wholly unrelated to national security. Mr. Lilley was saying that the Bell System companies were placed in the middle of a bad situation. The management personnel would be normally responding to what they had perceived as legitimate requests for help from official Government sources. Nevertheless, there is enough evidence in the record now to show that Government agencies have engaged in various "Big Brother" activities. Law and regulations should be written, to protect all telephone people from being placed in the category of having been misused, by apparent proper authority.

4. Mr. Lilley says the privacy problems will have to be decided eventually by Congress. We fully agree, and expect the Bell System will join with CWA in urging passage of the tightest possible legislation to cover the privacy problem areas. We believe the potential for abuse is recognized by the Bell System.

Mr. Chairman, earlier we cited the use of the telephone lying in its cradle as an open microphone for eavesdropping. We also direct the Subcommittee's attention to the November 1970 discovery by Maryland Governor Marvin Mandel that the civil defense "hot line" telephone installed within his personal office had been incorrectly wired, so that all conversations taking place within his office could be overheard at a remote location. Please see Appendix G.

The American Telephone & Telegraph Company disclosed that at least 6 Governors' "hot line" telephones were so wired. This special telephone system was installed to give instant communication to the Governors of the 50 States for national disaster and emergency use. The company announcement was that the "hot line" telephones were connected to North American Air Defense Command transmission points at Cheyenne Mountain, Colorado, at Denton, Texas, and at a classified location near Washington, D.C.

The explanations given to the Governors of Maryland, Delaware, Pennsylvania, Arkansas, Utah, and Illinois were to the effect that the wiring irregulartities were unintentional.

In our view, Mr. Chairman, a system was set in place to accomplish a socially useful goal, that is, alerting Governors of imminet disaster, in order that militias could be called into service. But we see a system capable of a good use also rendered capable of wanton abuse.

On September 24, 1971, the Washington Post printed a story headed "New Bug All Ears -- Snoops Through Hung-Up Phone," under the by-line of Ronald Kessler. We also include this story in Appendix G. Reporter Kessler described what he had seen and heard at a symposium in Washington sponsored by the Association of Federal Investigators. The device, termed a "breakthrough" in electronic eavesdropping, was able to "... be placed anywhere on a line leading to the phone to be tapped -- on telephone poles, in underground cable vaults, or in telephone company switching offices miles away. It picks up both telephone calls and conversations in the room where the phone is installed, even when the receiver is on the hook," Mr. Kessler reported. In this instance, the device would act as a wiretap and a "bug."

Possibly this could have been justified at that 1971 symposium on ground that it furthered economy and efficiency in Government.

The remote observing or "REMOBS" systems I cited have the potential for a frightening degree of abuse. Inasmuch as they are available, it is necessary for any citizen to ask whether any government agency has such equipment--- either on the basis of purchase, rental, lease, tariffed interconnection, informal borrowing, or other arrangement. We hope the Subcommittee can secure dispositive information. In Appendix H we include some technical data on the "REMOBS" system marketed by Tel-Tone Corporation, of Kirkland, Washington, as well as some information from a sales manual of the Alston Division of the Conrac Corporation, Duarte, California. We understand the Subcommittee has in its files a set of the technical specifications of the Alston system.

The Tel-Tone and Alston systems have comparable uses.

Mr. Chairman, the following paragraphs are taken directly from the technical information on the Tel-Tone Corporation's M-220 remote observing system:

"General Description. The M-220 Service Observing System provides a means of observing service on lines or trunks from a remote location. All that is required is a telephone equipped with a TOUCH TONE (AT&T Registered Trademark) dial. The system consists of an automatic answering unit and various switches to select the trunk to be observed. The service observing unit is accessed by dialing a regular telephone number. It is connected to the telephone lines to be observed. The service observing unit is accessed by dialing a regular telephone number. It is connected to the telephone lines to be observed in such a manner that you will monitor the conversation without being heard yourself.

"Accessing the System. Dial the telephone number assigned to the system you wish to access...

"Releasing from the Observed Line. When you no longer wish to observe a particular line you must dial the second digit of the Security Code (Reset Digit) to release the connection. You will then be able to observe the next incoming call."

The sales brochure for the Alston 370/389 Subscriber Dial Service Measuring System, whose chief purpose appears to be the qualitative and quantitative grading of customer dial service. The No. 370 component is a "call selector," which is "... an automatic unit designed to simultaneously monitor a number of trunks and to select the next trunk offering a new outgoing call.

Under the heading "Dialed Number Detection," the Alston brochure states: "After a trunk has been selected for observation, the number being dialed by the subscriber is detected and forwarded to the service monitor (or tape recorded) for display. The system will process dialed numbers coded in dial pulses, touch tone, or multi-frequency or combinations of the three."

The No. 389 component is the service monitor unit, which receives the information from the No. 370 call selector. The information which appears on a 16-digit display panel includes calling number and called number.

The Alston price sheets, brochure and technical books note that 50- and 10-trunk options are available.

Both Tel-Tone and Alston advertise regularly in the weekly trade journal of the telephone industry, "Telephony," and the annual issue

of "Telephony's Directory." We trust this Subcommittee will get information into the record on Government and private users of these systems, as well as any constraints on their use.

What is plain to us is that telephone technology has made many advances in the last 15 years. About a dozen years ago, a chief operator in a Bell System operating company had service-observing equipment installed in the bedroom of her home, in order to keep track of the operators in her traffic office. She ultimately caused dismissals of several operators, as a result of the conversations she heard. We of CWA do not know whether the chief operator was alone while listening in, or whether she used the gadgetry for the entertainment of her friends.

Some of those disciplinary actions were overturned on grounds the chief operator was unable to make positive visual identifications to accompany what she "knew" were the voices of the operators at work at the time. The chief operator's monitoring set was installed in the residence by management personnel, we found.

In November 1972, we at CWA were appalled to learn of the magnitude of the "Big Brother" study, more officially known as "Communications for Social Needs: Technological Opportunities." We paid especially close attention to your announcements of the plan, emanating from the President's Domestic Council and the Office of Science and Technology, because it showed that serious thought had been given to employment of telecommunications in a fashion subject to phenomenal abuse.

We were appalled by the very real possibilities that the systems could be used in spying, invasion of privacy, telephone bugging,

censorship, propaganda, electronic surveillance, and other practices most aptly termed totalitarian. It was the arrival of "1984," as novelist George Orwell envisioned it. We do not think the United States should have an electronic mail-handling system which can so easily provide a "Mail cover" for government snoopers. We do not believe every car, home, or rowboat should be required to have the "emergency" radio set which can be switched on from outside the premises. We have serious reservations about the "wired city" and "wired nation" concepts, by which the government could maintain better contact with the citizenry. And the possibility that educational facilities could be wired into a central bank of information causes me to question whether the plurality and diversity which have made the National so great would not be destroyed. While the term "local schools" can conjure up some unfortunate racial implications, it also denotes a most salutary lack of centralized control over educational content.

From what we have seen of the documents on the "Big Brother" study, the technological advances now exist. For example, the electronic mail-handling process would be a form of facsimile, on an automated basis between two computer centers. It would be a logical outgrowth of the "Mailgram" service, instituted in 1969 as a joint undertaking of the Post Office Department (now U.S. Postal Service) and Western Union Telegraph Co. CWA learned that subsequent to the startup of the "Mailgram" service, Western Union and the Department carried on a discussion of a new service called "Mailfax," using the present Western Union communications/computer system with some modifications. As we understood "Mailfax," the postal patron would purchase "Mailfax" blanks

at the Post Office, much like postage stamps. The sender of the letter would write the message on the purchased blank, and would place it in an envelope and then into the mailstream. In the Post Office, the letter would be taken automatically from the envelope, and sent by electronic facsimile means. What would happen to the "hard" copy of the letter at the sending Post Office is a large question to me. In the receiving Post Office, the reverse of the process would occur; the facsimile letter would go from receiving machine into an envelope and eventually to the mail carrier. Such mail matter --- which would be simply computer data "bits" --- would be simply retrievable from the computer system as a major advance in the "mail cover" technique, with the major difference being the ability for government agents to read the message going to an individual, not merely the return address of the sender.

The December 1972 issue of "Datamation" magazine notes the treatment of mail privacy in the Domestic Council study, but adds this thought, from its standpoint of expertise in the field: "It takes only rudimental technical knowledge, however, to realize that such a system could easily be programmed to detect, and print out, letters bearing particular names and addresses."

Mr. Chairman, the electronic mail handling process represents to us still another example of technology subject to grave abuse. We believe the United States should choose methods and techniques which appear cumbersome, if the alternative is to lessen the privacy of the individual. The temptation to abuse is too great to allow shortcuts.

Before departing from the subject of "mail cover," I would like to refer to Appendix I, which is a CWA staff paper prepared to summarize the subject, with the electronic techniques I cited above included. A Senate subcommittee has looked into a specialized form of "mail cover," this one on Congressional "franked" mail going to regulatory agencies. The Federal Communications Commission and the Federal Power Commission were among agencies found to divert Congressional mail. Several items on the issue are included with the Appendix.

Southern Bell Telephone & Telegraph Co., pursuant to Georgia State law, is required to identify the companies which are licensed to use service observing equipment. Each telephone directory carries the appropriate notation to this effect, offering a listing of the companies. CWA has secured such a listing, which is attached to the copy of the directory pages. We understand that about 72 private businesses, three non-Federal agencies, the United States Marine Corps and the Veterans Administration are licensed to use such equipment. The Internal Revenue Service is reported to have such equipment, but is not required to license or register it, according to an opinion of the Attorney General of Georgia.

A CWA staff study prepared in 1972, headed "Monitoring and Other Service Evaluations," gave several examples of the problems faced by employees of telephone companies, represented by the Union. Included are Western Electric sales catalog sheets showing models of desk calendar-inkpen sets in which microphones could be concealed, a letter from a Local President describing a dozen methods of monitoring, and the CWA News story of October 1963 telling how a closed-circuit TV camera had

been installed in a men's restroom to catch someone in the act of scrawling graffiti on the walls. (Appendix J)

Invasion of privacy using the telephone, aided and abetted by the spending of Federal Funds, has struck at CWA. In early 1972, a CWA member in San Mateo, California, was dismissed by Pacific Telephone & Telegraph Company and subsequently charged with a criminal offense on the basis of "evidence" gained through the "Voiceprint" technique. Your Subcommittee's interests are involved in "Voiceprint," Mr. Chairman, because substantial sums of Federal money have been spent by the Law Enforcement Assistance Administration, Department of Justice.

On the basis of a CWA analysis of the tables in the Government-financed study of "Voiceprint," we are forced to believe there was a sizeable degree of intellectual dishonesty in expounding the benefits of the "advance" in identification of persons accused of crimes. The CWA member in California was exonerated after criminal proceedings, but only after the court concluded the "Voiceprint" technique is burdened with questionable reliability. The CWA analysis, Appendix K, shows an error rate of up to 37% in various kinds of voice sample matching, as well as the details of the case.

The case of the CWA member, Stephen Chapter, is pertinent to these hearings because the telephone was one means of securing a voice sample, on which the tests were based. The other voice sample was secured direct from Mr. Chapter, recorded on a low-fidelity, inexpensive tape recorder.

Mr. Chairman, the news on telephone wiretapping is not all bad. And I wish to state in public that Southern Bell Telephone & Telegraph Co., a unit of the Bell System, handled the situation properly and

promptly. The Company did not cooperate in any fashion in installing the wiretap, which was discoverd at Wallace, S.C., in February 1973 in the motel room being used by organizers of the Textile Workers Union, another AFL-CIO affiliate. As you will recall, that Union has for many years been trying to organize the employees of J. P. Stevens Co. Because the Union organizers' telephone went dead, the Southern Bell repair service sent a man to restore service. The repairman found the wiretap device on the motel room telephone and went through reporting channels, which ended with the FBI, called into the case by both Union and Southern Bell. After 8 months, during which the Textile Workers continued to prod the FBI for action, indictments were returned against 2 J. P. Stevens Co. management employees on Federal wiretapping charges. The company officials were subsequently convicted. We believe the Subcommittee has an interest in this matter because of the 8-month period necessary to take the matter before the Federal Grand Jury. The FBI should be pressed to answer as to the degree of political pressure exerted on it by the Stevens Co. and members of the State's Congressional Delegation who have espoused the Stevens cause. (Appendix L)

Telecommunications technology has provided a means of cracking the traditional doctor-patient relationship. The existence of large computerized data banks with detailed information on the health of millions of Americans was established in 1973 hearings before a Subcommittee of the Senate Banking and Currency Committee. Most notable of the health data banks is Medical Information Bureau, of Stamford, Connecticut, which serves 760 insurance companies. Information is fed in and retrieved over telephone lines, with the Social Security number being the "identifier."

Among recent moves in the centralized health data field is the marketing of various kinds of medical identification cards. We have samples here of the "Emergency MD Card," and the "Hotline Emergency Medical Card." Each of these cards contains a microfilm of a medical data form executed and signed by the individual on his or her conditions. The buyers of these are requied to furnish their Social Security numbers. We are much concerned that the data on these forms also will enter computer banks for the insurance companies, since health-hospitalization insurance policy numbers are secured, in addition to the Social Security account number. CWA believes some safeguards are essential. The "Medic-Alert" bracelets and medallions are far more likely to be used in emergencies, since medical personnel are trained to look for these items. For more detail, we refer to Appendix M, a CWA staff paper headed, "Medical Information: How Private."

The July 1973 report, "Records, Computers, and the Rights of Citizens issued by the Department of Health, Education and Welfare, provides a mass of valuable information on the extent of information-gathering on individual citizens, who are caught in the web of technology. One chief problem highlighted in the 372-page HEW report (which to me does not appear exhaustive) is the ever-widening use of the Social Security number as a kind of "universal standard identifier," for the convenience of business and credit firms, telephone companies, the armed services, State motor vehicle departments and many other organizations. Appendix N consists of 2 CWA staff papers on the HEW computer study and data banks problems.

The HEW computer study makes numerous recommendations for legislative

and administrative regulation safeguards. These recommendations, at pp. 136 to 143, are reasonable; CWA would support them without hesitation.

We note the recent interest of the Subcommittee in hearings on legislation to amend the Freedom of Information Act, to guarantee the privacy of individuals and to provide access to records concerning themselves maintained by Federal agencies. We support these moves.

We have examined the proposals made by the American Civil Liberties Union's Project on Privacy and Data Collection. CWA would certainly support the concepts of the ACLU proposals. However, we would oppose one point, the matter of conviction records. ACLU would urge that conviction records be destroyed after the person has served his or her sentence. On the assumption that the conviction is a proper one, we must brand such a proposal at best unrealistic. An employer must be allowed to learn whether a prospective employee has been incarcerated; otherwise, in the most extreme case, we might see a person who had served time for embezzlement somehow handling cash of another business house. ACLU appears to have taken too hard a line on the information available to an employer.

In March, 1974, there were reports that some automobile dealers in Baltimore were electronically eavesdropping on the private conversations of customers in sales office cubicles. Our understanding of the events is that the eavesdropping --- usually of man and wife left alone by the salesman --- is accomplished by an adaptation of the intercommunication system. We at CWA have been attempting to follow the matter, since the basic right of private conversation is involved, and since the eavesdropping may in some cases be by a flagrant abuse of communications technology.

Appendix O consists of statements from a CWA Local President and a Vice President on the "service Monitoring" practices in their Bell System companies. In order to protect these Local officers, we have had names and places expunged.

On March 25, 1974, the Maryland House of Delegates Committee on the Judiciary held a hearing on a bill to restrict telephone monitoring in one single aspect--- to ban the making of any form of records of monitored conversations. We supported the legislation, although we believe that new Federal law is required. As Appendix P, we include the recent testimony of CWA Executive Vice President Louis B. Knecht, given at Annapolis on the Maryland legislation, House Bill 1678, which did not pass in the recent session.

Mr. Chairman, your letter inviting CWA to give testimony to the Subcommittee set out the "chartered areas" for this inquiry. I hope what I have given here today will be helpful. This has gone well beyond what you asked, and for that I must thank you for your forbearance. The sole reason for the mass of detail is that the subject of invasion of privacy is one of incredible complexity.

Two centuries ago, before our forebears took arms, invasion of privacy normally meant entry into private homes by British soldiers and mercenaries. The framers of the Constitution thought that they had quite adequately disposed of the issues of privacy. And in their defense, I must agree that they did accomplish that aim. But the onrush of technology has led to a deterioration of understanding of the spirit in which the safeguards of the Constitution were written into our most sacred body of law. I believe your Subcommittee's work is helpful in leading the Congress to a rebirth of the spirit. Thank you, Mr. Chairman.

APPENDIX A

CWA 1973 Convention Resolution

The June 1973 CWA Convention adopted Resolution 35A-73-8, "The Abuse of Technology: Freedom's Enemy, Corruption's Ally," in response to the shocking revelations of the Watergate investigations and hearings, as well as the development of equipment and techniques to allow major invasions of privacy.

The resolution recited provisions of the Declaration of Independence and Constitution which had been considered the guarantees against invasions of privacy, and noted the abuses which have arisen in recent years by virtue of technology.

The resolution called for a comprehensive review of the technology subject to abuse, and asked the Congress to establish standing committees on individual privacy, to help "...move the Nation away from the invitation to the massive corruption of our liberties."

* * * * *

The Moorhead Subcommittee (Foreign Operations and Government Information, of the Committee on Government Operations) has held hearings throughout 1973 on privacy questions and the manner by which Government agencies have disregarded the intent of the Constitution.

The Subcommittee Chairman, Representative William S. Moorhead, in November 1972 "blew the cover" on the John Ehrlichman-inspired plan to establish a domestic spy and propaganda system, as outlined by Dr. Edward David, then head of the Office of Science and Technology, an agency no longer existing. David came to OST in 1970 from Bell Labs.

As a result of the Moorhead revelation, OST released a "final" version of the study, which includes several aspects subject to abuse: the electronic mail handling process, together with the FBI's use of postal service data and facsimile lines for processing of criminal case information. The danger is the possibility of a "mail cover" direct into FBI by the proper access to the computer processing the mail by electronic means.

37-871 O - 74 - 3

RESOLUTION 35A-73-8

"THE ABUSE OF TECHNOLOGY":
FREEDOM'S ENEMY, CORRUPTION'S ALLY

The question of privacy of the individual has reached its most serious point since the pre-Revolutionary period, when British military men were able to invade and search homes.

The Declaration of Independence cited ". . . a long train of abuses . . ." and "Despotism" suffered by the Colonies at the hands of George III. The Fourth Amendment to the Constitution guarantees that:

> "The right of the people to be secure in their persons, house, papers, and effects, against unreasonable searches and seizures, shall not be violated . . ."

The noble intentions of the founders of the Nation appear to have been vitiated in recent years, not by a King of England, but by native Americans who seek such a degree of leeway as to invade by technological means.

The ever-present wish to pry into others' personal business has been aided by the abuse of technology. Literally and figuratively, "bugs" have been eating their way into the body politic.

Electronic and optical devices, available in the mid-1970s, are capable of allowing snoopers to overhear telephone conversations, to operate "mail covers," to retrieve bank account and medical history information, and to have two-way television in the home. Using certain telephone equipment and the proper codes, an eavesdropper can dial a citizen's number and listen in at wish. CWA files contain the details of other abuses of communications technology, including the illegal tap of a telephone used by an employee of the Federal Communications Commission, a closed-circuit TV camera in a restroom of a telephone building, and a chief operator's monitoring console in the bedroom of her home. A device on the market allows a telephone set not in use to become an "open microphone" for eavesdropping.

Detection of these devices is difficult, usually impossible. Thus the existence of such devices and practices is an open invitation to corruption. The citizen appears to have little protection of law.

In an awareness of the dangers, CWA gave testimony in 1965 and 1967, when a Senate Subcommittee held hearings on "Right of Privacy" legislation. The CWA position has historically been outright opposition to wiretapping and other forms of eavesdropping, except when a clearly defined and genuine national security issue is involved.

Numerous major events since 1969 have shown that "national security" has been used to justify wiretapping and attempts to corrupt the American political process. Felonies have been procured and condoned by high government officials, with "national security" now used as the reason. The situation now has taken on the mark of a "secret snooperstate."

Presently, no single Committee of Congress and no single Executive Branch Department or Agency has entire jurisdiction over the questions of individual privacy. The responsibilities are fragmented.

The time has come, CWA believes, for a comprehensive review of the state of communications technology which can be abused in the area of privacy. The time has come, CWA believes, for a complete review of the statutory provisions against such abuses.

BE IT RESOLVED: That this Convention call upon the Congress to establish standing committees on individual privacy, with mandates to study the problems and report the appropriate legislation to interpret Fourth Amendment guarantees in the light of present technology, so as to move the Nation away from the invitation to the massive corruption of our liberties.

APPENDIX B

Bell System — Appendix B

The Bell System will play an important role in the Moorhead Subcommittee hearings, for several reasons:

1. Bell has developed a number of monitoring devices and techniques over the years--for its own use and for others' use.
2. The local AT&T unit, C&P, assigned management personnel to install the wiretap in the FCC building, in early 1970, because of suspicion of a leak of agenda matters. (This is treated in the separate section, "Monitoring of FCC Employees," q.v.)
3. Bell apparently provides wiretapping/eavesdropping devices to police agencies, as noted in the Wall Street Journal article of October 5, 1973, attached.
4. Bell has employed the M-220 Remobs (Remote Observing) system in some locations. This device only needs a push-button phone, via which the snooper can punch the appropriate access codes and listen in on other lines without detection and without any other physical connection.
5. C&P appears to have actively cooperated in the bugging of the home of columnist Joseph Kraft. The Post article of June 26, attached, was based on testimony of John Dean at the Watergate hearings.
6. Bell has stated its policy and procedures for handling wiretaps discovered by its employees. (See, e.g., the

AT&T Management Report of August 9, 1973, No. 33, attached, and also in the section tabbed "Monitoring of FCC Employees.") Some of the procedures outlined by Bell management could place a CWA-represented person in the position of cooperating in the continuance of criminally installed wiretap.

* * *

The foregoing items --- troublesome in retrospect, especially in the light of various civil liberties considerations --- can show that the higher levels of management of the Bell System are "in the middle." Management personnel can be faced with the desire to act as good citizens, which means a willingness to assist Government officials, who are presumed to be acting under the color of law. Events of the last 2 years would indicate better and tighter laws are required.

[The Wall Street Journal, Oct. 5, 1973]

LISTENING IN: DESPITE ALL THE TALK, LEGAL AND ILLEGAL TAPS ON TELEPHONES ARE FEW—TOUGH LAWS, CLIMBING COSTS DISCOURAGE THE PRACTICE; TWO STATES ACCOUNT FOR MOST

BOBBY SEALE AND ABBIE HOFFMAN

(By Jonathan Kwitny—Staff Reporter of The Wall Street Journal)

Let's say you're a Mafia bigwig, an important U.S. Senator, or the chairman of one of the country's largest corporations, and you think your telephone—legally or illegally—is tapped.

You probably have less to worry about than you think.

Largely because of Watergate, concern over wiretapping is widespread. Yet there probably is less of it than some Watergate-inspired scare stories would have you believe. Almost certainly, there's less of it than there was before 1968, when Congress strictly regulated legal wiretapping and set stiff penalties for illegal tapping.

The Internal Revenue Service, which used to tap so many phones that it ran a special school for tappers, now says it doesn't use electronic surveillance in income tax cases except when bribery is suspected—and there's no evidence that the IRS is lying. Manufacturers who sold tapping and bugging gear to the armed forces in the 1960s say they've made no such sales in the 1970s, and only with the Army is there evidence of continued electronic spying on American citizens. Private wiretappers likewise have retrenched. Sixty-eight percent of all court-approved wiretapping, and 80% of such tapping by state or local police, occurs in only two states, New York and New Jersey, according to statistics gathered by the administrative office of the U.S. courts, which has been assigned by Congress to keep tabs on wiretapping activities.

Lax laws and modest costs once permitted police and federal investigators, as well as private detectives, to wiretap freely. Now illegal tappers risk jail for damage suits. Prosecutors must go before a judge and provide detailed justification for a court-ordered tap. Moreover, they must inform a suspect 90 days after the court order expires that he has been tapped, and they may be required to give him a full transcript of any evidence thus produced.

THE "NATIONAL SECURITY" TAPS

Law-enforcement wiretappers also face high costs. Routine taps cost upward of $10,000, and complicated jobs can cost more than $100,000. Private persons who want to wiretap illegally can do it more cheaply because they don't need the manpower necessary to prove a criminal case. But they face other strictures. "It requires a good deal of expertise to do a good job," says James Robinson, who supervises illegal-wiretap prosecutions for the Justice Department. "The expertise doesn't appear to be as available as everybody believes."

The 1968 law allows persons whose phones are tapped illegally to sue the tappers for large damages. Dozens have sued Justice Department and Federal Bureau of Investigation officials to collect. Though none of the damage suits has reached trial, preliminary fact-finding has smoked out substantial evidence about improperly authorized government tapping activities—which have been curtailed since a June 1972 Supreme Court decision against "national security" taps or bugs on persons with "no significant foreign connection."

Under most interpretations of the 1968 law, the one kind of tapping or bugging that doesn't need prior court approval is surveillance ordered by the President under his constitutional power to pursue national security. But as a result of the June 1972 decision, the Justice Department says it dropped six of the "national security" taps then operating, presumably on domestic activist groups, and presumably because there was no clearly demonstrable "national security" threat in their activities.

(Still, two Federal Bureau of Investigation agents were discovered with wiretap gear in the telephone terminal room of the Jacksonville, Fla., federal building during a recent trial of antiwar veterans. The judge in the case accepted the FBI's explanation that the agents merely were checking FBI phone lines.)

COURT-ORDERED TAPS LEVEL OFF

The government apparently still conducts just over 100 national-security taps a year, mostly on foreign establishments in the U.S. At times during the 1960s, national security taps were placed on the Cuban Mission to the United Nations, the South Vietnamese Mission in Washington, and a Soviet trade mission in New York. Officials claim that even friendly countries do the same to U.S. missions abroad.

There's no evidence any of the national-security taps has produced dramatic information. The government values them so highly, nonetheless, that it has forfeited criminal cases against defendants overheard on taps—Bobby Seale, accused of contempt, Abbie Hoffman, of rioting, and lesser-known persons—rather than submit to court rules and disclose the locations of the taps.

Besides national-security taps, there are two other kinds of legal electronic surveillance. Probably the most common is "one-party consent" tapping. In all but a few states anyone can legally record his own telephone conversations (although he will violate a telephone-company rule if he doesn't beep a signal to warn of the taping), or hide a tape recorder in his pocket.

The other kind of legal tapping is court ordered. Its use seems to be leveling off. From 1968 to 1971, the number of court-ordered taps nearly doubled each year. But last year, courts issued 855 tap and bug orders, up only modestly from 816 in 1971. Of course, there are no statistics on the illegal—or possibly illegal—tapping by investigative agencies, police and private eyes before or since 1968. But there's no evidence it is widespread today. And many illegal tappers, including private detectives and White House "plumbers," eventually seem to get caught.

By the end of last year, the Justice Department had indicted 37 persons for illegal wiretap activities under the 1968 law. Of these, 16 were convicted, six were acquitted, and 15 were awaiting trial. Few citizen complaints—only one in 50—actually resulted in prosecution, however. Most of them stem from husband-wife disputes that Mr. Robinson, the department's enforcement supervisor, thinks are better resolved by a divorce settlement than the federal courts.

Another obstacle for illegal wiretappers, whether official or unofficial, is the ability of a suspicious telephone customer to have his line checked. The phone company says it quickly investigates whenever a customer requests; many private countersurveillance firms perform a similar service for a fee. Most police tappers, and even most illegal tappers, use equipment simple enough that a routine check will spot it, though some remote-controlled equipment is so supersophisticated it would escape detection.

Both New York's and New Jersey's telephone companies say they never have found a court-ordered tap in checking complaining customers' phones, though they have found illegal taps. New York Telephone Co. found five in 1972 and has found eight so far this year, most of them installed because of divorce disputes.

COSTLY AND BURDENSOME

Of last year's court-ordered taps, only 206, or less than 25%, were requested by federal agencies, mostly by the FBI but a few by the Internal Revenue Service, the Secret Service (in counterfeiting cases) and narcotics agents. The rest were requested by state and local authorities, mainly in New York and New Jersey.

Judges and law enforcement officers look on tapping with varying degrees of tolerance. Judge Frank S. Kingfield of the superior court in Mercer County, N.J., has never refused a request for a wiretap order. Last year he issued 134, or one of every six in the country. Many of the 134 were requested by state police headquarters in Mercer County for use elsewhere, but many also were requested by local officials.

Two-thirds of the taps in Mercer County were used to gather information or deter operators in numbers, or illegal lottery, cases. "Our purpose isn't to arrest gamblers but to try to control volume," says assistant prosecutor Wilber Mathesius. "Instead of giving the (numbers) information over the phone, they (the lottery operators) are running around with bags of slips. It puts a crimp in the volume they can handle."

Outside of Mercer County, some district attorneys decline to apply to a judge for most taps requested by police. New York prosecutor David Cunningham, who helps screen police requests for taps in drug cases, says only 20% get approved. He tries to weed out requests for taps that probably wouldn't help convict major importers of hard drugs. But elsewhere, taps have been used even in marijuana cases.

"I'LL MEET YOU OUTSIDE"

Many law-enforcement officials disapprove of wiretapping as a deterrent, or as a way of getting evidence in minor cases, especially those involving "victimless" crimes. It is too costly in money and manpower, they think, and "Wiretaps are enormously less productive than most law enforcement officials would admit, or than most citizens realize," says Joseph Joch, a New York narcotics prosecutor who works under Mr. Cunningham.

Others fear that abuse or overuse of wiretapping will create a backlash against it. New York Detective Sgt. Lawrence Mullins, who has cracked multimillion-dollar Mafia operations with phone taps, says that "the greatest weapon in sophisticated investigation is being threatened by nonsense." He makes clear his distaste for investigators who use tapping as a substitute for other methods.

Tapping systems differ. FBI and New Jersey tappers use more sophisticated equipment, and have a much closer working relationship with the telephone company, than do New York police. "We use a system where you can effectively sit in your home and monitor any phone in the country," says a New Jersey assistant prosecutor. "You'll hear everything that transpires over that number. We have to pay (New Jersey) Bell Telephone a rental fee." It takes only one detective a shift with a tape recorder to monitor each tap, the prosecutor says. The FBI uses a similar system.

In New York, investigators prefer "direct-line" devices, simple wires attached to the phone line and running to an eavesdropping spot in sight of the place being tapped. Sgt. Mullins says, "I find it very hard to understand how you can conduct an investigation from your office. If a guy says on the phone, 'I'll meet you outside,' we want to be able to see who's that guy he's meeting. I want to see who's coming and going." New York police also believe that direct-line gear gives better recording quality. Remote taps by the FBI sometimes have been so garbled they have been thrown out of court or have had to be redone.

HOPING AND PRAYING

The Justice Department is in danger of losing on appeal nearly 100 wiretap-based convictions and indictments because former Attorney General John Mitchell allowed Justice Department employes to sign their superiors' names to wiretap documents in violation of the "due process" defendants are entitled to under the 1968 law.

The law prohibits tappers from listening to conversations unrelated to the crime they're investigating. Tap evidence was thrown out in a New York heroin case recently because police had heard and recorded a mass of irrelevant conversations (though the defendants still face jail because they opened fire on the police who came to arrest them). "The (defense) lawyers listen carefully in pretrial hearings, and they just hope and pray they're going to hear something you shouldn't have recorded," says Sgt. Mullins. "That's the end of the case." Criminals sophisticated in the law often start phone conversations with harmless and irrelevant chatter, hoping any tapper will cut off before damaging talk develops.

Despite the deterrents, a legal or illegal snooper, if the information at stake is worth the cost and the risk, can find the technology to reach into almost any home, office or public building. Companies that manufacture the equipment report a steady drum of business, but no great upsurge. Business in the bug-detection field, however, is definitely on the upswing. One long-time supplier says he recently sold high-cost detection gear to such big corporations as General Electric and Carborundum Co. and to many smaller firms. At least three Senators recently have had their offices swept for listening devices, though none were found, and senatorial aides say other such sweeps are in the making.

[The Washington Post, June 26, 1973]

EX-BELL SYSTEM AIDE SAID TO HELP TAPS

(By Peter Jay, Washington Post Staff Writer)

The White House wiretappers who bugged the telephone of columnist Joseph Kraft in late 1969 used classified technical information supplied them by a former Bell System official, John Dean said in his Senate testimony yesterday.

Dean said he was told that the "pair numbers"—a code needed to identify one particular line in a cable that may carry 2,000—for Kraft's telephone were provided by John S. Davies of the White House staff, who had spent 28 years with Bell and worked on communications for three of Richard M. Nixon's political campaigns.

Officials of Bell's Washington affiliate, the Chesapeake & Potomac Telephone Co., say that their policy bars release of "pair numbers" except by court order or upon receipt of a written request citing national security considerations from either the Attorney General or the director of the FBI.

There was no such order or request, the FBI subsequently told Kraft.

In his testimony to the Senate Watergate committee, Dean said he was told about the tapping of Kraft's phone by John J. Caulfield, a former New York police investigator and security consultant who also worked in the White House.

"Caulfield told me (the wiretap) was performed by Mr. (Anthony) Ulasewicz, Mr. John Regan (sic) and himself," Dean said in his prepared testimony.

Ulasewicz has been identified in testimony as having conducted various covert operations for the White House. John Regan was a security consultant for the Nixon campaign in 1968 and then for the Republican National Committee. He left the payroll in late 1971 and could not be reached for comment yesterday.

AT+T Management Report
August 9, 1973 ✓

Perspective:

Bell System restates its full commitment to policy of privacy in communications

Privacy of communications has long been a basic concept of the Bell System's business. Bell believes that its customers have an inherent right to feel they can use the telephone with the same privacy they enjoy when talking face-to-face. Any undermining of this confidence seriously impairs the usefulness and value of telephone communications.

Over the years, the Bell companies have worked hard to insure that unwarranted intrusions do not occur. Employees, for example, are continuously reminded that privacy of communications must be safeguarded and that this responsibility is a condition of employment. And the Bell System has repeatedly gone on public record as welcoming legislation to strengthen and preserve the privacy of communications.

Wiretapping is an invasion of privacy and the Bell System strongly believes that any unlawful interception, use or disclosure of telephone communications should be prohibited. The extent to which wiretapping should be authorized for purposes other than national security is, in the Bell System's opinion, a matter for Congress, state legislatures and the courts to decide after a careful balancing of the interests involved—the right of an individual to privacy of communications and the rights of society to have court-authorized wiretapping used as a method of law enforcement. The Bell System companies have deliberately taken no public position on the wisdom of court-ordered wiretapping, other than to urge that proper safeguards be adopted if any legislation is passed authorizing court-ordered wiretapping.

Recent laws concerning wiretapping —chiefly the Federal Omnibus Crime Control and Safe Streets Act of 1968, as amended in 1971—make a public policy judgment that court-authorized wiretapping and eavesdropping by law enforcement agencies are in the public interest as effective methods of combatting serious crime and are acceptable when authorized under proper safeguards. These laws recognize that law enforcement agencies will need certain limited assistance to accomplish court-authorized wiretapping. The Bell System believes that any assistance on its part should be the very minimum necessary to accomplish the wiretapping—generally line access information such as cable and pair and multiple appearance identification. In no instance does the telephone company make the actual wiretap or place any bug, nor does it send a telephone employee along. Nor do Bell companies trace incoming calls to a suspect's line (line identification). Nor do they furnish telephone company trucks, tools, equipment, uniforms, employee identification cards or training to law enforcement agents.

What The Federal Laws Provide

The Federal Omnibus Crime Control and Safe Streets Act, originally enacted in June 1968, flatly prohibits under penalty of criminal law all illegal wiretapping and eavesdropping. It also prohibits the possession, manufacture, distribution or advertising of any wiretapping or bugging device. Bell System companies refuse all such advertising in the Yellow Pages in conformity with the law. They also go a step further and refuse all "debugging" ads, on the ground that the ability to debug also reflects the ability to bug.

The Federal Act authorizes wiretapping and eavesdropping by federal law enforcement officers (and by state and local law enforcement authorities if an appropriate state enabling law has been enacted) under court order in connection with the investigation of specified major crimes. Strict judicial controls are spelled out and prescribed procedures must be adhered to—covering for example, the type of crimes involved, the category of federal officials who can authorize applications for a court order, the use and disclosure of information obtained, and the specific procedures to be followed in obtaining and using a court order. Under federal law, interception without a court order by federal law enforcement authorities is permitted in an "emergency" involving conspiratorial activities relating to national security or organized crime, provided an application for a valid court order approving the wiretapping is made within 48 hours. This provision, however, has not to the Bell System's knowledge, been used.

The Federal Omnibus Crime Control and Safe Streets Act also provides that nothing therein shall limit the constitutional power (if any) of the President of the United States to authorize federal agents to engage in wiretapping without court order in cases involving national security.

Section 605 of The Communications Act of 1934, as amended, protects the privacy of telephone company communications. As a matter of policy, Bell companies conform to the

requirements of Section 605 and do not disclose toll record information except under lawful process—that is, a subpoena of a court, grand jury or, in the language of The Communications Act, "on demand of other lawful authority" (for example, a Congressional committee subpoena or an Internal Revenue Service summons). The companies make certain such demand is valid and requests specific information covering a designated period of time before any of these records are released.

What The State Laws Provide

State laws authorizing court-ordered wiretapping by state and local law enforcement agencies must conform to the strict requirements of the Federal Omnibus Crime Control and Safe Streets Act. At present, 22 states and the District of Columbia have such enabling legislation. In all other states, state and local law enforcement agencies cannot obtain court orders authorizing wiretapping.

The states with enabling legislation are:

Arizona	Nebraska
Colorado	New Hampshire
Connecticut	New Jersey
Delaware	New Mexico
District of Columbia	New York
Florida	Nevada
Georgia	Oregon
Kansas	Rhode Island
Maryland	South Dakota
Massachusetts	Virginia
Minnesota	Washington
	Wisconsin

Notification to Parties Under Surveillance

Under the Federal Omnibus Crime Control and Safe Streets Act, the court issuing a wiretapping order (or denying approval of a prior "emergency" interception) must notify the parties named in the application—and, at the discretion of the judge, other parties to the interception conversations—of the following:

- the fact that an application was received;
- whether the application was authorized, approved or denied;
- the period of authorized, approved or denied interception;
- whether communications were or were not intercepted.

Such notification by the court must be made within 90 days of the expiration of the order and its extensions (or within 90 days of the denial of an application for approval of an "emergency" interception), unless the time for notification is extended by the court on a law enforcement showing of good cause.

Wiretapping applications and orders are "sealed" by the court. The act provides that a person, including a telephone company employee, can be held in criminal contempt for disclosing the existence or content of any such application or order without prior approval of the issuing judge. The Bell companies, accordingly, are obliged to advise their customers that they cannot answer any inquiries concerning the existence or nonexistence of such orders.

Discovery of Wiretaps

When a customer requests a telephone company check for a suspected wiretap, the recommended Bell System policy is as follows:

- If no tap or no evidence of a tap is found, the customer is so informed.
- If an illegal wiretap is found, the appropriate law enforcement agency and the customer are informed that "a device" has been found and that any questions should be addressed to the proper law enforcement authorities, whom the Bell company identifies. Law enforcement authorities generally are given a reasonable opportunity to investigate before the device is removed.
- If a legal wiretap is found, law enforcement authorities are advised that the customer will be told "a device" has been found and any questions should be addressed to the proper law enforcement authorities, whom the company identifies.

The report to the customer is identical whether the wiretap is legal or illegal. The customer is merely told that "a device" was found without characterizing it as legal or illegal. This is done to avoid inadvertently disclosing the presence of a legal wiretap.

If there has been no subscriber inquiry but a telephone employee finds a wiretap, the recommended Bell System policy is as follows:

- If the wiretap is illegal, both the customer and law enforcement authorities are advised that "a device" has been found. The law enforcement authorities generally are given a reasonable period to investigate before the wiretap is removed.
- If the wiretap is legal, the customer is not advised and the device is not disturbed unless it is causing trouble on the line.

The number of wiretapping devices Bell companies have found has been low in relation to the number of customer requests asking them to check for suspected wiretaps. In 1972, there were some 10,000 requests asking them to check for suspected wiretaps and about 175 devices were found, less than one per Bell System company per month. □

APPENDIX C

Monitoring of FCC Employees

In early 1970, FCC Chairman Dean Burch and the executive director had the suspicion that items from the weekly commission agenda papers were being leaked by an employee of the Network Study Branch in the Broadcast Bureau to a lawyer who used to work at FCC and now is in the private broadcasting industry. An employee who seemed to want to be an amateur investigator reported the suspicion to the security officer.

Instead of doing a methodical job of investigation, the security officer got permission to install a wiretap on the employee's phone The man's three lines' terminals had jumper wires run from the wire room on the third floor up to the security officer's desk, on the eighth floor. The idea was to learn if the ex-FCC employee was getting agenda items from the FCC employee in Network Study.

FCC arranged with a Vice President of C&P Telephone Company to get the tap installed. The job involved running the extension wires up five floors. The company was required to do the job after working hours at FCC, with the instructions to be given by the security officer. The billing was to go directly to the security office, where it would be discreetly handled.

A C&P foreman was given the work order orally. He saw something fishy and asked a superior what to do. The superior told the foreman not to do the job without a written work order. When the written order was produced, the foreman went to FCC, joined up with the security officer and did the work. The wiretap stayed in place five weeks, early in 1970.

Late in 1970, the FCC security officer decided to close the investigation, because he had by then gotten no evidence. He

reported hearing only trivial conversations.

* * * * * * *

In early 1972, the House Commerce Committee got a tip that the tap had been used two years earlier, and Chairman Harley Staggers assigned his investigators to get the facts. After the wiretap was confirmed, the Investigations Subcommittee held two sessions of hearings, in March and May 1972. FCC Chairman Burch and five top FCC officials appeared and were required to explain the situation under oath.

During the course of the hearings, the FCC officials attempted to hold to the position that the agency was not covered by the wiretap statute. In the hearing the FCC Chairman was confronted with his own contradiction. He had written to another Subcommittee Chairman, Representative John Moss, who was looking into monitoring devices, flatly stating that FCC employed no wiretaps because of agency regulations.

In mid-1972, the Justice Department wrote to the House Subcommittee flatly rejecting the FCC legal opinion that the tap was legal.

The latest FCC position was a promise not to repeat the use of taps.

See page 48 of the Staggers Subcommittee hearings on the matter. It is interesting to read the "Introduction" paragraph of the "Memorandum of the Use of Telephone Extension to Monitor Improper Communications," dated May 15, 1972, prepared by the Commission's

General Counsel, John W. Pettit. As the "fact situation" reads, there was a suspicion in 1970 in a single instance that Commission agenda items were "regularly being disclosed to outside parties." That suspicion, in the next clause, escalates to the status of "evidence" and remains as "evidence" in the third and final clause. The final sentence in that paragraph is highly interesting: some "information" was the basis for the decision to install a wiretap, euphemistically termed a "telephone extension" so the security personnel could monitor the "illicit calls." The remainder of the Pettit memorandum does not document how the suspicion was borne out to become evidence. Mr. Pettit and the security personnel would be well advised to adopt more precision in their operations.

CWA was concerned over the very serious implications of the type of monitoring employed at FCC, since what was done could have been construed as a criminal offense. CWA President Beirne took the following actions:

1. On January 16, 1973, wrote a memorandum to the Executive Board members and National Directors advising of the incident, enclosing copies of the hearings and report issued by the Staggers Subcommittee.
2. Directed, in that memo, that the Union's Vice Presidents immediately bring the FCC monitoring to the attention of telephone company management personnel with whom they maintain contact.

3. Directed the Vice Presidents to report back to CWA Washington the results of their contacts with company management.

The CWA concern was twofold: the Union has long held the position that wiretaps are highly subject to abuse, so much so that they should be banned, and that installations of certain wiretaps, like the one at FCC, could place CWA-represented craftsmen in violation of criminal law. The January 1973 Beirne memo said that management should be required to perform such work, in order that any possible criminal charges would remain within management ranks.

COMMUNICATIONS WORKERS OF AMERICA,
Washington, D.C., October 31, 1972.

File: 1.12.23.57 x 3.1.

Hon. HARLEY STAGGERS,
Chairman, Special Subcommittee on Investigations, Committee on Interstate and Foregin Commerce, House Office Building, Washington, D.C.

DEAR MR. CHAIRMAN: Your Subcommittee's investigation earlier this year of the wiretapping activities being conducted at the Federal Communications Commission showed the latter's sincere disregard for law. The activities admitted can only be justified in a police state. The Commission certainly must have been aware of the legal strictures on monitoring, since its organic statute, the Communications Act of 1934, which the Commission is charged with enforcing, contained the main communications privacy provisions, in Section 605. We note that 1968 legislation made changes in Section 605 and eased to some degree the laws on monitoring.

The Communications Workers of America has for a number of years been decidely "hard-line" in opposition to the use of wiretaps, with a single exception: cases involving genuine national security. For your Subcommittee's use, I am enclosing copies of the resolutions dealing with invasion of privacy, adopted by the Union's Conventions of 1965, 1966, and 1967. In addition, I testified before the Senate Subcommittee on Administrative Practice and Procedure on May 5, 1965, and April 21, 1967, on invasions of privacy, with special emphasis on the telecommunications industry, where the bulk of the Union's members are employed. Copies of pages from the 1965 and 1967 hearings also are enclosed. [Enclosures hereto have not been printed for this report].

It is interesting to read the "Introduction" paragraph of the "Memorandum on the Use of Telephone Extension to Monitor Improper

Communications," dated May 15, 1972, prepared by the Commission's General Counsel, John W. Pettit. As the "fact situation" reads, there was a *suspicion* in 1970 in a single instance that Commission agenda items were "regularly being disclosed to outside parties." That suspicion, in the next clause, escalates to the status of "evidence" and remains as "evidence" in the third and final clause. The final sentence in that paragraph is highly interesting: some "information" was the basis for the decision to install a wiretap, euphemistically termed a "telephone extension" so the security personnel could monitor the "illicit calls." The remainder of the Pettit memorandum does not document how the suspicion was borne out to become evidence. Mr. Pettit and the security personnel would be well advised to adopt more precision in their operations.

The transcripts of your Subcommittee's hearings, on March 28 and May 16, 1972, disclose that no solid evidence of wrongdoing was produced, even after a month of eavesdropping. The security officer, Mr. Goldsmith, could not testify that he had heard conversations involving agenda items.

Somehow, the attorney who once had been employed by the Commission is termed a "trespasser," by a tortuous exercise in logic, inasmuch as he was in the Commission's offices after normal working hours—even though some Commission personnel from time to time remain after 4:30 p.m. The Commission employee spied on had working hours ending at 5:30 p.m. The attorney may have, and probably did, use the Commission's telephones for his own purposes. But employment of an illegal eavesdropping device is not warranted in the situation described on the hearing record.

It is quite clear that the Commission's security force resorted to the illegal wiretapping expedient, despite no solid evidence except that provided by a person who liked to play "amateur investigator," because of unwillingness or inability to perform sound investigative work.

The Pettit memorandum of May 15 steered away from the limited monitoring authorization granted to the Commission in Section 802 of Public Law 90-351, the "Omnibus Crime Control and Safe Streets Act of 1968." The new Chapter 119 added to Title 18 U.S.C. included Section 2511, whose paragraph 2(b) allows the Commission to monitor oral communications but only in the interests of service quality. That "explicit Congressional intent" was laid forth in the section-by-section analysis included in Senate Report 1097, 90th Congress. In crime detection situations, certain procedural safeguards including court orders are required.

We hope that in the future, all persons and organizations, whether part of government or private industry and including telephone companies, will refrain from such nefarious activities. And if they so indulge themselves, the responsible parties should be criminally prosecuted to the full extent of the law.

Sincerely yours,

JOSEPH A. BEIRNE,
President.

Communications CWA Workers of America

(AFFILIATED WITH AFL-CIO)

OFFICE OF
THE PRESIDENT

1925 K STREET, N.W., WASHINGTON, D.C. 20006
TELEPHONE FEDERAL 7-7711

January 16, 1973

File: 3.1
x 1.12.23.57

TO: Executive Board Members and National Directors

FROM: Joseph A. Beirne, President

SUBJECT: "FCC Monitoring of Employees' Telephones"

Fellow Officers:

The House Committee on Interstate and Foreign Commerce, which holds legislative oversight jurisdiction over the Federal Communications Commission, recently released the printed hearings and investigative report entitled "FCC Monitoring of Employees' Telephones." Copies of the hearing record (Serial No. 92-101) and House Report No. 92-1632 are enclosed herewith.

Your attention is being called to significant portions of these documents.

In the interest of protecting telephone company plant employees who are represented by CWA, I strongly urge you to bring this monitoring incident to company management's attention immediately. If company management is willing to help someone else commit a highly illegal act, such as installing a wiretap, we must let company management perform all of the work, and take the consequences which include 5 years in prison and a $10,000 fine.

In the FCC monitoring of early 1970, the responsible FCC officials claimed they were acting within the law. The Department of Justice flatly disagreed. FCC has promised not to repeat the monitoring.

Your attention is especially called to these pages:

Hearings, pp. 1-5, FCC Chairman Burch explains the situation.

pp. 10-20 and 78-80, Security Officer Goldsmith explains how the wiretap was arranged for and installed. Names of C&P personnel involved are included.

pp. 39-45, Chairman Burch recalled; admits no evidence was gained from the monitoring; admits irregular billing procedure was used.

Report pp. 1-3, Committee description of case.

pp. 18 and 47, extract of, and full text of, Beirne-to-Chairman Staggers letter commenting on the monitoring and supporting the Subcommittee's efforts.

pp. 62-63, text of Justice Department letter to Staggers, in which a 1967 Federal Court case's findings against Michigan Bell are cited. This letter, and the follow-up Justice Department letter (p. 69) show the rejection of the FCC attempts at justifying the 1970 monitoring.

The Investigations Subcommittee has advised it can furnish additional copies of the hearings and report in reasonable quantities, upon request. Please advise if you need additional copies.

I am most anxious to have your reports as to the company management reaction you perceive when you discuss this matter.

Joe Beirne

Enclosures

EBP-1913

APPENDIX D

[The New York Times, May 14, 1974]

High Court Voids Drug Wiretaps; 600 May Be Freed—Justices Upset 1970 Conviction of Narcotics Sellers, Citing Invalid Federal Order; Wide Effect Foreseen

Errors in gaining evidence under Mitchell likely to embrace other cases

(By Warren Weaver, Jr., Special to the New York Times)

Washington, May 13.—The Supreme Court ruled today that a group of narcotics sellers were illegally convicted in 1970 because the Department of Justice had obtained evidence against them with invalid wiretapping orders.

Although the decision directly involved only one case and a few defendants, it appeared almost certain to wipe out convictions of more than 600 other Federal offenders against whom the same kind of evidence was used.

The high court agreed unanimously that evidence could not be used against a Federal suspect if it was obtained through a wiretap based on an application signed by the Attorney General's executive assistant rather than by the Attorney General himself, then John N. Mitchell.

Some taps supported

In a parallel case, however, the Court voted 5 to 4 in support of wiretap applications that were in fact authorized by the Attorney General but appeared to be signed by an Assistant Attorney General who had actually not played any part in their preparation.

The effect of this ruling will be to preserve the convictions of 807 Federal convicts for whom Mr. Mitchell authorized surveillance but whose papers incorrectly indicated that the authorization had come from Assistant Attorney General Will R. Wilson.

In the first case, all nine justices agreed that an initial authorization signed by Sol Lindenbaum, executive assistant to Mr. Mitchell, had not met the requirements for a wiretap order set by the Organized Crime Control Act of 1968.

Four Justices, however, did not agree with the majority that an extension of this order and two related orders to record numbers dialed from a given telephone were also improper. They were Chief Justice Warren E. Burger and Associate Justices Lewis F. Powell Jr., Harry A. Blackmun and William H. Rehnquist.

Dissenters in second case

Dissenting from the decision that the Wilson-signed authorizations did not result in tainted evidence were Associate Justices William O. Douglas, William J. Brennan Jr., Potter Stewart and Thurgood Marshall.

The decision may cost the Justice Department a substantial amount of money, as well as embarrassment at having mishandled 60 cases. Federal law provides that anyone whose telephone is illegally tapped can recover $100 a day in damages plus unspecified punitive damages and legal expenses.

The principal case involved Dominic N. Giordano, whose telephone was tapped for a month in the fall of 1970 after he had sold narcotics to an undercover agent. The application for the wiretap order was signed by Mr. Lindenbaum rather than by Mr. Mitchell or an Assistant Attorney General designated by Mr. Mitchell.

Writing for the majority, Associate Justice Byron R. White rejected the Government's argument that the Attorney General has broad power to delegate his authority. Justice White maintained instead that Congress had clearly specified that wiretap requests could be signed only by the Attorney General or a designated Assistant Attorney General.

In the second case, Mr. White wrote for the narrow majority that in misidentifying Assistant Attorney General Wilson as the official who authorized the wiretaps, when it was actually Mr. Mitchell, the Justice Department had not made the seizure of evidence unlawful.

Pay Your Telephone Bill or You'll Be on Party Line

(By a Wall Street Journal Staff Reporter)

Although the 1968 federal wiretap law appears to limit tapping to use by law-enforcement agents, the telephone company claims an exemption for many of its employes—much to the benefit of government prosecutors. AT&T contends that anyone it suspects of dodging its bills, through fraud or mechanical devices, isn't entitled to privacy in calling. So the company listens in and passes evidence of toll fraud to the government.

But sometimes—by what the phone company says is "sheer coincidence"—these toll-fraud taps produce evidence of other, more serious, crimes. Some of the Justice Department's most prized wiretap convictions against important gangsters resulted from toll-fraud wiretaps—although toll fraud wasn't charged in court.

Over the years, according to interviews with law-enforcement veterans, phone-company security officers have offered the FBI and local police forces easy access to information about phone line locations (to facilitate tapping) and customer toll records, despite public denials by the company. Despite further denials, interviews indicate that phone-company employes sometimes help lawmen by stringing wires for a tap. And, human nature being what it is, employes sometimes take advantage of their technical ability to listen in on customer phone lines, just out of curiosity.

[The New York Times, June 1, 1974]

Police Use Illegal Wiretaps in 33 Cases Here

(By Deirdre Carmody)

The Police Department has informed the special state prosecutor, Maurice H. Nadjari, the citywide narcotics prosecutor, Frank Rogers, and the five District Attorneys that 33 narcotics-related arrests between 1969 and 1971 were based on illegal wiretapping and that untruthful evidence was presented at some of the trials.

The information was in a letter sent on May 22 to the prosecutors by the first deputy police commissioner, James M. Taylor. It was based on testimony at an interdepartmental trial in April by a former detective who had been a member of the special investigating unit for narcotics.

He startled spectators in the courtroom by asserting that he had placed illegal wiretaps on suspected narcotics dealers before arresting them, and that he had perjured himself a number of times when called as a witness at their trials.

INVESTIGATION ORDERED

The testimony was given by Detective Carl Aguiluz at the interdepartmental trial of Sgt. James M. O'Brien, his former colleague in the narcotics unit. Following his trial, Sergeant O'Brien was cleared of the various charges against him, but Police Commissioner Michael J. Codd immediately ordered an investigation into any cases that might have been affected by Detective Aguiluz's actions.

One defendant was sentenced to state prison for a maximum of up to seven years. Two other defendants have probably already served sentences, although this could not be confirmed yesterday. Seventeen cases were dismissed. Warrants are out in another five cases on defendants who have presumably jumped bail, and the disposition of the other cases could not be learned.

CAPTAIN FINED $15,000

In an unrelated development, a captain in one of the Police Department's highest anticorruption commands was allowed to retire yesterday with his pension after paying a $15,000 fine in connection with charges of receiving payments in lieu of making prostitution arrests more than 10 years ago.

Capt. John O'Shea, the second-ranking member of the inspectional services division, pleaded no contest to charges he received an initial payment of $500 and subsequently monthly payments of $200 from April, 1963, to April, 1964, from Thomas Chaipis, proprietor of Magoo's, a bar at 21 Avenue of the Americas, where prostitution was allegedly taking place. Captain O'Shea was then the training officer in the Manhattan South Precinct.

APPENDIX E

FBI and Other Snoopers in the Wireroom and Elsewhere

Although AT&T has stated its policy of "full commitment to privacy in communications," a few recent examples of abuses call the policy into question.

The AT&T Management Report of August 9, 1973, apparently responding to the June 1973 CWA Convention resolution, "The Abuse of Technology: Freedom's Enemy, Corruption's Ally," recited what has been the Bell System policy on wiretaps and the degree of cooperation with law enforcement operations. Attached in this section is a copy of the Bell System policy statement. Those of the other Bell units are virtually identical to the AT&T statement. The statements proclaim: "Nor do they (i.e., Bell System companies) furnish telephone company trucks, tools, equipment, uniforms, employee identification cards or training to law enforcement agents."

If that Bell System policy statement means what it purports to say, then the Bell System should be asked to explain several incidents:

1. In July 1973, two FBI agents with a briefcase full of electronic equipment were found in the telephone wireroom of the Federal Courthouse in Gainesville, Florida. The wireroom was adjacent to the room being used at that time by the lawyers defending seven anti-war Vietnam veterans who were on trial at that time. The FBI agents explained that they were checking out FBI telephone lines. The FBI agents were assigned to the Jacksonville field office, 60 miles from Gainesville. Southern Bell Telephone & Telegraph Company serves the Gainesville area.

2. A former Bell System employee, who went to the White House staff after 28 years with Bell, assisted in the bugging of the telephone of columnist Joseph Kraft. The facts of this incident came to light June 26,

1973, in the testimony of ex-White House Counsel John W. Dean III, in the Watergate hearings. C&P Telephone Company said its policy bars release of cable pair numbers except on court order or a written request citing "national security" considerations and signed either by the Attorney General or FBI Director. The former Bell System employee, John S. Davies, was reported to have worked on three Nixon political campaigns.

3. In early 1970, C&P management installed a wiretap on the telephone lines of an employee of the Federal Communications Commission who was suspected of leaking FCC agenda items to a trade lawyer. (For details, see separate section, "Monitoring of FCC Employees.")

* * * * * * * *

The FBI should be asked to provide full information on the following incident:

> In April 1969, an FBI agent with a radio transmitter in hand was discovered eavesdropping on a lawyer-client conference involving eight defendants indicted for conspiracy to riot at the 1968 Democratic National Convention in Chicago. The FBI attempted to explain that the radio set was merely for keeping the agent in touch with his office.

(The incident described above was the subject of a New York Times story on April 11, 1969.)

* * *

The New York Times of December 26, 1973, notes the existence of a confidential FBI report that appeared to contradict the testimony of onetime Acting FBI Director L. Patrick Gray III, who was forced to resign in ignominy in the Watergate scandal. The Times secured a copy

of the confidential report, which points out that Gray had information available to him on the existence of about 20 so-called "national security" wiretaps ordered by President Nixon on various newsmen and administration officials. Gray testified under oath he knew of no such taps.

The Moorhead Subcommittee should acquire a copy of the FBI report, subject of the by-lined story of John M. Crewdson, and call Gray in for testimony on the subject.

[The Washington Post, Aug. 1, 1973]

FBI Men Found in Wireroom

(By Timothy Robinson, Washington Post Staff Writer)

Gainesville, Fla., July 31.—Two FBI agents, one of whom carried a briefcase full of electronic equipment, were discovered this afternoon in a telephone wireroom of the federal courthouse here adjacent to the offices of lawyers for seven antiwar Vietnam veterans and one supporter who are on trial on charges of conspiracy to riot at the Republican National Convention last summer.

Members of the defense staff discovered the two men through a knee-high grating connecting their office and the phone room. They immediately contacted U.S. District Judge Winston E. Arnow, who ordered a U.S. marshal to open the room and called an immediate extraordinary hearing in his chambers to discuss the incident.

The two agents, one of whom admitted to having worked on the VVAW conspiracy case, told the judge they were in the room checking out FBI telephone lines.

One of the agents, Carl Ekblad, said he was doing the checking with a telephone handset to make sure there were "no connections" on the lines. The other, Robert Romans, said he was "just holding the paper" on which several phone numbers—among them the local FBI main number—were written.

Ekblad, who indicated he was knowledgeable about telephone equipment, said the briefcase contained two amplifiers, a transmitter, a receiver, earphones and other tools and equipment. Romans said he was not familiar with the equipment or what Ekblad was doing in the room. Both of the agents are from the Jacksonville field office, about 60 miles from here, and Romans said he had investigated VVAW members in the past.

The Gainesville FBI office is on the same floor as the telephone wireroom in this three-story courthouse.

Any attempts by defense attorneys to get further details on the FBI agents' activities in the room were stopped by Arnow, who said the defense attorneys appeared to be making "mountains out of molehills."

He refused to seal the room where the men were discovered or to impound any of the equipment, and took no action concerning the FBI agents.

After a 45-minute hearing in his chambers, interrupted once as lawyers, defendants, marshals and the press went down the hall to inspect the wireroom, Arnow refused a defense motion for a full evidentiary hearing, at which electronic experts could testify about the equipment. However, attorneys for the defense, who are limited by a "gag rule," imposed by the judge, from talking about the case, indicated they would renew attempts to hold such a hearing Wednesday.

Justice Department attorney Robert Schneider, one of the prosecutors in the case, objected to any further, detailed questioning of the agents about the purpose of their being in the wireroom, and several times Arnow told the agents not to answer questions even before Schneider made objections. Schneider said the agents had been in his office earlier in the day to make sure his lines were not bugged, but said he did not know specifically why they were in the wireroom.

Schneider would not say whether it was normal FBI procedure to have its phone lines checked for taps.

"I realize it doesn't look good," Schneider said. "I don't want to talk about it."

The discovery was made at 6:15 p.m., about 30 minutes after the first day of the VVAW trial, devoted to questioning prospective jurors.

The veterans claim that the charges against them were trumped up by the Nixon administration in an attempt to justify the Watergate break-in. They also claim that FBI informants were the only persons who suggested violence during the convention, but those suggestions were rejected.

Prosecutors, while reluctant to go into details for fear of violating the broad gag rule imposed on lawyers, defendants and witnesses, contend they have a strong case to prove their charge that the vets were arming themselves with assorted weapons—some of them as bizarre as wrist slingshots—to cause violence at the GOP convention.

Strong security procedures have been placed in effect at the courthouse for the trial. More than 500 VVAW supporters are expected to participate in a demonstration here Saturday.

[The New York Times, Aug. 1, 1973]

Check of Phone Lines by F.B.I. Stirs Dispute at Trial of 7 Antiwar Veterans

(By John Kifner, Special to The New York Times)

Gainesville, Fla., July 31.—A short-lived imbroglio developed today on the first day of the trial of seven antiwar Vietnam veterans here after two F.B.I. agents were discovered with telephone and electronic gear in a broom closet adjacent to the court-supplied defense offices in the Federal Building.

The seven veterans and a supporter are accused of plotting an assault by automatic weapon, crossbow and slingshot on the Republican National Convention in Miami Beach in 1972.

In an informal hearing in the chambers of Federal District Judge Winston E. Arnow, defense attorneys directed a series of questions at the two F.B.I. men from the Federal Bureau of Investigation in an attempt to discover if they were bugging the lawyers' offices.

But Judge Arnow overruled many of the questions and said he thought the lawyers were making "mountains out of mole hills."

Judge Arnow denied the defense's motion for evidentiary hearing to discover if there had been bugging, wiretapping or other penetration of the defense camp.

"CHECKING F.B.I. LINES"

Clutching a telephone receiving device equipped with alligator clips and a small plastic box of screw drivers, one of the F.B.I. agents, Carl Ekblad, asserted that he was only "checking the F.B.I. lines."

The other agent, Robert Romans, said that he "had no knowledge" of the use of any electronic devices, but was "only holding the paper" on which they took notes.

The agents had with them, when one of the defendants, Peter Mahoney, saw them through a vent, a large Samsonite attaché case packed with electronic equipment including, they testified, a battery pack, an amplifier, an output transmitter, a receiver and "a couple of little earphones" and other gear and tools.

Although the defense attorneys indignantly attempted to press their questioning of the two men, Judge Arnow said, with a wave of his hand, that "these gentlemen have been perfectly candid and honest."

The trial began this morning in an atmosphere of gathering tension.

Electronic metal detectors stand in front of the elevators in the lobby of the Federal Building and in the corridor leading to the third-floor courtroom. Some 25 Federal marshals have been brought in from around the country and others have been placed on standby alert.

At a park by the airport at the edge of the city, about 200 veterans and supporters have set up an encampment, preparing for a series of demonstrations against the trial.

Federal District Judge Winston E. Arnow has placed a "gag rule" on the defendants, their attorneys and "all persons in active concert or participation with them." Citing their contention that the trial is an example of "political-suppression," he has forbade them from speaking to reporters.

PAPERS PROTESTED

Yesterday, Judge Arnow refused to modify the order despite arguments brought on behalf of The Miami Herald, other papers and the Reporters Committee for Freedom of the Press. In a pretrial hearing last month, he banned a television artist and fined the Columbia Broadcasting System $500 for airing sketches she made from memory outside the courtroom, but was later reversed by the United States Court of Appeals for the Fifth Circuit.

The Government charges that the seven members of Vietnam Veterans Against the War and an employe of a local hippie store conspired to "organize numerous 'fire teams' to attack with automatic weapons, fire and incendiary devices police stations, police cars and stores" in Miami Beach during the convention.

The indictment further alleges that they would "fire lead weights, 'fried' marbles (heated so they would shatter on impact), ball bearings, 'cherry' bombs, and smoke bombs" at the police with "wrist rocket slingshots and cross bows."

Denying the charges, the defendants contend that the indictment is an attempt to discredit their antiwar activities and part of an attack by the Department of Justice on radical groups.

The defense—noting that James W. McCord Jr., convicted Watergate conspirator, testified before the Senate Watergate Committee that he had been briefed by the Justice Department's Internal Security Division and that he cited the indictment in saying that fears of violence had prompted the bugging of the Democratic national headquarters—have attempted to link the case with the Watergate scandal.

Judge Arnow has shown scant patience with such arguments in pretrial sessions and has repeatedly said that he does not regard this as a "political trial." In a pretrial session last month, he ruled out 30 defense questions directed at former Attorney General John N. Mitchell seeking such political links.

The indictment is one of a series of conspiracy cases brought against radical groups by the Internal Security Division—recently placed under the Criminal Division—primarily by the chief of its Special Litigations Section, Guy L. Goodwin.

Over the last few years, Mr. Goodwin has traveled about the country directing grand jury investigations of radical groups. His indictments include the Berrigan case—in which Roman Catholic activists were charged with plotting to kidnap Henry A. Kissinger, the Presidential adviser, and a series of indictments against alleged Weathermen.

As in his past cases, Mr. Goodwin will not be trying the case in the courtroom. The prosecution is being handled by Jack Carrouth, the senior assistant United States Attorney for the Northern District of Florida, aided by Robert Schneider, a prosecutor sent down from Washington who has worked under Mr. Goodwin on racial cases. However, Mr. Goodwin is here.

The seven antiwar group members—all combat veterans, most of them decorated—are: Scott Camil, Alton C. Foss, John W. Kniffin, Peter P. Mahoney, William J. Patterson, Donald P. Perdue and Stanley K. Michelson Jr., who is charged with knowing of the alleged conspiracy but not telling the authorities. The eighth defendant, John K. Briggs, is charged with ordering 60 wrist rocket slingshots from the store at which he worked.

At the rain-drenched cluster of tents where they are camped, the other members of the Vietnam veterans group held a news conference this afternoon to read a statement of support in apparent defiance of Judge Anrow's order.

"SERIOUS JEOPARDY"

"The trial of the Gainesville Eight clearly shows the extremes the Government will go to smash legal dissent against its policies," the statement said. "This order by Judge Arnow continues a precedent that is putting the basic human rights of the people of this country in extremely serious jeopardy."

In pretrial motions this morning, Judge Arnow directed the Government to turn over any exculpatory evidence. He overruled a defense motion objecting to a mass questioning of the prospective jurors from Morton Stavis, a lawyer, who attempted to have Richard Christie, a Columbia University social psychology professor, testify that this would be ineffective in discovering possible prejudice. This afternoon the jury selection began, with the judge conducting the questioning.

As they entered the courtroom shortly before 8 o'clock this morning, Mr. Camil, Mr. Kniffin and Mr. Foss triggered the electronic metal detectors and had to remove their belts and shoes.

The detectors had been set off by shrapnel remaining in their bodies from their Vietnam wounds.

[The New York Times, Apr. 11, 1969]

LAWYERS SAY F.B.I. EAVESDROPPED ON RIOT SUSPECTS IN CHICAGO

(By Sidney E. Zion)

The Federal Bureau of Investigation was accused yesterday of eavesdropping on a conference in the United States Courthouse in Chicago between lawyers and eight defendants under indictment for conspiracy to incite a riot at the Democratic National Convention in August.

The charges were made by Gerald B. Lefcourt and Leonard I. Weinglass, attorneys for some of the defendants. Mr. Lefcourt said in an interview that he had "caught" an F.B.I. agent, David Hill, trying to "get away" from the conference room with a transmitter in his hand.

Mr. Hill denied yesterday that he had eavesdropped on the lawyer-client conference but conceded that he had been outside the 15th floor office with a radio transmitter.

"I had no tap equipment," Mr. Hill said. "It was just a radio that I used to let my office know where the demonstrators were."

Mr. Hill said he could make no further comment on the incident.

Mr. Lefcourt and Mr. Weinglass said that a motion would be filed in Chicago Federal Court today charging the F.B.I. with eavesdropping and demanding that a "cease and desist" order be issued against "all further bugging, wiretapping and surveillance."

The lawyers added that they would ask United States Attorney Thomas Foran to press criminal charges "against any and all F.B.I. agents involved."

But Mr. Foran said he did not consider the charges to be serious.

"The agent had no eavesdropping equipment," he said in a telephone interview yesterday. "The agent was charged by his superiors with following the defendants wherever they went in the building. He had a recording device to our office. It was a regular transmitter radio with a hand mike and nothing more."

Mr. Foran said that there were "demonstrators all over the building" and thus F.B.I. agents were "checking on their whereabouts."

LAWYER DISPUTES REPORT

Mr. Foran said he had called Mr. Hill into his office when Mr. Lefcourt and other lawyers complained about the incident.

"I offered to turn over the equipment to them and I showed them that it had no eavesdropping devices. In fact, when Kunstler [William B. Kunstler, another attorney for the defense] saw it he said 'Oh, forget it.' "

But Mr. Kunstler denied this yesterday. "I never said anything like that," the lawyer asserted. "In fact, I was coming out of the conference room when the whole thing happened and I never saw anybody look as guilty as that agent when he was trying to duck around the corridor corner."

Mr. Kunstler said that he and all the other lawyers for the eight defendants were joining in the motion to be filed today.

Mr. Weinglass challenged the assertion that the equipment was merely a device to report on the whereabouts of the defendants. He said that agents with walkie-talkies were "all over the place, following us all day" but that Mr. Hill's device was "much bigger and much different than all the others we saw."

According to Mr. Lefcourt, Mr. Weinglass and Mr. Kunstler, the lawyers and clients were in a conference room some 100 feet from the United States Attorney's office discussing travel restrictions on the defendants proposed by the Government, as well as other defense matters.

After about 20 minutes, the lawyers said, the meeting broke up and Tom Hayden, one of the defendants, walked out the door followed by Mr. Lefcourt and Mr. Kunstler. When they spotted Mr. Hill they asked him for his name and he allegedly refused to give it. Another F.B.I. agent then appeared and reportedly told Mr. Hill that he did not have to say anything.

The lawyers then went into Mr. Foran's office and described the incident, with Mr. Lefcourt shouting angrily that the F.B.I. had eavesdropped on the room.

Mr. Lefcourt said that the United States Attorney appeared surprised at the incident and that Mr. Hill later came into the office and explained that he had not been eavesdropping. "I called him a liar to his face," Mr. Lefcourt said, "and I say it again."

The defendants, who are also charged with crossing state lines to foment disorder or to otherwise violate the Civil Rights Act of 1968, will also join in the motion today. The defendants are Rennard C. (Rennie) Davis, Bobby G. Seale, John R. Froines, Lee Weiner, David T. Dellinger, Hayden, Jerry C. Rubin and Abbott H. (Abbie) Hoffman.

TRAVEL RESTRICTIONS LIFTED

CHICAGO, April 10 (UPI)—The Government reversed its position today and agreed to lift travel restrictions on the eight defendants.

United States District Judge Julius J. Hoffman signed the Government order. It allows the defendants to travel within the continental limits of the United States and Puerto Rico on condition they report their itineraries to the United States Attorney.

[From the New York Times, Dec. 26, 1973]

Report by F.B.I. Disputes Gray on Wiretaps

(By John M. Crewdson)

WASHINGTON, Dec. 25—A confidential F.B.I. report apparently contradicts the testimony of L. Patrick Gray 3d last March that he had no knowledge of nearly 20 "national security" wiretaps that President Nixon had ordered on newsmen and officials of his Administration.

Following the first published report of the wiretap effort, Mr. Gray told the Senate Judiciary Committee, which was holding hearings on his nomination to become Director of the Federal Bureau of Investigation, that he had made an inquiry and found "no record of any such business."

However, a copy of the confidential F.B.I. report, obtained by The New York Times, indicates that Mr. Gray, while the bureau's acting director, had been advised in advance of his testimony of the by-then defunct surveillance operation.

A recent telephone message left at Mr. Gray's law offices in New London, Conn., went unanswered and efforts to reach him today at his home in Stonington, Conn., were unsuccessful.

QUESTION BY KENNEDY

The existence of the wiretaps, which, between May 6, 1969, and February, 1971, involved at least four newsmen and 13 Government officials, was first reported in Time magazine on Feb. 26, 1973, shortly before Mr. Gray began testifying in support of his nomination.

Three days later, Senator Edward M. Kennedy of Massachusetts, one of the committee's nine Democrats, asked the acting F.B.I. head to respond to the report, which both the White House and the Justice Department had rejected as without substance.

Mr. Gray replied under oath that he had examined the F.B.I.'s wiretap surveillance records and found no evidence of any such program, adding that "Mr. Hoover [J. Edgar Hoover, the late F.B.I. director and Mr. Gray's predecessor] is not going to do something like this in the first place."

NIXON APPROVED WIRETAPS

President Nixon later acknowledged, however, that he had approved the wiretaps as part of an effort to halt leaks of classified information to the press and had given joint responsibility for coordinating the effort to Mr. Hoover, Henry A. Kissinger, then the President's adviser on national security and now Secretary of State, and John N. Mitchell, then the Attorney General.

Mr. Gray's assertions that he had found nothing in the F.B.I. files to support the existence of the wiretaps was apparently technically correct. As the F.B.I. report on the matter relates, records on the wiretaps were sent to the White House before Mr. Gray took over the bureau, the result of an internecine struggle between Mr. Hoover and one of his assistants.

But the report, compiled after an internal inquiry ordered last May by William D. Ruckelshaus, the next to take over the F.B.I.'s top post, shows that Mr. Gray was provided with a memo on Feb. 26, the day the Time article appeared, that related the known details of the disappearance of the wiretap records.

The report also notes that Mr. Gray was advised before that date of the circumstances surrounding the disappearance of the records, which included authorizations for the wiretaps and summaries and logs of the overheard conversations.

The records were eventually recovered by Mr. Ruckelshaus from the White House office of John D. Ehrlichman, about two weeks after Mr. Ehrlichman resigned on April 30 as President Nixon's chief domestic adviser.

According to the F.B.I. report, an inquiry ordered by Mr. Hoover had been able to reconstruct much of the surveillance operation in the absence of the missing records, including data on 16 of the 17 individuals whose telephones had been tapped.

This information, judging from the bureau's report, was also available to Mr. Gray before his testimony.

At one point, Mr. Kennedy recalled Mr. Gray's earlier denials of knowledge of the matter, asking, "You said that you had no basis for believing that the Time story had any basis in fact; is that correct?"

STANDS BY TESTIMONY

"That is correct, sir," Mr. Gray replied. "I said I personally checked the record, and that has been my testimony consistently. That is my testimony today."

Asked whether after learning of the Time account, Mr. Gray had felt that he "ought to talk to anybody at the White House about this," he replied, "The White House has already issued a denial. The answer is No, Senator."

During his interrogation, Senator Kennedy noted that Richard G. Kleindienst, Mr. Mitchell's successor as Attorney-General, had declared that neither he nor Mr. Mitchell had authorized any electronic surveillance of newsmen, White House officials or others "as reported by Time."

Did Mr. Gray, the Senator asked, attach the same qualification to his assertion that he had no reason to believe the report had any basis in fact?

"I don't draw any kind of qualification or implication from that at all, Senator," he replied.

"I don't really know what you are talking about—that we are tapping our own telephones, is that really the thrust of this question?

"That practice has never come to my attention. I am trying to imagine how you do it."

GAVE UP POSITION

On April 27, Mr. Gray stepped down as the F.B.I.'s acting head following news reports that he had destroyed certain materials taken from the White House safe of E. Howard Hunt Jr., one of the seven convicted Watergate conspirators.

The baldish, 57-year-old former submarine captain had asked Mr. Nixon to withdraw his nomination from the committee's consideration a month earlier, after it had become clear that he could not be confirmed.

Mr. Gray told the Watergate committee that he had destroyed the Hunt papers, some of which might have been material evidence in the Watergate criminal investigation.

But, he conceded, he had lied both in telling Justice Department officials that he had not read the files before burning them and in telling a member of the Watergate committee that he had destroyed the papers immediately after receiving them. In reality, he had kept them intact for months.

[The Washington Post, Mar. 5, 1974]

Communication Aims of FBI Hit by GAO

(By Susanna McBee, Washington Post Staff Writer)

The Federal Bureau of Investigation wants to take control of the day-to-day exchange of messages among police departments across the country, the General Accounting Office has reported.

Moreover, the bureau does not really know how state and local police are using the computerized criminal-history data that it now supplies them from its own message interchange system at the National Crime Information Center (NCIC) here, the GAO says.

These findings, which seem to raise the specter of the FBI's assuming a big-brother role in handling all kinds of police information, are contained in a report sent last Friday by Comptroller General Elmer B. Staats to Sen. Sam Ervin Jr. (D-NC). The FBI declined comment.

Sen. Ervin's Constitutional Rights Subcommittee of the Senate Judiciary Committee will begin a two-week series of hearings on the issue today. The subcommittee had sought a report form GAO, the congressional investigative arm, on Feb. 21.

Involved in the issue are two separate police communications systems.

One is called NLETS, National Law Enforcement Teletype System, which is run by the states. In 1966 NLETS was set up as a nonprofit corporation to handle administrative messages, such as checks of driver records, prisoner transfer and all-points bulletins between state and local police agencies.

For instance, in January, when the body of a young woman was found in northwest Washington, police discovered a nearby car with Vermont tags, queried Ver-

mont state police over the NLETS system and within seven minutes had a positive identification of the woman, Pan American World Airways ticket agent Barbara L. Meyersburg.

The other system is the FBI's NCIC, which began operating in 1967 as a telecommunications network linking the FBI and state and local police for the exchange of information on wanted persons and stolen property.

Since 1971 NCIC has also been receiving and disseminating computerized criminal histories, which now make up 450,000 of the 4.8 million records the network holds. In 10 years the bureau expects NCIC to contain 8 million criminal histories among 21.7 million records.

A major difference between NLETS and NCIC is that the state-operated system does not maintain records of its communications in a data bank, and the FBI's system does.

Because of the proliferation of criminal information storage and the potential for its misuse, the Justice Department has passed legislation to regulate its use and some members of Congress, including Sen. Ervin, have introduced bills to that end.

Last July 11, FBI Director Clarence M. Kelley asked then Attorney General Elliot L. Richardson for funds in the fiscal 1975 budget to upgrade NCIC's message-switching capability. In that memo, according to the GAO report, Kelley asked for Richardson's concurrence that the bureau has the legal authority to expand NCIC Jurisdiction to the state systems.

On Aug. 6 the department's Office of Legal Counsel said it was arguable whether such authority exists. On Jan. 15 of this year Kelley renewed his request to Attorney General William B. Saxbe and contended that NCIC operation of the central message-switching unit for the states would save the taxpayers money.

On Feb. 1 the Law Enforcement Assistance Administration, a Division of the Justice Department which aids states and cities in improving their criminal-justice systems, wrote Saxbe a memo strongly opposing the FBI proposal. The LEAA argued that states and localities are fully capable of handling their own message systems and that the FBI, as police agency, should not concern itself with other agencies that use NLETS, such as courts and correctional units.

The LEAA-FBI fight goes back to 1969, when the LEAA funded a state-run project with $4 million to develop the prototype of what is now the computerized criminal-history part of NCIC. The LEAA wanted the central computer here to contain only summary data, not complete files, on state offenders, and it wanted to set up a policy board consisting of the FBI, the LEAA and the states.

The GAO report said that the Office of Management and Budget had agreed with the LEAA position in a September 1970 letter to then-Attorney General John N. Mitchell. But Mitchell never passed the OMB recommendations on to either the FBI or the LEAA, and he decided that December to let the FBI take control of the computerized criminal histories, the GAO said.

"Data is not available to indicate how computerized criminal-history information has been used," Staats said in his covering letter to Ervin.

He also noted that with the upgrading of NCIC by the FBI and an LEAA plan to build a satellite telecommunications system for NLETS, the two systems "could result in duplication and unnecessary expenditure of federal funds."

According to a well-placed source, the issues raised by the legislation to regulate use of criminal information and the FBI's bid for preeminence over all criminal information are these:

Who will regulate and control federal, state and local criminal information, intelligence and statistics?

If NLETS is merged into NCIC, what kinds of information will be in it, what kinds of records will be kept and who will receive it?

Should the FBI have a dominant role in operating and regulating for the states key portions of criminal-information systems, including data on the routine operations of police, courts and corrections agencies?

APPENDIX F

FROM SPEECH OF ROBERT D. LILLEY, PRESIDENT, A.T. & T. BEFORE NATIONAL PRESS CLUB, JANUARY 30, 1974

Even a cursory examination of the record will substantiate that, over the years, the Bell System has urged, and argued for, strict protection of its customers' privacy—and argued against invasion of that privacy.

It would take far more time than we have available to us on this occasion to discuss each and every aspect of the problem. So I'll confine myself to one that I know is of immediate concern to the press; namely, the conditions and circumstances under which we disclose our toll (long-distance) billing records to anyone other than the customer concerned. (I say "toll records" simply because those are the only ones that provide specific information as to when and where a call was placed and whence it was directed.)

Our policy has been to provide that information only to the customer or to an appropriate law enforcement or other governmental agency acting under lawful process. The records do not reflect who said what to whom in the course of a conversation or other communication. They couldn't. We don't know that. They do show the originating phone number, the date of the call, the city and phone number called, the time, the duration, and the cost.

Our release of such information has been made only under subpena or, in some instances, when an appropriate, lawful authority (such as a chief of police, for example) has requested it in writing.

That policy has been sustained in the courts and approved by the FCC.

Representatives of the press have expressed the concern, however, that the constraints on such disclosures ought to be tightened even further.

We are sympathetic with that concern. When the reporters' committee for the freedom of the press asked us recently to provide information concerning the release of its members' billing records to lawful authorities, we immediately undertook to do so.

As it turned out, our available records showed only six or seven instances of such disclosure over the past 5 years.

Maybe six or seven are just that many too many. But as we pointed out to the reporters' committee, we have no authority in the telephone companies by which we can judge whether the legal process is being abused by governmental agencies in obtaining the billing records of members of the press—or anyone else.

Given the proper assurances that we would not be acting contrary to the public interest, we would prefer not to reveal anything to anybody about the billing records of our customers.

We are currently studying our procedures once again. We are looking for ways, within the law, to tighten up, if possible, and further enhance the privacy of our customers. We hope we can find ways which will not at the same time be construed as an obstruction of justice.

It may be that this issue will have to be decided eventually by the Congress. But I assure you that the Bell System is going to be on the side of privacy, wherever and whenever the issue is considered.

Now I'm ready for your questions. Thank you.

APPENDIX G

[From the Washington Post, Nov. 18, 1970]

6 GOVERNORS' PHONES INCORRECTLY WIRED

(By Lawrence Meyer)

The American Telephone and Telegraph Company has found that civil defense telephones in the offices of six governors were incorrectly wired so that conversations in the offices could be monitored, but only if the lines were tapped nearby, a company spokesman said yesterday.

The phone survey, begun Tuesday by AT&T after Maryland Gov. Marvin Mandel revealed that his phone could serve as a listening device, uncovered wiring errors in the "hot line" phones in five other states—Delaware, Pennsylvania, Illinois, Utah and Arkansas.

In 38 other states, a company spokesman said, "no wiring errors or conditions that would permit eavesdropping of any kind were found."

The phones in five more states remain to be examined. Where wiring errors have been found, the mistake "is or will be corrected," the spokesman said.

According to Mandel, a private electronics expert making a routine check of his office discovered that the civil defense phone—part of the national warning system installed by AT&T affiliates—was capable of picking up and transmitting conversations in Mandel's office while the phone was cradled. The phone could

not amplify the conversations, however, and any potential eavesdropper would have had to tap the line.

The telephone company said that the phone had been improperly wired but that a safeguard inside the statehouse would prevent transmissions from the cradled phone going any further.

Mandel's electronics expert, Edward Boyle, said that it would be "very difficult" to monitor conversations from outside the statehouse, but that it could be done.

"It would take almost a laboratory to do it," Boyle said. Mandel said he would have the phone moved out of his office.

Boyle said he thought the wiring error was unintentional because if it were deliberate, "it wouldn't be that obvious."

The national warning system is made up of about 1,600 telephones including those in the governors' offices in executive mansions or in statehouses. The governors' phones duplicate those operated by the "state warning point."

These phones are connected to three transmission points of the North American Air Defense Command: At Cheyenne Mountain, Colo., in a two-story underground building in Denton, Tex., and at a classified location "outside Washington." According to the Office of Civil Defense, the system costs about $1 million annually for maintenance and operation.

The phones are special, four-wire circuit devices designed to insure at least one-way transmission in an emergency. A spokesman for AT&T said last night that the wiring error could not in any way be duplicated on normal household telephones, which are differently constructed. Another company official said the phone company is preparing a complete explanation of the error for the public.

Delaware Gov. Russell W. Peterson learned that his phone was capable of eavesdropping after Mandel called him about the Maryland phone.

Pennsylvania Gov. Raymond P. Shafer had his phone checked earlier in the week by the phone company and announced that it had no problem. A spokesman for Shafer said yesterday that Shafer's phone had not been checked since and that he was unaware of any wiring defect.

Arkansas Gov. Winthrop Rockefeller could not be reached for comment.

[From the Washington Post, Nov. 17, 1970]

MANDEL'S "HOT LINE" BUGGED, HE BELIEVES

(By Richard M. Cohen)

Maryland Gov. Marvin Mandel is convinced that a "hot line" telephone in his executive office, supplied by the federal government and similar to those provided about 30 other governors, could function as an electronic eavesdropping, device, his aides said yesterday.

Sources close to the governor said, however, that he does not know whether his phone was inadvertently wired so that it served as a listening device, or was deliberately planted for that purpose.

A similar situation, it was learned last night, was found in the office of Gov. Russell Peterson of Delaware.

Existence of the devices is reported by syndicated columnist Jack Anderson in today's Washington Post and other papers. Anderson reports that he heard the phone in Mandel's office transmit conversations even while it was hung up.

Anderson says that "an estimated 30 other governors have similar phones that have been rigged for eavesdropping." He does not say who was responsible for the alleged rigging, but reports that "some think it must be the FBI. Others say the CIA is the most likely culprit."

Herbert G. Klein, President Nixon's director of communications, last night called the charge "ridiculous."

A few governors reached by The Washington Post last night said they had had special checks made of their phones after learning of Anderson's charges, but had found no problems. Others said they knew nothing about it.

The device on Peterson's phone, it was learned last night, was discovered when Mandel dispatched an electronics expert to Delaware.

Peterson's phone, like Mandel's, sources said, proved to have been wired so that even when it was hung up it continued to transmit a signal. Neither Peterson nor Mandel could be reached for comment last night. Mandel, however, has scheduled a press conference for this afternoon, reportedly to discuss the telephone situation.

In Baltimore, the president of the C&P Telephone Co., Thomas E. Bolger, confirmed that the company had been summoned to check Mandel's phone.

Mandel's phone, which Bolger said was installed about 10 years ago, had been incorrectly wired so that only one of two systems to forestall eavesdropping was functioning.

However, Bolger said, the second system was functioning and "definitely did prevent any signal from going beyond a locked and guarded equipment box in the basement of the statehouse."

In other words, Bolger said, it was possible for Anderson to hear the conversations in Mandel's office that the phone in its cradle was transmitting, but only if the tap was applied in the Annapolis statehouse. The signal, he said, could not travel beyond that point.

It could not be determined last night where Anderson had tapped the wire. He was reported en route Oregon and could not be reached for comment.

In Washington, a Pentagon spokesman said the National Warning System "is a party line system and like any other telephone system could be bugged.

"All precautions against sabotage, and to make the system as secure as possible are taken," the spokesman told the Associated Press. "However, its purpose is quick warning and it is not intended as a secure system. We are aware of no past instances of bugging."

In response to Anderson's column, Georgia Gov. Lester Maddox yesterday called in investigators and then crawled under his desk to see for himself. He found nothing wrong.

In Washington State, a spokesman for Gov. Dan Evans said that his "hot line" had been examined and cleared by workmen from Pacific Northwest Bell. "We haven't laid it to rest," press spokesman Neil McReynolds said, "but we're satisfied so far."

In Helena, Mont., Gov. Forrest A. Anderson reported that he had not heard of the Anderson column and had not used the phone in two years. But, he added, "nothing surprises me anymore."

Mandel, according to his aides, has never used the phone, which sits on a table behind his desk. The governor, whom one aide described as "nearly paranoid" about electronic eavesdropping, did not have the phone checked for a bug until recently, when he acceded to the wishes of a new state investigator.

Mandel, according to aides, revealed his suspicions to very few members of his staff. According to one staff member, "no one knew the complete picture."

Maryland secretary of state and lieutenant governor-elect Blair Lee III—one of Mandel's closest advisers—said he knew nothing about the alleged bug.

"You mean I've been sitting in that room for the last 21 months and Richard M. Nixon is on the line?" Lee said.

Reliable sources said Mandel personally examined the phone and the suspect microphone. The "mike," these sources said, is the standard one found in all Bell System phones. This one, however, had been wired differently.

Mandel, these sources added, became very excited when he discovered the suspected "bug." His office is routinely canvassed for bugging equipment and he was reportedly dismayed that the "red phone" had escaped surveillance.

[From the Baltimore Sun]

5 "HOT" LINES ARE FLAWED

MANDEL SHARES PHONE WOE WITH 4 OTHER GOVERNORS

(By G. Jefferson Price 3d)

The American Telephone and Telegraph Company reported yesterday the Civil Defense telephones of at least four other governors were wired in the same improper manner as that of Governor Mandel, who said his "hot line" could be used to monitor conversations anywhere in his private office.

The telephones connect the nation's governors with various Civil Defense headquarters in the event of a national emergency.

37-871 O - 74 - 5

UNORTHODOX WIRING

A company spokesman in Washington said that out of 38 telephones the company checked in statehouses across the country including Governor Mandel's, [five] were improperly wired. The other four telephones are those of the governors of Delaware, Pennsylvania, Utah and Illinois.

The company spokesman blamed the unorthodox wiring on the failure of those who installed the phones "to properly follow wiring instructions."

Telephone experts still have 10 Civil Defense telephones to check, for they are looking into the Civil Defense connections of every state except Alaska and Hawaii, regardless of whether the apparatus is located inside or outside of a governor's office.

MANDEL TRIGGERED PROBE

The nationwide investigation was launched by the company under orders of the national Civil Defense headquarters in the Pentagon after Governor Mandel discovered that the wiring in the phone caused the apparatus to act as a permanent transmitter which could be monitored from within or outside the State House.

The Governor and a private investigator who discovered the wiring said the receiver was transmitting even when it was on the hook.

However, telephone company officials kept insisting that the transmissions could go no further than a locked terminal box in the basement of the State House.

WIRING CORRECTED

The telephone company spokesman said that the improper wiring in the five Governors' telephones had been corrected yesterday.

Governor Mandel intends to move the hot line out of his office into the State Police room in the State House "Where someone can immediately contact me if it rings."

[From the Washington Post, Nov. 17, 1970]

THE WASHINGTON MERRY-GO-ROUND

MOST OF GOVERNORS' OFFICES BUGGED

(By Jack Anderson)

The most confidential conversations of the nation's governors can be overheard at any point along an emergency telephone system that links their private offices with Civil Defense headquarters.

It has just been discovered that the red emergency telephones in most governors' offices have been transformed into secret listening devices. The microphone in each receiver will pick up conversations in the room when the phone is on the hook.

I personally listened to a conversation that an electronics expert, using simple wiretap tools, easily picked up in the office of Maryland's Governor Marvin Mandel. The conversation was transmitted through the emergency telephone under the governor's desk.

An estimated 30 governors have similar phones that have been rigged for eavesdropping. These insidious phones connect into a hotline, which enables Civil Defense to have instant communications with the governors in a national crisis.

The hotline, referred to in classified documents as "The Special Service Line for Civil Defense," is supposed to be strictly hush-hush. It is difficult, therefore, to get any official information.

From unofficial, but reliable sources, this column has established the following facts:

HOT LINE TAPPED

The emergency phones were installed about 15 years ago as part of a secret network whose main terminal is located in Colorado Springs. The network links most governors who can be called in case of an emergency.

The receivers were wired in such a way that they can pick up everything said in the governors' offices. Some officials insist the wiring was an "innocent mistake." But electronics experts say flatly there was no possibility of a mistake.

They say the phones must have been deliberately rigged to eavesdrop on the governors.

Secrecy is used to cover up the identity of those responsible for transforming the governors' phones into hidden mikes. Some officials say the phones were wired by the American Telephone and Telegraph Company. Others say the rigging was done by the federal government. AT & T would make no comment, except to say all information would have to come from the customers.

Even more mysterious is the identity of the listeners. Some think it must be the FBI. Others say the CIA is the most likely culprit.

Governor Mandel was the first to discover his emergency phone was bugged. He angrily summoned telephone officials and demanded to know who was responsible. This column got wind of his protests and questioned him.

He confirmed that an electronics specialist had checked the red phone under his desk and found it was wired to pick up every sound in the room.

AGNEW'S OFFICE BUGGED

He said his predecessor, Spiro Agnew, had discovered a hidden mike in the governor's office before moving up to the vice presidency. As a result, Mandel begin checking the office regularly for mikes and wiretaps after he moved in.

The red emergency phone had been ignored, he said, on the assumption that the secret hotline must be secure. But last month, a new electronics expert insisted upon checking it and demonstrated how the emergency phone functioned as a secret transmitter.

Outraged, he called in the telephone people and made other confidential inquiries. He said the telephone officials not only acknowledged that his special phone was bugged but said all emergency phones were wired the same way. This would mean all the governors on the hotline had bugged phones, they told him.

Mandel could hardly believe it. To satisfy himself, he arranged to send an electronics specialist to check the emergency phone of a neighboring governor. Mandel said the governor, whom he declined to identify, was also shocked to find how the phone transmitted all the conversations in the office.

EMERGENCY RINGS

Meanwhile, Mandel ordered the microphone removed from his emergency phone. He said the phone had never rung during his 22 months as governor and probably hadn't been used since it was installed. But the day after he removed the microphone, the phone rang.

He happened to be out of the office, but his personal secretary, Grace Donald, confirmed to this column that there had been six short, sharp rings on the emergency phone. Since only the governor is supposed to answer the hotline, she didn't pick up the phone.

I asked the governor's permission to tap into the hotline to test for myself whether I could overhear what went on inside his office. He assigned Lt. Norval Cooper, a state trooper trained in electronics, to accompany me. The microphone was screwed back into the emergency phone, and Cooper used common wiretap tools to plug into the hotline at a nearby switchbox. Every word spoken in the governor's office was distinctly audible. By using a voice-activated recorder, the full conversation could easily have been taped.

[From the Washington Post, Dec. 4, 1970]

COLUMNIST'S REPLY ON PHONE BUGS

(By Jack Anderson)

I have received a number of letters from editors about my recent column about the governors' "bugged" telephones. Although most comments were favorable, editors may be interested in the critical analysis of the Washington Post's Richard Harwood. Here are the excerpts relating to the column, followed by my response:

". . . Back on the comic page last Tuesday (Nov. 17) the Washington Post carried a column by Jack Anderson under a headline that read: 'Most of Governors' Offices Bugged.' The column reported that all governors have 'hotline' phones that enable them and federal civil defense authorities to communicate in times

of national crisis, that 'most' of these phones are 'bugged,' and that the alleged culprit may be either the CIA or the FBI. The column seemed to be based on information supplied by Governor Marvin Mandel of Maryland.

"It caused something of a stir in the newsrooms of The Post and The Baltimore Sun and led to lengthy stories, some of them on page 1. As it turned out, no evidence came to light that any governor's phone was 'bugged,' Mandel's included.

"On that evidence one can only conclude that the Anderson column made much out of little or nothing, that it then became the subject of a great volume of 'news,' that the implication that the federal government was eavesdropping on 'most American governors' (or on any of them) was false, and that the newspapers in this case constructed a larger view than the facts at hand' would support. . . ."

ANDERSON'S REJOINDER

Here is my response to The Washington Post.

"Richard Harwood's critiques of the press, pointing out the errors of our ways, have been a worthwhile contribution to good journalism.

'He said newsmen often rush into print half-cocked. He cited various examples, including my story about the governors' 'bugged' telephones.

" 'The column seemed to be based,' he wrote, 'on information supplied by Governor Marvin Mandel of Maryland.' The suggestion that I spoke only to Governor Mandel is wrong.

"Harwood concluded that, although six governors' phones had been 'wired improperly,' none of the phones apparently had been bugged. He may be right. He may also be wrong.

"The best way to avoid errors, I have found, is to talk to people before writing about them. I would have been pleased to discuss my reporting of the telephone story with Harwood if he had cared to check with me.

"The column in question illustrates how difficult it is to break sensitive stories. Much of the information, which now provides Harwood with such excellent hindsight, was withheld from me by the same sources who later made the information public.

"I spent about three weeks checking the story, I talked to three electronic experts familiar with eavesdropping techniques. I called upon Governor Mandel who, at my request, permitted me to listen for myself to conversations picked up by the emergency phone in his office.

"The telephone company spokesman refused any comment, but declared all information would have to come from the customers.

"After my column reached the desks of more than 600 editors, the telephone company began issuing statements all over the country. In Delaware, for example, a spokesman said Governor Russell Peterson's emergency phone had been checked and nothing amiss had been found. This statement was quietly retracted after the company learned that Peterson's phone had been checked by an independent expert who had found it was transmitting every word spoken in the governor's office.

"Governor Mandel told me a telephone company representative had advised him that the emergency phones in 48 governors' offices were all wired identically. The White House, in response to my inquiries, said only 30 governors were linked by the emergency system.

"After my column hit the headlines, telephone officials apologized for refusing to comment earlier and invited me to their offices for a 90-minute briefing. They presented a persuasive case that the conversations picked up by the mis-wired phones couldn't have gone beyond the state houses.

"Yet an independent expert still insists that the conversations could have been intercepted anywhere on the network; also that anyone familiar enough with the technology to wire a telephone could not have turned the governors' phones into transmitters by mistake.

"Meanwhile, the telephone company conducted its own inspection of the governors' emergency phones. With all respect, this was a bit like the fox inspecting the chicken coop. It is noteworthy, at least, that the only two phones checked by outside experts were found to be mis-wired. The telephone company, in acknowledging that six governors had mis-wired phones, also confessed to a startlingly high rate of error.

"Of course, Harwood is entitled to accept the telephone company's version, just as I should be entitled to be suspicious."

[From the Washington Post, Sept. 24, 1971]

NEW BUG ALL EARS—SNOOPS THROUGH HUNG-UP PHONE

(By Ronald Kessler)

A breakthrough in electronic listening devices permitting any home or office to be bugged and tapped without entering it was disclosed by a wiretap expert at a conference of federal law enforcement and security investigators here yesterday.

The device can be placed anywhere on a line leading to the phone to be tapped—on telephone poles, in underground cable vaults, or in telephone company switching offices miles away. It picks up both telephone calls and conversations in the room where the phone is installed, even when the receiver is on the hook.

This feature, said government bugging experts who were queried yesterday, would make it unique.

According to Clyde Wallace, a bugging equipment manufacturer who disclosed the development, the device is already being used by two federal investigative agencies.

Wallace described the device at a symposium of the Association of Federal Investigators at the Mayflower Hotel. Others on the three-day agenda were officials of the Justice Department, Federal Bureau of Investigation, Bureau of Narcotics and Dangerous Drugs, and Treasury Department.

Spokesmen for the FBI and Central Intelligence Agency declined yesterday to comment on whether their agencies were the ones alluded to by Wallace in his speech as using the device.

The FBI has primary responsibility for court-approved wiretapping, which is interception of telephone calls, and bugging, which is monitoring of room conversations through electronic devices. The CIA conducts extensive electronic surveillance outside the U.S. but is not supposed to operate domestically unless the matter is related directly to its foreign intelligence work.

After his speech, Wallace expressed surprise and some dismay that a reporter had been present while he talked.

Other devices, called infinity transmitters or "harmonica" bugs, can bug and tap phones simultaneously, but they all require physical entry to permit rewiring of the phone or installation of a bug.

Government bugging experts interviewed yesterday said no public mention had been made before of a device that would not require entry, and several expressed surprise at the development.

However, Bernard Fensterwald, former chief counsel of former Sen. Edward E. Long's Subcommittee on Administrative Practice and Procedure, which held extensive hearings on government surveillance, said he has had information for some time from nonpublic disclosures during the committee's investigation that security agencies, such as the CIA, use such a device.

Wallace earlier this year was investigated by the FBI to determine if any devices sold by the Spy Shop, which he owns, violate federal wiretap laws, according to FBI sources.

Wallace said he operates strictly within the confines of the law. The outcome of the FBI investigation could not be learned yesterday.

Asked about the propriety of an FBI official appearing on the same agenda with the target of an FBI probe, an FBI spokesman said the FBI representative appeared on a different day than did Wallace. Other than that, he said, the bureau would not comment. He declined to answer any questions on the new device.

During the speech, however, Wallace described it as the first method for simultaneously tapping a phone and bugging the room where it is installed without tampering with the phone or even going near the premises.

To tap and bug a phone, he said, the device is placed anywhere on the telephone line running to it. It then emits a radio frequency, which trips a switch in the phone. This switch normally prevents conversations in the room from traveling over the telephone wire. When it is bypassed by the signal, the phone becomes an open microphone, transmitting both room conversations and telephone calls to the listener.

Normally phone calls can be made while the device is in operation, according to Wallace, who said he is developing his own version of the device.

Last year, a cut-off switch was found by an electronics expert to be bypassed on the civil defense telephone in the office, of Maryland Gov. Marvin Mandel, making the phone capable of transmitting conversations from Mandel's office. The telephone company attributed the situation to a wiring error.

APPENDIX H

M-220 Remote Observing (REMOBS) System

Telephone companies are able to employ observing "REMOBS" systems, which only require the ordinary push-button telephone instrument for access. Two major types of this instrument are on the market--- available to and used by telephone companies and various other kinds of businesses, such as hotels, airlines, department stores, and credit bureaus.

One version of this REMOBS equipment is the M-220 system, made by Tel-Tone Corporation of Kirkland, Washington. The M-220 and a more advance M-240 system are ordinarly advertised in Telephony magazine, the weekly trade journal. The ad in the issue of September 10, 1973, which is attached, indicates that Tel-Tone specializes in making equipment adapted to the "touch-tone" switching system.

Early in 1972, some CWA craftsmen employed in a Bell System company in the midwest discovered the existence of an M-220 system. Immediately thereafter, according to the report of the CWA field staff, the M-220 was removed. The technical information also included with this section has come to CWA via confidential channels.

Another form of remote observing is with the Alston Subscriber Dial Service Measuring System, models 370/389, manufactured by the Alston Division of Conrac Corporation, located at Duarte, California. The Alston system is capable of holding sensitive information on a display panel and preserving it in a tape recorder. The information would include calling number, called number (including area code), duration of call and other items. The sales literature also notes that the Alston system provides a tape recording of the conversation if desired.

What is especially significant about the Alston system is that it effectively negates the remarks of AT&T President Robert D. Lilley, made January 30, 1974, at the National Press Club (p. 9 of his prepared text). Lilley said that toll records are the only ones able to provide specific information as to telephone calls, such as calling and called number, duration of call, time and date. The information on the Alston system shows the same information available, on both local and toll calls, on the selected telephone lines.

SERVICE OBSERVER'S GUIDE FOR

M-220 SERVICE OBSERVING SYSTEM

INTRODUCTION

The purpose of this guide is to explain the general operation of the M-220 Service Observing System and how to use it. Your ability to use the system properly will make your task of observing call conditions much easier.

GENERAL DESCRIPTION

The M-220 Service Observing System provides a means of observing service on lines or trunks from a remote location. All that is required is a telephone equipped with a TOUCH TONE [R] dial. The system consists of an automatic answering unit and various switches to select the trunk to be observed.

The service observing unit is accessed by dialing a regular telephone number. It is connected to the telephone lines to be observed in such a manner that you will monitor the conversation without being heard yourself.

[R] AT&T Registered Trademark

ACCESSING THE SYSTEM

Dial the telephone number assigned to the system you wish to access. When the line is reached, the unit will automatically answer the call. You will hear very little, if any, ring back tone. Once connected, a distinctive answer tone will be heard for approximately two seconds. If you do not hear the tone, release the call, wait 15 seconds and place the call again.

SECURITY DIGITS

In order to prevent unauthorized persons from using the system, it is necessary for you to dial into the unit a locking Security Code. The code consists of two digits. You must touch dial the Security Digits within five seconds after receiving the answer tone. All digits touch dialed into the M-220 must be held down at least one second. This slow dialing is necessary to prevent voice and other extraneous sounds from interferring with operation of the M-220. Should you not dial the code in time, the unit will automatically disconnect and the call must be placed again. If the Security Code is dialed before the time out period, the Service Observing Unit will be locked to your call. Unless your system is equipped with a Trunk Group Selector, you will hear a low level Idle Tone. This tone indicates that you will be connected automatically to the next incoming call.

RELEASING FROM THE OBSERVED LINE

When you no longer wish to observe a particular line you must dial the second digit of the Security Code (Reset Digit) to release the connection. You will then be able to observe the next incoming call.

DISCONNECTING FROM THE OBSERVING SYSTEM

When the M-220 automatically answers your call, it attaches itself to the Central Office switching system. Once the Security Code has been dialed, the M-220 locks to the Central Office switching equipment until you release it. This is done by touch dialing a disconnect digit. Should you fail to touch dial the disconnect digit, the next attempt to access the system will receive a busy tone. A second method of restoring the M-220 is to dial another telephone number specifically assigned for the purpose of releasing the system. After dialing the release number and hearing it ring, hang up and redial the M-220 on its assigned access number.

If the Security digits are not dialed, the disconnect digit is not necessary since the M-220 will automatically disconnect in five seconds.

UNUSUAL SITUATIONS

The M-220 Service Observing System is designed to give years of trouble free operation. Experience has shown that

ALSTON
SUBSCRIBER DIAL SERVICE MEASURING SYSTEM

Models 370 and 389

- 100 trunk capacity, continuous monitoring
- Live or recorded service observation
- Automatic selection of outgoing calls
- Displays trunk I.D., dialed number, elapsed time
- Audio output of call events
- Portable or dedicated
- 100% solid state and modularized construction

The Alston Model 370/389 is an extremely versatile system which allows quantitative grading of subscriber dial service. In addition, the system may be used to determine developing trouble patterns and to provide a means by which documented quality of service data may be generated for interested regulatory agencies.

When connected to subscriber lines or trunks, the system will monitor up to 100 of these circuits and, if not currently engaged in an observation, will automatically select for observation any new outgoing call. The system will visually display the number being called, the elapsed time between various circuit events and the identity of the circuit being observed. Additionally, an audio output is provided to allow for operator determination of various circuit conditions, such as, trunk busy, line busy, don't answer, no ring, and wrong number.

Extreme versatility is an inherent characteristic, as the system will interface with crossbar or step-by-step type systems and will accept dial pulse, touch tone, multi-frequency signaling or a combination of D.P. and either T.T. or M.F.

Due to its modular design, the system components may be arranged for portable or dedicated installation and data may be collected in a live or recorded mode with local or remote readout. This modularized solid-state design, coupled with a variety of options and size configurations, insures that the user will initially obtain maximum price performance, and at the same time, allows the system to grow as the user's requirements grow.

THE SYSTEM

The system consists of three basic elements with various modes of operation available in each element. These elements are:

The Call Selector (Model 370)

Located in the switchroom and used to interface to the circuits to be monitored, to sense and select new outgoing calls, and to identify, decode, and format the call data.

The Transmission Medium

Used to accept data from the call selector and to record the data for later playback or to transmit the data to the local or remote service observation quarters.

The Service Monitor (Model 389)

Located in the service observation quarters, this unit provides the operator a visual display and audio output of the call events.

These system elements may be combined into a number of configurations, as shown in Figure 1.

The "live" configurations are generally used in metropolitan areas or in areas where offices are geographically clustered and where the observation call volume within an office will generate 40 to 50 observations per hour.

The "record" configuration is generally used in low observation volume offices, in offices widely scattered geographically, or where a permanent, taped record is desired.

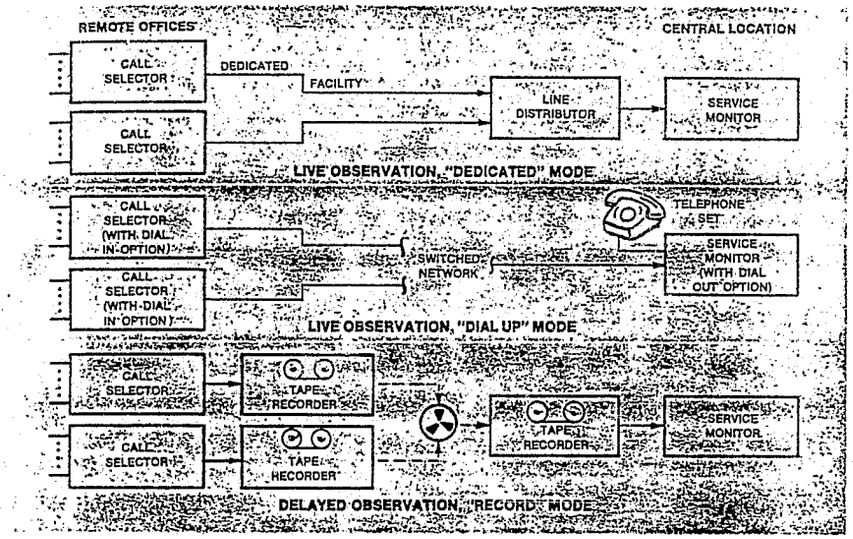


FIGURE 1. TYPICAL DIAL SERVICE MEASURING SYSTEMS

THE CALL SELECTOR MODEL 370

The call selector, as its name implies, is an automatic unit designed to simultaneously monitor a number of trunks and to select the next trunk offering a new outgoing call.

Utilizing modular construction, the Model 370 is equipped to handle 50 trunks. Capacity for an additional 50 trunks may be added at any time with an expansion module which mounts within the standard card file package. The unit is supplied with brackets which allow mounting in either a standard 19-inch or 23-inch relay rack, or the unit may be mounted in an accessory carrying case for portable operation.

When not currently engaged in observation, the call selector automatically scans the tip-ring and sleeve connections from each trunk. When a trunk becomes busy with a new outgoing call, the unit will select it for observation.

Output Modes

The Model 370 offers two modes of data output. These are "live observation" output and "recorded observation" output. In the live configuration, the call selector offers observations to a remote or local Model 389 Service Monitor over either a dedicated pair or a dialed-up connection. In the record configuration, observations are recorded on a magnetic tape unit under the control of the call selector and the observations may then be played back to the service monitor at a later time.

Trunk I.D.

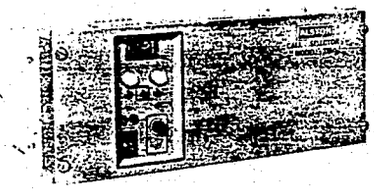
After a trunk has been selected for observation, the call selector identifies the trunk by displaying a two digit number on a front panel readout. In addition, this information is forwarded to the service monitor for visual display on the service monitor readout.

Incoming Call Rejection

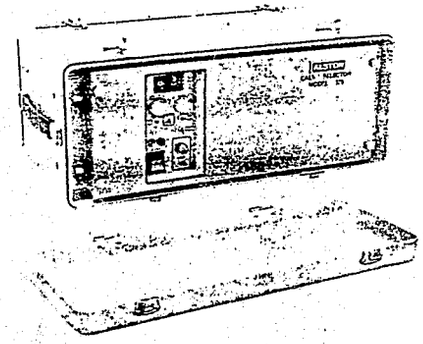
To optimize the number of calls sampled and to preclude partial observations, the unit has built-in circuitry that will cause the call selector to ignore trunks with incoming calls and to allow selection of only those trunks that present an outgoing or originating call.

Dialed Number Detection

After a trunk has been selected for observation, the number being dialed by the subscriber is detected and forwarded to the service monitor (or tape recorder) for display. The system will process dialed numbers coded in dial



Model 370 CALL SELECTOR



Model 370 CALL SELECTOR IN PORTABLE CASE

pulses, touch tone, or multi-frequency or combinations of the three.

Call Time Out

The unit employs a highly stable and accurate crystal controlled clock used to time out the observation and to allow the unit to process additional observations. Two time out intervals are provided.

The first time out interval is fixed and will cause the call selector to release the observation 12 seconds after call supervision (called party answers).

A second variable time out is also available which may be set from "01" to "99" seconds in 1-second increments may be set to infinity (no time out). When in the manual mode or if supervision is not received in the auto mode, the unit will release the observation after the number of seconds set on the variable time out thumbwheel switch. When set to infinity, the call selector will continue to monitor the call until call termination or until the service observation operator manually releases the observation. If the observation is being recorded and the unit is under time out control that exceeds 15 seconds, then a 1000 Hz beep tone may be enabled to notify the subscriber that the call is being observed.

Intermittent Studies

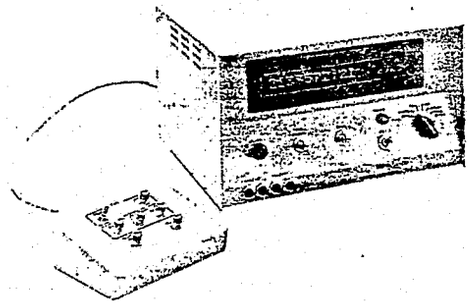
Frequently it is desirable to limit observations to peak traffic periods or to only certain days of the week. To accommodate this requirement, the call selector may be equipped with an accessory 14-day study timer which may be set to turn the unit on and off at different times during the day and on selected days of the week.

Installation

For dedicated installations, the unit may be rack mounted in the switchroom and hard wired to the trunks to be monitored. In portable applications, the unit is fitted with an accessory ruggedized aluminum carrying case and is connected via patch cables to prewired trunk patch panels mounted in the office under study. For stable operation, the unit is powered from 48V office battery and is totally immune to switchroom electrical noise.

THE TRANSMISSION MEDIUM

Live or recorded observations with local or remote data display are available configurations in the Alston system. Available configurations pictured in Figure 1 allow the user to gather data in the switchroom through a call selector with live service observation analysis, via dedicated or dialed-up facility, at a remote location. The system may also be configured to record the data in the switchroom on magnetic tape for playback at a later time through the service monitor. Alston's Sales Engineers will be happy to work with the user to provide the configuration best suited to his particular application.



Model 389 SERVICE MONITOR

THE SERVICE MONITOR MODEL 389

Trunk I.D., dialed number information and audio call events data are all forwarded to the Model 389 Service Monitor for decoding and display and for analysis by the service observer.

The all solid-state Model 389 consists of a 16-digit display, plus operating controls, in a sloping panel desk cabinet. The 16-digit solid-state readout displays numbers coded in dial pulse, touch-tone, or optionally multi-frequency. These numbers are received directly from a call selector or from a previously recorded tape. The unit also reproduces voice circuit information allowing the operator to measure the quality of service being observed. In addition to the called telephone number, the readout displays the elapsed time, in seconds, of various circuit functions, such as dialing period duration and call switching duration. The display may be frozen at any instant to allow easy notation of elapsed time. Also displayed, at the end of the observation, is the I.D. of the trunk being observed.

A selector switch on the monitor's front panel may be set to Dial Pulse (DP), Touch Dial (TD), Multi-Frequency (MF), DP and TD, or MF and DP, depending upon the type of calls to be monitored. Each type of signal can be decoded by the monitor for display. An accessory keypad contains a recorder start/stop key and a pushbutton rewind control; clock start, stop, and hold buttons, a button which resets the display; and a button which releases the current observation and allows the call selector to proceed to another. The face of the monitor also includes a volume control and a phone jack for connection of one or two standard 600 ohm headsets.

For live observation, the service monitor may be connected directly to the local or remote call selector via a single dedicated DC facility. The unit may also be connected to a remote call selector through the use of the switched network. This configuration may be easily implemented by using the dial-up options available on the 370/389 and by using a standard telephone set connected to the service monitor.

In addition to live observation, playback of previously recorded data may be observed through the use of an accessory magnetic tape recorder.

ORDERING INFORMATION

Model 370-50 Call Selector

50-trunk call selector unit with 19" and 23" rack mounting brackets, power cord and instruction manual.

Model 370-100 Call Selector

Same as Model 370-50, but equipped with a 100 trunk input capacity.

APPENDIX I

"Mail Cover"

Massive abuses of the right to privacy of the individual exist in the technique of "mail cover," a process by which the U. S. Postal Service (ex-Post Office Department) cooperates with other agencies.

Since 1965, several Congressional inquiries have been instituted, none resulting in legislation. However, since two inquiries are in the current Congress, legislation would be possible in 1974.

The most recent examples of mail surveillance were reported in the press in August. The Chairmen of the Federal Communications Commission and Federal Power Commission gave orders that all Congressional mail except that addressed to individual Commissioners was to go to the Chairmen's office for opening and processing.

The Investigating Subcommittee of the Senate Government Operations Committee, has launched an inquiry into the practice; further hearings are expected.

The Subcommittee on Postal Facilities, Mail Labor-Management of the House Post Office and Civil Service Committee began its own inquiry into the wider question -- mail cover use by all Government agencies -- to uncover abuses.

In 1965, Senator Edward V. Long directed a major inquiry into privacy matters, a major portion of the hearings devoted to mail cover use.

Because of the 1970 domestic surveillance plan advocated by the White House and brought to light during the current hearings on the Watergate scandal, Members of Congress have begun asking questions about the serious implications of the mail cover practice. The Congress should fully pursue the line of inquiry.

Mail cover, as now defined, involves the recording of return addresses and descriptions of pieces of mail addressed to individuals or businesses

or groups. The mail is not normally opened, especially the first-class pieces.

However, the advances of electronic technology promise that future mail covers will be usable to read the actual content of letters, in a further deterioration of individual liberties. The technology for this technique is already in existence; the system has been proposed.

Chairman Moorhead's Subcommittee in November 1972 disclosed the existence of the "Big Brother" study prepared by the Office of Science and Technology at the direction of John D. Ehrlichman, then chief Domestic Adviser to President Nixon.

The OST study described the process of "Electronic Mail Handling," with the justification that in a few years, the Postal Service will be unable to process the ever-growing volume of "hard copy" mail. In the EMH system, an outgoing letter is transmitted electronically. A machine at the receiving-end Post Office would print the letter and insert it into an envelope for regular mail delivery. However, the OST study refers only in passing to the problems of privacy of first-class mail matter. It does not discuss the ease with which the FBI or other agencies which would tap into the computer system could establish a mail cover on either the sender or receiver of the letter. The "Big Brother" study of OST, officially entitled "Communications Needs for Social Needs: Technological Opportunities," also notes that the FBI and Department of Justice will be part of a nation-wide computerized communications network.

The Electronic Mail Handling process is already in existence, as one of the tariff offerings of Western Union Telegraph Company known as "Mailgram." A minor adaptation of "Mailgram" is the only requirement for instituting EMH, in one form contemplated. The other basic form of EMH is for use of optical scanners, which again exist and are under continuing development. Receiving machines in Post Offices currently used for "Mailgram" perform the same work as envisioned in the EMH system.

37-871 O - 74 - 6

[From the Wall Street Journal, Aug. 28, 1973]

Open Letters

SURVEILLANCE OF MAIL BY INVESTIGATORS RAISES THE QUESTION OF ABUSE

CONGRESSMEN, OTHERS CHARGE INVASION OF PRIVACY, FEAR EXPANSION OF THE PRACTICE

A Questionnaire for a Rabbi

(By Les Gapay)

WASHINGTON.—Amid a Christmas mail rush a postal truck here was robbed of $382,000. Within a few weeks several suspects were arrested, and they gave authorities the name of an accomplice who had fled the country.

Postal inspectors secretly kept under surveillance all the personal mail to and from the fugitive's friends and relatives, painstakingly logging the names, return addresses and postmarks on all the envelopes. Sure enough, one day a letter arrived from Ottawa bearing as part of the return address an alias that police knew the suspect had used in the past. With Canadian cooperation the man was extradited to the U.S.; he was convicted and went to prison.

The snooping technique that made this international catch possible is a "mail cover," a little-known but oft-used investigative tool prized by federal law enforcers. Mail covers have helped track down suspected narcotics dealers, gamblers, smugglers and tax evaders, among other criminal types. Two hundred or more may be in operation in the U.S. at any one time. Chief Postal Inspector William J. Cotter hails the mail cover as "one of the greatest, cheapest, simplest techniques to find out leads."

But some others, including Congressmen and civil libertarians, aren't at all enthusiastic. They detect a Watergate odor; the domestic intelligence-gathering plan approved and then quickly disapproved by President Nixon in 1970 called for, among other things, expanding use of mail covers from criminal cases to include monitoring of radical groups.

BIG BROTHER ON LOOSE?

Questions are also being raised about possible big-brother scrutiny of the mail of individuals outside the political arena. When Federal City College Dean Joseph O. Paige was indicted here recently for fraud, his attorney complained in court that the defendant's mail had been tampered with during the government's investigation of the case. The lawyer presented to the court a letter sent to Mr. Paige that he said had been opened and initialed by a postal official prior to delivery. The court has asked the U.S. attorney handling the case to determine whether it had been opened and, if so, why.

The Postal Service says it has investigated such charges but has found no evidence of wrongdoing. Certainly evidence of illegal acts is hard to come by, but a look at what the Postal Service and other federal agencies do quite legally in keeping mail under surveillance is something of an eye-opener. In essence, the only mail that can't legally be opened by one agency or another without special court permission is domestic first-class mail—mainly letters.

The Postal Service has authority to open all other classes of mail, including circulars, packages, publications and books, as part of a criminal investigation or to make sure proper postage is being paid. The Bureau of Customs can do even more: open all mail, including letters, coming from abroad to make sure that duties aren't evaded and that such contraband as drugs or firearms aren't enclosed.

Moreover, domestic letters may be opened through a special search warrant granted by a federal court to a law-enforcement agency. Postal officials say such cases number only 10 or 12 a year nationwide.

A typical search-warrant case is recounted by a former federal attorney: An informer notified authorities that some hashish would be mailed to a certain individual. The suspect's mail was monitored; when a suspicious packet was spotted, a warrant was obtained, the letter was opened, the contents confirmed, the envelope resealed and the letter returned to the mail stream. After it was delivered, FBI agents moved in to arrest the recipient.

More common, and equally controversial, is the mail cover. The job is handled by postal inspectors but often at the request of the Federal Bureau of Investigation, Internal Revenue Service, Central Intelligence Agency, Secret Service or some other federal, state or local police or prosecuting agency. Most officials involved are reluctant to talk; one Justice Department lawyer who serves on a "strike force" attacking organized crime says, "I don't want to give away our tactics." When first asked, a public-relations-conscious spokesman for the Postal Service, Hank Lewis, insisted that mail-cover operations ended several years ago.

But Mr. Cotter, head of the Postal Inspection Service, confirms that mail covers do exist. He says about 200 are in operation at any one time; each can include the surveillance of mail of many individuals. Not only are all data appearing on all the covered mail recorded, but the contents of other than first-class mail are frequently checked. About 95% of all the covers are used in criminal investigations and the rest in "national security" cases, according to Mr. Cotter. He says he and his colleagues find them most effective in combating crime.

Through a mail cover, a postal inspector in Indiana helped nail a swindler who wrote to business saying it was time for them to renew their ads in his newsletter. In fact, they hadn't advertised previously, and the newsletter was a phony sent only to advertisers. One renewal notice was sent to a hardware store that had been in business only a few days. The miffed owner notified postal inspectors; a mail cover on the con artist yielded the names of hundreds of his unsuspecting victims who later filed complaints.

OPENING OF MAIL, TOO

Moreover, government mail surveillance routinely goes much further, regularly including opening of nonletter mail in criminal investigations and occasionally extending to opening of letters with court permission. These "normal" practices, some of which have been expanded during the Nixon era, now are raising invasion-of-privacy complaints. Former Postmaster General J. Edward Day, now a Washington lawyer, declares: "Opening mail is a poor idea, with a court order or otherwise."

But howls of protest may grow much louder within the next few months. For charges are being investigated, by Special Prosecutor Archibald Cox, by the Senate Watergate Committee and by a House Post Office subcommittee, that mail surveillance may have been misused for political purposes during the 1972 presidential campaigns, that letters may have been illegally opened.

Democratic Rep. Charles Wilson of California, chairman of that postal subcommittee, has instructed his staff to investigate reports that the mail of Democratic presidential candidates was tampered with last year by postal employees. In a letter to Rep. Wilson, Sen. Hubert Humphrey has complained that several bags of his political mail during the Wisconsin primary campaign last year were found undelivered after the election. And the subcommittee staff has received an anonymous phone call from a man purporting to be a Washington postal supervisor, who said the mail of Edmund Muskie was "covered" and perhaps opened during the 1972 campaign.

Whether such charges are true or not, the atmosphere of suspicion springing from the Watergate scandals is certainly breeding fears of political abuse of mail surveillance. Alan Westin, a Columbia University law professor who heads the American Civil Liberties Union's privacy committee, says, "Watergate raises the question of how much mail is opened and whether mail covers are used politically." He adds: "If any organization's mail is opened, that is a misuse of authority never intended by Congress."

A former postal inspector relates how a cover was put on the mail of the Iowa relatives of a man wanted by the law in Florida. Naive about such tactics, the man wrote his name and the address of his hideout in Baton Rouge, La., on one letter; to his surprise, he was promptly arrested. "It's very hard to go for a long time without communicating with friends or relatives," says C. A. Miller, recently retired head of criminal investigation for the Postal Inspection Service.

Mail covers aren't specifically authorized by any law, but their use dates back to 1893 when the procedure was spelled out in postal regulations. The practice has been challenged in the courts and has been upheld. The Supreme Court hasn't ruled but has denied requests to hear attacking lawsuits.

EVEN THE RABBI

Whatever their legal standing, mail covers have gained some ill fame before now, particularly in the case of Roy Cohn, the Senate committee counsel for the Army-McCarthy hearings in the 1950s who later got into legal trouble in his business dealings; he was tried and acquitted three times during the 1960s. In 1964 a postman accidentally and inexplicably delivered mail-cover instructions pertaining to Mr. Cohn and his law partner to the latter's home in New York City. Mr. Cohn charged in court that his mail was opened as well as monitored; the government admitted the cover but denied opening mail.

Moreover, the IRS, after learning the names of Cohn correspondents, sent questionnaires about him to every acquaintance from his rabbi to an ex-girlfriend. "After they questioned my rabbi, I wouldn't put anything past the government," says Mr. Cohn, now a New York lawyer.

After one of his trials there was a congressional outcry about mail monitoring, and hearings were held. The results were limited: the postal Service banned mail covers on any attorney of any individual under investigation, and for a time the operations were cut back to about 100 apparently from some thousands.

Controversial, too, is the Customs Bureau's inspection of packages and letters arriving from abroad each year, and particularly its power to open letters. Officials say millions of letters are inspected each year, but they don't say how many are actually opened. (Only in 1971 did the bureau acquire authority to open letters; its employes are prohibited from reading them.) Short of opening mail, agents may x-ray it for metal contents such as guns or have dogs sniff it to detect drugs.

Following the Customs Bureau's lead, the Postal Service recently got its own x-ray machines to screen letters and packages for contraband and bombs. At a recent demonstration here, one of the machines penetrated a bundle of 100 letters to pick up the outline of a letter bomb planted for demonstration purposes. It looked like a ball-point pen with wires. In the main Post Office alone, 500 to 1,000 pieces of suspect mail are x-rayed each week. So far, one postal inspector says, none has contained a bomb.

[From Television Digest, Aug. 20, 1973]

FCC CAUGHT IN MAILSACK

Many staffers at FCC haven't been getting some of their mail for nearly a year, and they probably didn't even know it. Practice of immediately sending mail from congressional offices directly to FCC Chairman to be opened—except that addressed to individual Commissioners—was abruptly halted August 8 after Senator Jackson, Democrat, of Washington, inquired about procedure.

As chairman of Senate Investigations Subcommittee, Jackson wrote FCC and over 4 dozen other agencies after subcommittee learned that FPC used similar procedure. It was started at FCC August 1972, in an attempt to speed up answers to congressional inquiries, Burch told Jackson. However, only three Commissioners—R. E. Lee, Rex Lee, and Johnson—in their offices August 17 said they knew nothing of practice until seeing Burch letter saying it had been halted. All three expressed concern over opening of mail and fact they didn't know it was being done. There also was consternation because August 15 letter had gone to Jackson over Burch's signature without being brought before Commission. (Burch was on vacation in West Virginia last week, didn't actually see letter, but aide Charles Lichtenstein said it was read to him over telephone.)

Lichtenstein said monitoring of mail was halted as direct result of Jackson inquiry. "It seemed like a good idea to stop," he said. "The implication that maybe this wasn't kosher was enough for us." He also said commissioners were informed a year ago when it went into effect. Original order to screen congressional mail was given verbally to mail branch by executive directive. Burch sent August 8 memo to bureau chiefs and staff officers, saying in future "all congressional mail is to be routed to the addressee unopened and is not to be logged." Other Commissioners weren't consulted in advance.

In the letter to Jackson, Burch said screening was started "to permit central logging and careful surveillance of due dates * * *. Entirely too many requests for information and special services were going unanswered, sometimes for several months running. Mail delivered directly to the addressee was never centrally logged and was often mislaid or simply lost." He said even though new procedure may "result in some degradation of our service to Members of Congress and their staffs, I have taken such action because I, too, believe * * * that the previous practice might pose serious questions as to rights of individual privacy."

Rex Lee noted he had served in three agencies under six Presidents and that congressional mail and contacts "has always been a problem [but] I would prefer that no attempt be made to pry, to monitor or check * * * although there's a lot to be said for the other side." Congressional inquiries, he said, must be directed to a level where there is authority to make decisions. "The whole thing bothers me," added R. E. Lee.

Jackson also was concerned over monitoring employees' phone calls. "I want to assure you," Burch said, "that this agency does not have and never has had any policy or practice of restricting or clearing or monitoring either meetings or telephone conversations between Members and staff of Congress and our staff." Burch didn't refer, however, to 1970 wiretap incident at Commission and hell he caught from House Investigations Subcommittee for authorizing bug of employees' phone allegedly to stop agenda leaks (vol. 12:52 p. 6).

[From the Washington Post, July 5, 1973]

AIDES TO FPC CHIEF OPEN HILL MAIL TO STAFF

(By Morton Mintz)

Congressional mail addressed to key staff members of the Federal Power Commission is opened by aides to commission Chairman John N. Nassikas "when there is no indication that the contents of the envelope are personal or confidential," he has acknowledged.

"I have required that all incoming congressional correspondence be routed through my office where it is promptly sent on to the appropriate addressee," Nassikas said in a letter Wednesday to Sen. Henry M. Jackson (D-Wash.).

"With their knowledge and concurrence, we do open the congressional mail of certain key staff personnel when the information on the envelope reveals that it was addressed to the staff member in his official capacity with this commission," the chairman continued.

"Mail so opened that relates to a matter pending before this commission is referred immediately to the secretary of the commission by the stenographer in charge of mail in my office," Nassikas said.

He told Jackson that he has a different policy for the Office of Economics, where there has been open opposition to decontrol of prices for new natural gas intended for interstate customers, as advocated by President Nixon, and to a recent FPC decision giving three producers a 73 per cent increase.

Nassikas, the dissenter in the 2-to-1 price-increase decision, said, "As to the Office of Economics, my policy has been to refer congressional inquiries unopened to the addressee. Inadvertently, some correspondence addressed to an economist has been opened by my stenographic staff but not read.

"If any other employee's mail has been opened in my office or if mail has been opened under circumstances other than those I have outlined in this letter, it has occurred strictly as a matter of inadvertence," he said.

Soon after President Nixon appointed him in 1969, Nassikas said, he became aware that important inquiries from Capitol Hill "were sometimes lost or delayed for inordinate periods of time in the course of internal processing."

Nassikas said he ordered mail routed through his office in order to end the previous inconvenience and dissatisfaction.

Jackson inquired about Nassikas' mail policies in a letter on June 29. He wrote as chairman of the Senate Interior Committee. Its staff is inquiring into the authenticity of the claimed shortage of natural gas reserves, which is the basis for the President's appeal to Congress for decontrol and for such administrative actions as the 73 per cent price increase.

The Jackson letter dealt mainly with "a very disturbing matter": the restrictions he said have been placed by Nassikas on the access of congressional committees to the expertise of selected FPC staff members.

Jackson's protest developed from a phone request by Interior Committee counsel William Van Ness to Dr. David S. Schwartz, assistant chief of the Office of Economics, to meet with the committee staff to review a report it was preparing on the natural gas situation.

The senator said Schwartz told Van Ness that any contact between FPC staff members and members or committees of Congress would have to be reported to Nassikas' office and that the chairman would have to clear any meetings or discussions.

Van Ness told an aide to Nassikas last Thursday that he wished to have Schwartz meet with the committee staff the next morning. But Schwartz then told Van Ness he had been told by Nassikas not to come to Capitol Hill until the FPC chief had received and approved a formal request from Jackson "specifying the nature and purpose of the meeting," Jackson said.

The senator conceded that it may be "entirely proper" for the commission chairman to be fully informed and to maintain a veto over contacts with FPC staff members.

However, Jackson charged, the FPC has implemented such a policy "in a discriminatory manner for the purpose of monitoring the views of those staff members whose views on factual, legislative and policy matters differ from your views or the views of the commission as a whole."

Nassikas, in reply, insisted that the case of Schwartz is unique, because it involved the first known request by a congressional committee's staff to have a member of the FPC staff review a proposed report "relating to policies affecting our jurisdictional responsibilities."

Consequently, Nassikas said, he asked that the request for Schwartz's services be made "officially" and publicly to make it clear that the participation of "an economist with divergent views from the policies of this commission" could not be misconstrued to constitute commission or staff participation.

Nassikas said that "no restrictions have been placed on the access of congressional committees to the expertise" of any FPC staff members. Neither has he ever vetoed a request by a congressional committee for aid from the FPC staff, the FPC chairman said.

APPENDIX J

Monitoring and Other Service Evaluations

Prior to the advent of the Tel-Tone M-220 and M-240 and the Alston 370/389 service monitoring systems, telephone companies of the United States used other means to observe employees at work--- and sometimes while not at work. Attached are items from the files of CWA to portray situations of the last decade.

*** "Progress Observation" forms used, for example, by Michigan Bell and Pacific Telephone & Telegraph Companies. The forms are virtually identical. Some of the checkoff items are completely subjective, such as "Faulty Judgment," "Faulty Start of Conversation," and "Failed to Be Helpful."

*** CWA report on results of a California Public Utilities Commission case, which brought in restrictions on monitoring for disciplinary purposes. The California Commission rules required the telephone companies to inform all employees of the new monitoring procedures.

*** Extracts of a letter from a Bell System Local President, telling of the monitoring techniques of which he was aware and in which he had come into contact.

*** CWA memorandum detailing the May-June 1966 revision of service observing procedures, flashed throughout the Bell System on an "emergency handling" basis.

*** Pages from Western Electric supply catalogs, showing "transmitter mountings" for business offices. These items were desk calendar-inkpen sets, inside which microphones could be concealed for "... observation of conversations between customers and telephone company employees."

*** Reproduction of a news story from the October 1963 issue of CWA News describing the discovery of a closed-circuit TV camera in a men's room. The company had the observing system installed because of graffiti being scribbled on the walls.

Attachment 3

Communications CWA Workers of America
(AFFILIATED WITH AFL-CIO)

OFFICE OF
THE PRESIDENT

1925 K STREET, N.W., WASHINGTON, D.C. 20006
TELEPHONE FEDERAL 7-7711

May 10, 1971

File: 4.3
x 1.12.13.57

To: All Executive Board Members and Nat'l Directors

Subject: Supervisory Monitoring -- California Public Utilities Commission Ruling

Fellow Officers:

The California Public Utility Commission has ruled that telephone companies cannot use information obtained through supervisory (secret) monitoring for disciplinary purposes.

This case arose as a result of disciplinary action taken by Pacific Telephone and Telegraph and General Telephone against CWA members where information obtained during supervisory monitoring was used in support of the companies' cases.

The Commission stated that supervisory monitoring of telephone, traffic, and plant operations is permitted without notice only when performed without the making of any written notation or any record of the contents, substance, purpose, effect and meaning of any conversation which may have been heard during the monitoring. Furthermore, information obtained by supervisory monitoring cannot be disclosed to any other person.

If a monitored communication is going to be used for disciplinary purposes, notice must be given that the employee's privacy is being violated.

In response to the companies' claim that secret monitoring is necessary to maintain effective control over its workforce, the Commission stated:

> "It is not necessary to sacrifice for ease of employee discipline the principle that, if the privacy of a

> communication is being violated, notice should be given of the violation of the privacy."

Having found the telephone companies in violation of Commission rules regarding supervisory monitoring, these corporations were ordered to take specific steps to insure that every employee is aware of the rules regarding supervisory monitoring. The companies were ordered to set up a training program on the subject, to receive written acknowledgement from every employee in contact with monitoring equipment that he has read the rules regarding supervisory monitoring and to require of every new employee that he reads the rules on supervisory monitoring.

While the legal effect of this decision only covers the State of California, its value as precedent in other states could be significant.

If you have any further questions on this decision, or if you want copies, please advise.

Sincerely and fraternally,

Joseph A. Beirne,
President

EBP-1660

The Pacific Telephone and Telegraph Company (Company) has the responsibility for providing high-quality telephone service to the public. This includes not only the proper functioning of equipment but such things as accuracy, completeness, promptness, courtesy and helpfulness of employees in business transactions with customers. It is agreed by the Company and the Communications Workers of America (Union) that appropriate procedures will be used to meet this obligation.

In addition, the Company and the Union agree that the laws with respect to secrecy of communications must be followed, and that both have an obligation to prevent any acts by employees which tend to perpetrate fraud, violate secrecy or cause loss of revenues.

It is agreed that supervisory monitoring as defined and referred to in CPUC Decision No. 73146 may be used to achieve the above objectives.

As defined, "Supervisory monitoring" is used by telephone companies to train and supervise individual employees in their performance of telephone service assignments.

Under CPUC Decision No. 73146, supervisory monitoring is permitted without notice (i.e., without a "beep tone") when performed without the making of any written notation or any record of the contents, substance, purpose, effect, or meaning of any conversation (which includes the employee's conversation) which may have been heard during said supervisory monitoring.

A person performing supervisory monitoring may not disclose to anyone (including supervisory personnel and the observed employee) any part of any conversation overheard while performing such supervisory monitoring.

The Company is obligated to insure, by proper training and direction of its supervisory people, that supervisory monitoring is properly used. To insure that this is done the Company agrees to train its supervisory people in the implementation of this Agreement covering the use of supervisory monitoring as follows:

a. Record of supervisory monitoring will be made on check-off type summary sheets recording only technical details and manner of job performance. No written notations of a conversation will be made except as absolutely necessary to protect secrecy of communications or to prevent fraud or loss of revenue.

b. When a record of a job discussion between a Traffic or Central Office Manager, or other supervisor and the observed employee is made, it will not include the contents, substance, purpose, effect, or meaning of any observed conversation, unless secrecy of communications, fraud, or loss of revenue is involved. An employee shall be permitted to review his/her personnel record upon his/her request.

c. Supervisory monitoring may be used to determine training needs and to evaluate the grade of service of individual employees. Other supervisory steps, such as training sessions, visual observation, individual discussions and coaching shall be used in addition to supervisory monitoring to evaluate and improve an employee's performance.

d. Employees subject to supervisory monitoring will be so advised.

e. Supervisory monitoring will be done only in the quarters where the employee is working.

This Agreement does not preclude the Union's right of grievance procedure and/or arbitration as set forth in the Agreement between the parties.

This Agreement may be terminated by either party in accordance with the appropriate Collective Bargaining Agreement covering Wages, Hours and Working Conditions for bargaining unit employees represented by the Union.

E. B. Montes
Communications Workers
of America, AFL-CIO

H. M. Gattone
The Pacific Telephone and
Telegraph Company
Bell Telephone Company of Nevada

Oct 12, 1971

F-1278 (10-63)

PROGRESS OBSERVATION
OUTWARD (MS)

OPERATOR _____ CENTRAL OFFICE: _____

SUPERVISOR: _____

								Total
Date								
Answering–Sta.								
Per.								
Coin								
Ass't								
CZD								
Watching For & Answering Signal								
Faulty Pos Mgmt								
Fld to Open Listen Key	o							
Fld to Hold Bk Cd	o							
Fld to Set # or D/N in Adv	o							
Faulty Attention to Sig	o							
Fld to Use Proper Cd – In WH	o							
Faulty Cd in Ans								
Faulty Ans Phrase								
Fld to Pick Up Front Cd	o							
Interpreting Call Request								
Order Rcpt'd Incor or Unnec	o							
Unnec Add'l Req	o							
Faulty Mark Seq								
Fld to Ack Approp								
Fld to Req Assist	o							
Advancing Call								
Del Search for Rte	o							
Faulty Pos Inf	o							
Fld to Use Tracer								
Incor Req for Rte	o							
Fld to Offer Area Code								
Incor Rate Quoted								
Faulty Deposit	o							
Incor Ckt or Trk	o							
Faulty Cd in Advancing								
Mem Rte Used*	o							
Faulty Keyset	o							
KP Before Sender	o							
KP Partial Order	o							
KP Incor # Digits	o							
KP Incor Rte or #	o							
Fld to Operate ST Key	o							
Fld to Sequence as Ovlp	o							
Incor Order Pad								
Fld to Give Cld #								
Faulty Ringing	o							
Incor "BY" Action	o							
Incor "DA" Action	o							
Incor Rpt Given	o							
Incor "RG" Action	o							
Incor "NC" Action	o							
Fld Secure Duress	o							
Fld to Give Sspy	o							
Other Errors								

								Total
Date								
Advancing Call (Cont'd)								
Fld to Use Nec Quest, Rpt, Opt								
Faulty LW	o							
Fld to, or Unnec Listen	o							
Faulty Start of Conv								
Faulty Reminders, Cord Clips								
Faulty Tkt-Handling								
Faulty Calcul – Start of Conv								
Fld to Rpt Tbl								
Timing and Releasing								
Faulty Notification								
Fld to Chal Promptly	o							
Del Timing								
Faulty Calcul – End of Conv								
Del Rel	o							
Rel in Error	o							
Fld to Time and Rel as Ovlp	o							
Fld to Quote Chg								
Incor Chg Quoted								
Faulty Cal	o							
Faulty Ret								
Faulty Rel	o							
Fld to File Tkt								
Judgment and Tone of Service								
Faulty Judgement								
Faulty Cut Out								
Fld to Be Helpful								
Fld to Be Courteous								
Faulty Voice								
Faulty Screech								
Displays Irritation								
Ticket Entries								
Det Omit								
Det Incor	o							
Det Illeg	o							
Faulty Mark	o							
Incor Rte Ent	o							
Incor Rpt Ent								
Fld Ent Rpt								
Unnec Tkt Ent	o							
Fld Mark Mis and Chg	o							
Faulty Stamp								

Notes: The dot (•) indicates the items affecting Call Carrying Efficiency.

88

PROGRESS OBSERVATION FORM

PRINTING SERVICE 5-63750
GTS 1-63

								TOTAL
Date	NOV 24 [illegible]7							
Calls	[illegible]							
Assist	[illegible]							
Coin								
Watching For & Answering Signal								
Faulty Pos Mgmt								
Fld to Open Listen Key	•							
Fld to Hold Bk Cd	•							
Fld to Set # or Time of Day in Adv	•							
Faulty Attention to Sig	•							
Fld to Use Proper Cd – In WH	•							
Faulty Cd in Ans								
Del or Faulty Ans	•							
Fld to Pick Up Front Cd	•							
Interpreting Call Request								
Order Rcpt'd Incor or Unnec	•							
Unnec Add'l Req	•							
Faulty Mark Seq								
Del or Fld to Ack Approp	•							
Fld to Req Assist	•							
Incor, Incomp or Fld to Give C.I.								
Fld to Quest Class of Service								
Fld to Comply with Cust's Spec Req								
Doubt or Qur Incor Order Acc	•							
Fld to Acc Cust's Rte	•							
Fld to Offer Credit: WNO, C'O, PTT								
Incomp or Incor Rate Quoted								
Advancing Call								
Del Search for Rte	•							
Faulty Pos Inf	•							
Fld to Use Tracer								
Incor or Incomp RAR Ord Pad	•							
Faulty Deposit	•							
Fld to Offer Refund								
Incor Ckt or Trk	•							
Faulty Cd in Advancing								
Mem Rte Used*	•							
Faulty Keyset	•							
KP Before Sender	•							
Comp Ord Keyed or no Dig Keyed-Ckt Rel	•							
KP Partial Order	•							
KP Incor # Digits	•							
KP Incor Rte or #	•							
Fld to Operate ST Key	•							
Fld to Vfy or Vfy'd Incorrectly	•							
Fld to Sequence # as Ovlp	•							
Incor Order Pad	•							
Fld to Give Cld No								
Faulty Ringing	•							
Incor "BY" Action	•							
Incor "DA" Action	•							
Incor "RP" Action	•							
Incor "AA" Action	•							
Incor "NC" Action	•							

Central Office

Operator

T.A.

								Total
Advancing Call (Cont'd)								
Incor "NO TRUNKS" Action	•							
Incor or Incomp Bus Ofc Action	•							
Incor or Incomp Rep Svc Action	•							
Rpt Given Unnec	•							
Fld to Time as Supv	•							
Faulty Announ	•							
Fld to Use Nec Quest, Rpt, Optios								
Faulty LW	•							
Fld to or Unnec Listen	•							
Faulty Start of Conv								
Faulty Reminders, Cord Clips								
Faulty Tkt Handling								
Faulty Calcul – Start of Conv								
Fld to Rpt Tbl								
Timing and Releasing								
Faulty Notification								
Fld to Chal Promptly	•							
Del Timing								
Faulty Calcul – End of Conv								
Del Rel	•							
Rel in Error	•							
Fld to Time and Rel as Ovlp	•							
Fld to Quote Chg								
Incor Chg Quoted								
Faulty Cal	•							
Faulty Ret								
Faulty Rel	•							
Fld to File Tkt								
Judgment & Tone of Service								
Faulty Judgment								
Faulty Cut Out (or Off Line)								
Fld to Be Helpful								
Fld to Be Courteous								
Faulty Voice								
Faulty Speech								
Displays Irritation								
Ticket Entries								
Det Omit								
Det Incor	•							
Det Illeg	•							
Faulty Mark	•							
Incor Rte Ent	•							
Incor Rpt Ent	•							
Fld Ent Rpt								
Unnec Tkt Ent	•							
Fld Mark Mis and Chg	•							
Faulty Stamp	•							

Notes: The dot (•) indicates the items affecting Call Carrying Efficiency.

89

March 1, 1967

Mr. Joe Beirne
President
CWA-AFL-CIO
1925 K Street, N. W.
Washington 6, D. C. 20006

Dear Sir:

I know your position and the oppositions you have been advertising to all types of monitoring within the Bell system and feel that you might answer some questions for me. I have been planning on writing an article in our local newsletter showing the types of monitoring in where the equipment is located and who does the monitoring.

Some of our members have questioned whether this publication would be in violation to the secrecy of the communications form we all signed for the Company or any Federal law. I personally feel we would be doing our duty as officers of the local to advertise this to our members.

Some examples of the equipment and monitoring devices in are as follows:

1. Observer shoes put on local telephone numbers and observed by the Traffic Service Observers. Each office has so many observer shoes and they are continually changing them to different telephone numbers each day. For example Office 2 - 3 in Shreveport has approximately 50 shoes. I remember over a year ago the FBI inspected their lines and when they found an observer shoe on them they were removed promptly.

2. Observer shoes on Cama trunks.

3. Observer shoes on Repair service trunks.

4. Observer shoes on Business Office lines through Operator.

5. Observer shoes on Local Testboard positions.

6. Monitoring connections to Local Dispatcher positions - Testboard and Assignment Dispatch.

Mr. Joe Beirne
Page 2
March 1, 1967

7. Special monitoring connection to various other phones. We assume them to be telephone Company phones bur we're not positive.

8. Special observer to monitor all business office positions and trunks.

9. Official service observer connections on most all switchboard positions.

10. Chief Operator monitoring circuit to switchboard and Service Assistant's desk.

11. C.O.I. monitor to switchboard.

12. Service Assistant monitor to switchboard.

13. Other miscellaneous monitoring.
Many of these circuits can be monitored from the Division Offices, District Offices, Plant Foreman's Offices, etc.

Since most businesses do not need such an elaborate spying system to operate efficiently and profitably , we feel that if these conditions were publicized it would be a help to our members and probably shock many of the Telephone Company customers.

The purpose of this letter is to ascertain if, by showing this information in our newsletter and sending copies to the Governor, Public Service Commissioner, Senators, The House Committee Investigating Monitoring, etc., would we be in any way legally violating the secrecy of communications? We would appreciate any opinions and assistance that you may give us, or any legal opinion you may give us before we take any action.

Sincerely,

Attachment 8

In May 1966, during the course of Senator Edward V. Long's preparations for hearings into the subject of "Invasion of Privacy," AT&T flashed the word to all operating companies to revise the service observing procedure. The AT&T directive was treated on an emergency basis, to become effective June 1, 1966. AT&T sent a teletype message May 10, 1966, followed by the letter from C.K. Collins, Assistant Vice President, to the operating companies. The letter, and the attachments thereto (Attachment3) prescribe very specific and detailed changes in the method of service observing. The letter says that after a trial of the new methods of observing, AT&T would issue "a printed revision of the observing practice."

CWA heard from a confidential source that AT&T on May 6 had issued a preliminary instruction to the companies, calling on them to cease allowing service observation on conversations. The Beirne letter of May 13, 1966, is included in Attachment 3. (The May 6 date probably was erroneous.)

CONTINUED

1 OF 4

The Bell System "Traffic Observing Practice" attached to Collins' letter, dated October 1965, contains very specific and mandatory language, usually by the word "shall."

In connection with the May 1966 instructions, pp. 2607-09 of the printed hearings of Senator Long's subcommittee inquiry, covering testimony of September 14, 1966, should be reviewed. The AT&T witness on the stand was Herbert L. Kertz, Vice President-Operations. Kertz was reading his prepared statement, making the point: "(1) We are not, in our service observing, invading our customers' privacy. We do not monitor customer-to-customer conversations."

At that point, Senator Long inquired whether that was not in fact a recent development. Kertz waffled; Long directed Kertz to quit filibustering and answer the question directly. Kertz replied: "We stopped that practice on toll calls on June 1, 1966." Subsequently he admitted that the nationwide halt to that practice took place on that same date. Kertz claimed the change had been planned since 1965. Long asked Kertz why, then, the AT&T telegram had been marked "emergency handling required." Kertz replied that emergency handling was the only way the operating companies could be gotten to make the change of procedure simultaneously on June 1, 1966. He added that some change of equipment Bell System-wide was needed and accomplished in the 20 days between May 10 and June 1.

37-871 O - 74 - 7

... and Assistance Observing Practice

Co Intrunk
Co Basic Ltr

AMERICAN TELEPHONE AND TELEGRAPH COMPANY

195 BROADWAY, NEW YORK, N.Y. 10007

AREA CODE 212 393-3178

C. H. COLLINS
ASSISTANT VICE PRESIDENT

May 17, 1966

File No. 386.3

As a result of the service observing experience meetings held in March and April of this year and the change in observing procedure covered in our teletype message of May 10, several revisions are being made in the Outward Toll and Assistance observing practice issued last December. Attachments to this letter cover these revisions; they include a digest of principle changes, insert pages for Sections A, B and C of the practice, and correction sheets for Sections E and F.

Additionally, in order to more directly reflect the impact of timing on customer service, the Outward Toll error category has been expanded to include all observed instances where timing errors of 11 seconds or more affect chargeable minutes. This could permit discontinuance of Over and Under Timings as a separate component of a future index, if generally felt desirable.

The detailed changes in the observing procedures to meet the requirements of the teletype message of May 10 are contained in Sections B and C and are to be effective June 1. They pertain chiefly to the subsection on "Starting and Terminating the Observation", changes in the application of Cutoff and Interruption errors, and elimination of Faulty Notification irregularities. One other change is being made. The maximum time an observation will be followed has been reduced from 10 minutes to 5 minutes on all calls, both coin and non-coin. There will be minor savings in observer time as a result of this change.

This change in observer involvement will require a high degree of management attention to the manner in which these new procedures are introduced. We will be interested in your approach to this problem. Serious consideration is being given to design changes in the circuitry of the observing boards to provide an audible tone or other device to assist observers in detecting immediately any change in supervisory or cord signals.

Although the attachments to this letter concern only the Outward Toll and Assistance practice, the change in procedure discussed above also affects other official and unofficial observing practices. Any necessary revisions in observing practices will be forthcoming at a later date. Traffic

Service Position observing would appear to be the only other service requiring use of the plug-switch by the observer. The observer's headset will be switched off during periods of conversation when no position is connected to the trunk under observation.

The major change in DDD Outgoing Trunk observing is the dropping of the observation immediately with the start of satisfactory conversation, thus eliminating transmission volume and noise measurements. With these measurements no longer recorded the need for the present large quota of Out Trunk observations is reduced. It is recommended that the quota on this service be dropped to 900 observations per month pending a detailed inquiry into future requirements.

Dial Teletypewriter observing will also be affected. Present instructions are to observe each attempt to termination or for a period of 5 minutes following answer of the desired station. Effective June 1, these observations will be discontinued immediately following answer of the desired station.

As suggested in the May 4-5 meeting of selected General Traffic Managers, we would appreciate the careful study of the revised Outward Toll and Assistance practice by all General Traffic Managers and equivalent staff people. By August 10 may we receive, from all who wish to comment, marked up copies of the practice incorporating actual sections rewritten to reflect your suggestions on making the measurement plan more valuable as a tool for field use in achieving excellence of service from the customer viewpoint. When these comments have been received, it is intended to review them preliminarily with a representative group of field people before a printed revision of the observing practice is issued.

The insert pages and corrections attached to this letter are not being distributed as a regular practice on standing order. Additional copies required for distribution and training purposes should be locally reproduced.

Because substantial overall changes are involved, it is recommended that a new accumulation of data be started when the revised practice is introduced in those companies where entity and city summaries are now being produced.

Any questions your people may have can be directed to anyone in the Service Observing section of the Traffic Measurements group.

Yours very truly,

C H Collins

Assistant Vice President

Attachments

To all General Traffic Managers

List of Principle Changes

1. Connection to distant Information call reclassified from Toll to Assistance.

2. "Starting and Terminating Observation" subsection changed to eliminate observing on conversations.

3. Maximum duration of observation reduced from 10 minutes to 5 minutes on all calls, coin and non-coin.

4. Errors caused by PBX operators and extension users excluded from central office results.

5. Cutoff and Interruption errors limited to those for which definite observed evidence is available.

6. New Potential Billing errors added for omission or incorrect recording of credit details on Toll Tickets and for timing errors of 11 seconds or more which result in wrong chargeable minutes.

7. Incorrect Report error now charged for giving a BY report when an NC signal was received, changed to an irregularity.

8. Present interval of 3 seconds for the difference between observer's and operator's record of conversation time for determining Rate and Charge errors, changed to 11 seconds.

9. New Rate and Charge error added for incorrect or incomplete information relating to the time reduced rates go into effect.

10. Delayed Acknowledgment interval changed from 6 seconds to 11 seconds.

11. New irregularity added for failure to establish connection when customer, after receiving dialing instructions for toll call, requests connection.

12. New irregularity added for failure to offer option phrase after giving dialing instructions on customer dialable call.

13. Eliminate irregularity for failure to offer refund when customer indicates unconcern by saying, for example, "Never Mind" or "Forget It."

14. Eliminate ticket irregularity for use of unauthorized abbreviation for called place.

15. Base charging of irregularity for incorrect marking of chargeable time on operator's record of time rather than observer's record.

16. Assistance irregularity added for incorrect or incomplete dialing instructions not accepted or corrected before observation is terminated.

5.03 No change.

B. New Subsection: Suspension of Observing During Conversation

5.04 Each service observing position will be equipped with special features which will enable the observer to cut out of the connection during periods of customer to customer conversation.

5.05 Cord and Trunk Observed Offices Equipped with Supervisory Signals: On calls completed on the observed attempt (excluding official calls), the observer will cut out of the connection immediately following the satisfactory start of conversation with the desired station. The observer will operate the special equipment and remain cut out of the connection during the conversation period until one of the following events occur.

(a) Release of the FPU or RPU.

(b) Receipt of a disconnect signal from the calling or called station, or both.

(c) Receipt of a flashing signal from either the calling or called station.

(d) Receipt of a ringing signal on the front or back cord (FR or RR lamp lighted for the duration of the ring).

Note: In instances where the observer cuts back into the connection upon receipt of a cord signal condition and the observed events indicate that conversation has not terminated satisfactorily or a customer is attempting to recall the operator, she shall remain cut in on the connection until conversation has resumed satisfactorily, the recall signal has cleared up or the call under observation has been terminated.

5.06 Trunk Observed Offices not Equipped with Supervisory Signals: On calls completed on the observed attempt, the observation will be discontinued immediately with the satisfactory start of conversation.

C. Conversations Followed to Termination (Formerly Subsection B)

5.07 Outward Toll: The observation on all calls completed on the observed attempt, shall be followed to termination or for a period of five minutes. This will provide data on those features of service which are observed at the end of conversation.

5.08 Assistance: Observations on non-coin calls, and coin paid calls on which a correct deposit has been observed, shall be dropped at the satisfactory start of conversation. All observations originating at coin telephones shall be followed to termination, or for a period of five minutes only if an incorrect deposit is obtained. If an incorrect deposit is obtained, the observer will cut out of the connection at the satisfactory start of conversation, and cut back in upon receipt of a cord signal condition as outlined in Paragraph 5.05.

5.03 *Trunk Observed Offices:* The observer will normally be in on both sides of the connection during the advancement of the customer's order, i.e., the recording-completing or toll terminal trunk, and either the toll line or tandem trunk. It is contemplated that the observer will also be in on the particular trunk used by an operator in securing rate, route or directory information.

B. Conversations Followed to Termination

5.04 *Assistance:* Conversations on calls originating at coin telephones shall be followed only if an incorrect deposit is obtained, and in such instances the conversation will be followed to termination.

Outward Toll

5.05 Conversations on Sent Paid calls shall be followed to termination, or for a period of 10 minutes, except where there is indication at the end of 10 minutes that conversation will end shortly. This will provide more complete data on those features of service which are observed only during conversation or at the end of conversation.

5.06 All conversations on coin paid calls shall be followed to termination.

C. Event Terminating the Observation

5.07 The observation shall be followed to one of the terminating events specified below, and the reason for the discontinuance shall be shown in "Remarks" whenever it is not evident from other entries on the detail sheet.

(1) The release of the recording-completing, tributary, switching, or toll terminal trunk.

Cord Observed Offices

Observing will be discontinued with the release of the back cord and any entries made shall be encircled in instances where the operator plugs in with a back cord, presumably to answer a trunk signal, and then disconnects after answering but before accepting or taking any action on the call. If the operator disconnects after accepting the call, observing shall not be discontinued until the observer is reasonably sure that no further action will be taken on the same cord pair.

Trunk Observed Offices

Observing shall be continued so long as someone is waiting on the trunk, in instances where the operator plugs out a recording signal and then disconnects without answering, or disconnects after answering but before the party or operator connected has an opportunity to respond.

(2) The release of the front cord in instances where this occurrence follows the release of the back cord. Observing shall be discontinued with the release of the back cord if it is evident from observed events that the front cord is being held to report a trouble condition.

(3) The start of conversation on an Outward Toll call in instances where, on trunk observing, the observer has not succeeded in securing the toll line or tandem trunk before the start of conversation.

(4) The start of satisfactory conversation on an Assistance-Local call on which connection has been established, provided the correct deposit is secured on a call originating at a coin telephone.

(5) The answer of the called operator on a call which is correctly referred to another operator for handling; for example, a distant operator on a Delayed Inward call, an Information operator, an International operator, etc.

(6) Any event identifying the call under observation as an Official call. Official calls may not be recognized as such immediately, and any events observed before the call is identified shall be classified and included in the routine summary of observations. Observations covering calls which are referred to a Supervisor, Service Assistant or Chief Operator because of a service difficulty shall be continued to the normal terminating event, since such calls are not considered Official calls.

(7) The receipt of an alternate order constituting a new call. Observing shall be discontinued at the time the original circuit is released, or at the time a change in ticket directions is acknowledged.

RETURN
J. A. BEIRNE

Communications Workers of America
(AFFILIATED WITH AFL-CIO)

1925 K STREET, N.W., WASHINGTON 6, D.C.
TELEPHONE FEDERAL 7-7711

OFFICE OF
THE PRESIDENT

May 13, 1966

File: 6,
x 1.12.13.57

PERSONAL AND CONFIDENTIAL

To: All District and National Directors ONLY

Subject: Service Observations

Fellow Officers:

It has come to our attention from a confidential source that AT&T sent a telegram to all operating companies on Friday, May 6, instructing them to cease allowing Service Observers to listen in on any conversation. We thought we ought to pass this along to you in a Personal and Confidential form in order that you might keep your ear to the ground on the matter.

We are not sure, of course, what the reason for this action is other then it may flow from the hearings being held by Senator Long's Committee here in Washington on eavesdropping. We are also not sure whether this extends to management listening in on conversations of employees. You should be extremely careful how you use this information. Any of you who might be in possession of any further details should send me a written report on the matter in order that we might be completely on board here in this office. No contacts should be made on the company in connection with this matter. Perhaps they will come to you.

Sincerely and fraternally,

Joseph A. Beirne,
President.

NP-2977

JULY 31, 1957

NOS. 16L & R TRANSMITTER MOUNTINGS

SEE RATINGS BELOW

Intended for use on desks in telephone company business offices for the observation of conversations between customers and telephone company employees.

Each arranged to mount one K2 transmitter unit.

Each consists of a black glass base with a felt bottom, a fountain pen and socket, a holder for calendar cards which also conceals the transmitter, a set of calendar cards and a frame with a card to identify the employee.

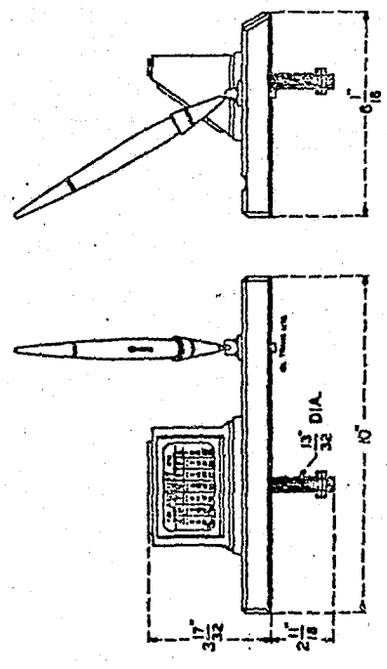
Illustration shows the No. 16L. The No. 16R is the same, except that the positions of the pen and calendar are interchanged.

Arranged to mount permanently on the desk, with the connecting wires to transmitter unit passing through the mounting tube and top of the desk. When it is not desired to fasten permanently to desk, mounting tube and stud can be removed and connection made by means of an R2DW cord for which a groove to the rear of the mounting is provided in the base.

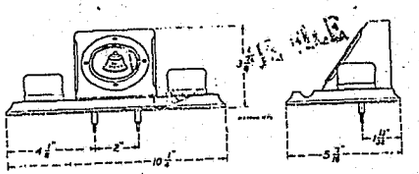
Orders for these transmitter mountings shall specify the year for which the calendar pads are to be used.

Replacing set of calendar cards can be obtained by ordering a P-290100 calendar set for year ____

Code No.	Side of Desk Intended for Use on	Part of Transmitter No.	Rating
16L	Left	1016L	A.T.&T.Co.Std.
16R	Right	1016R	"



JULY 29, 1953 | **No. 11A Transmitter Mounting** (Bears Marking "Bell System") | MANUFACTURE DISCONTINUED



Intended for mounting a No. 399A transmitter unit in telephone company business offices for the observation of counter conversations between customers and telephone company employees.

Consists of a wooden base, two glass ink wells, two M1W cords (4-1/2 in.) and a wooden box arranged for mounting the transmitter in a concealed manner.

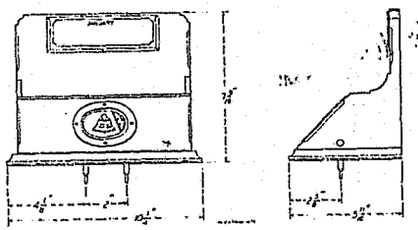
Two plugs extend through the base and are arranged to function with two No. 371 jacks.

All exposed wooden parts have a bronze lacquer finish.

Part of the No. 1011A transmitter.

CATALOG

JANUARY 29, 1953 | **No. 12A Transmitter Mounting** (Bears Marking "Bell System") | MANUFACTURE DISCONTINUED



Intended for mounting a No. 399A transmitter unit in telephone company business offices for the observation of counter conversations between customers and telephone company employees.

Consists of a wooden base on which is mounted a wooden box arranged for mounting the transmitter in a concealed manner and equipped with two compartments for holding cards or pamphlets. The back of the box has a holder for calendar cards which are furnished with the mounting.

Includes two M1W cords (4-1/2 in.).

Replacing set of calendar cards can be obtained by ordering a P-220440 calendar pad for the year ....

Two plugs extend through the base and are arranged to function with two No. 371 jacks.

All exposed wooden parts have a bronze lacquer finish.

Part of the No. 1012A transmitter.

CATALOG

Smile, You're on Candid Camera—Camera Is Uncovered in Employee Lavatory in A.T. & T. Building

New York.—The last bastion of individual employee privacy of the AT&T empire has fallen. American Telephone & Telegraph has entered the men's privy with a wide lens camera as final solution to the plaguing problem of how to keep tabs on the employee throughout the entirety of the working day.

Scene of the invasion of the employees lavatory was a building at 32 6th avenue in New York City. Excuse offered by the Company for the foul deed was that a "perverted mind" was at work scribbling obscenities on the walls of the lavatory.

According to a report from Kevin J. McEnery, President of Local 1150, employees in the 9th floor lavatory of the building noticed an overhead duct in the ceiling that was open. A few days afterwards, fellow employees noticed that a motion picture camera had been concealed within one of the open doors. When Local officers of 1150 were apprised of the situation, they immediately set into motion a thorough investigation. Discovered was a wide angle lens camera, focused for a direct side view of the urinals, capable of taking pictures at the rate of a frame every 15 seconds. Cabling led from the camera to an outlet concealed in a locked shower stall. Also discovered in one of the open doors in the overhead duct, was a large cardboard box with a pigeon hole cut in the side. Inside was a brown leather case, identified as property of the Pinkerton Detective Agency, containing unused film and other materials connected with the use of the camera.

Gathering all the proof necessary to support a case that could stand up in any court in the land, the Local got in touch with Lowell Wingert, AT&T Vice President in charge of the Long Lines unit. It was at this point, according to the Local, that management went into its "usual pass the buck act." Wingert passed the call on to F. H. Grobb, Assistant Vice President, who, in his turn, moved the call on to H. V. Camming, AT&T Attorney. Camming suggested that the matter be handled through "regular channels", but was advised of the obvious by the Local that something more than a mere grievance was involved. Camming, of course, said he'd have to discuss the matter with his bosses.

What horrified Local officers, however, was that throughout these conversations, and all that ensued, the Company not only failed to show remorse at what it had done, but worse, attempted to justify what it had done.

Further, the Company suggested that other methods of investigation had been used in their dogged pursuit of the wall scribbler in the 9th floor lavatory. Wrote Kevin McEnery in Local 1150's *Newsletter*, "Granted that this is an assault upon the dignity of the male employees which, whether by design or not, humiliates him, but, in light of the fact that they've only acknowledged what we ourselves have discovered, how are we to know whether they didn't carry this through to their illogical and unnatural end and plant a camera in the women's lavatory as well? And beyond this, if the Company persists in acting as if this act were justifiable, what is to keep them from going further—from going into our very homes, for example, to assure themselves that we aren't talking 'treason' or, to sing to their own dirty little argument, that we're thinking of 'scribbling on the bathroom wall?' The point is that if their argument prevails, then anything goes, because it's based on the oldest of all evil philosophies, that of the End Justifying the Means. This sort of philosophy was wrong when it was used by Adolf Hitler; it's no less wrong when used by AT&T management."

Added McEnery, "In its information bulletin posted on this situation, AT&T wrote that 'we intend to keep Long Lines a safe and clean place to work. We will not tolerate the disgusting, destructive actions involved in this case.'

"We would like to put AT&T on warning, that we also 'will not tolerate the disgusting, destructive actions involved in this case.' We condone no scribbling on the walls, or whatever it was that was involved. But by the same token, we condone no cameras either to observe us during our moments of privacy. Despite what management thinks, there are certain inalienable rights, even for employees. And unless AT&T acknowledges this, they're going to have a fight on their hands."

APPENDIX K

Voiceprint and PSE

Technology is at a point where tape recordings of human speech can be "analyzed" to determine if the speaker is (1) lying or (2) positively identifiable. Such beliefs appear a natural result of the age of technology which devalues the individual as an employee, or as a citizen.

Each of these new techniques, "Voiceprint" and use of the "Psychological Stress Evaluator," has been observed as having the same probative value of the polygraph, or "lie detector," which itself has not been universally accepted as sufficiently reliable for use as evidence.

CWA's interest in Voiceprint arises from the criminal prosecution in 1973 of Stephen Chapter, a member of Local 9404. Chapter was alleged to have telephoned a bomb threat to a plant service center of PT&T; the caller's voice was recorded. A poor quality sample of Chapter's voice, secured without his knowledge, was used for comparison with the bomb threat recording. Chapter was acquitted after a court trial, because of the errors in the Voiceprint development tests.

The Moorhead Subcommittee has a significant interest in Voiceprint because (1) the Subcommittee several years ago, when chaired by Representative John E. Moss, made a major study of polygraph techniques by Government agencies, and (2) the present stage of development of Voiceprint is the result of a development grant to the Michigan State Police from the Law Enforcement Assistance Administration (LEAA), Department of Justice.

The PSE technique was described in Newsweek magazine of July 23, 1973, I tor Counterintelligence and Security Inc., of Springfield, Virginia, developed a device to place key spoken words on graphs to measure stress and "prove" where untrue statements were made. The Dektor company performed analyses of two key Watergate hearings witnesses, former Attorney General

John N. Mitchell and former White House Counsel John W. Dean III. Dektor announced publicly that Dean got the highest rating for credibility and that Mitchell was not being fully truthful in his answeres to questions.

Security World magazine of October 1973, in an article headed "Truth Verification," described how the PSE system works, in terms much like a sales promotion brochure. PSE is alleged to be "... an important new development in the area of truth verification -- lie detection and stress evaluation. It has already demonstrated its usefulness, and in the hands of competent, trained, and ethical operators it should develop an enormous potential as an effective instrument and security as a valuable aid in the administration of justice." The article, by Gion B. Green, offers diagrams of spoken words and some general information on the technique, without scientific data reported.

PSE was briefly treated in the New York Times Magazine of November 25, 1973, as a sidebar to an article on polygraphs (lie detectors). The Times article notes that polygraph tests have yet to become accepted as court evidence-- although the newer Voiceprint has found its way into evidence.

* * *

The Moorhead Subcommittee should be interested especially in Voiceprint not only because of the sizeable Federal involvement in the experimental projects, but also because of the wrongs committed against those charged as a result of the "tests." The terms of the settlement offered by Pacific Telephone & Telegraph Co. can hardly be termed generous, as seen in the letter August 17, 1973, from the Company's labor relations director, W. L. Bowen, to CWA Area Director Cruice. Chapter was to receive his back pay, less

unemployment compensation payments and less his earnings. He did not secure compensation for his legal expenses; for such relief, Chapter will be required to institute a civil suit.

* * *

Epilogue. On June 6, 1974, the United States Circuit Court of Appeals for the District of Columbia made the first Federal appeallate ruling on the "Voiceprint" technology. The court ruled that "voiceprint identification is not sufficiently accepted by the scientific community as a whole to form a basis for a jury's determination of guilt or innocence." The story, from the Washington Post of June 7, 1973, is attached.

NOTE: The following is an extract of a CWA memorandum analyzing 4 tables in the LEAA-financed report, "Voice Identification Research."

Analysis of Tables

These 4 tables were copied from the report, "Voice Identification Research," submitted to the Department of Justice by Michigan State Police. The tables were the results from the tests conducted under direction of Oscar Tosi, who is the leading convert to the Voiceprint method.

The 4 tables are used because Hazen drew my attention to them as showing up the error possibilities inherent in the Tosi-directed study. These tables give results in tests of 6 words, single utterances, in "closed" groupings, with the first and second samples taken 1 month apart. The explanations of the ranks and files on the tables are at p. 41 (copy enclosed).

The biggest errors are in the Roman Numeral III, which means "clue words" spoken in random context. You will see that within that portion of each table, you can find many errors (listed as "OD") in the Beta and Gamma ranks. They are, respectively, telephone transmissions in quiet and noisy environments.

The table taken from p. 105 shows 24 errors in a possible 81. That means the panelists missed 24 out of 81 tries. If you want to refine that one further; you can see that the panelists had 4 out of 27, 10 out of 27, and 10 out of 27 errors. The overall error was 29%. The subgroup error was 14.8%, 37% and 37%.

Finally, it is noteworthy that a sizeable number of errors can be found in the vertical files headed "P3," which means panelists of criminal justice students, in other words, the people who want to be professionals in the field.

[From the New York Times, July 24, 1973]

Voice Print Trial Ends in Acquittal

Judge Calls Tape Unreliable and Frees Coast Suspect

San Rafael, Calif., July 23—The voice print is not yet a reliable means of identification for scientists, let alone the courts, a Superior Court judge said today in acquitting a telephone installer of a bomb threat charge.

Judge E. Warren McGuire of Marin County Superior Court attacked the voice print as unreliable in general and as riddled with mistakes in the case of Stephen C. Chapter.

Mr. Chapter, 28 years old, was charged with making a phone threat to blow up a San Rafael office of the Pacific Telephone Company on Feb. 1, 1972. The only evidence against him was a tape recording of his voice taken when Mr. Chapter, who was subsequently dismissed from his job, made a routine work order call.

He had refused to make a tape of his voice on the grounds that it was an invasion of privacy. He connected that he had been identified as the culprit because he was the only one of 17 phone employes to so refuse.

The case against Mr. Chapter was based entirely on testimony by the two men considered to be the nation's leading experts on voice prints, Dr. Oscar Tosi of Michigan State University, and his protege, Lieut. Ernest W. Nash of the Michigan state police.

Initially even Mr. Chapter's attorney, Robert L. Moran, thought the case against his client was strong.

During the six-day jury trial without jury, however the prosecution case slowly fell apart. At one point, it was revealed that Lieutenant Nash, who had initially identified Mr. Chapter as the bomb caller, later tentatively identified the voice of a deputy district attorney as the caller.

Further, Mr. Moran produced his own scientists, including experts from the Stanford Research Institute, who not only questioned voice print reliability but also expressed doubt that the voice on the bomb tape was that of Mr. Chapter.

In his ruling, Judge McGuire called Dr. Tosi's voice print method a good start but not yet reliable.

"Substantial additional research" is needed "before the reliability of speaker identification through auditory and spectrographic analysis is generally recognized and generally accepted by the scientific community, let alone admissible by the legal community," he said.

[From the Washington Post, June 7, 1974]

Court Bars Voiceprints as Evidence

(By Eugene L. Meyer)

In the first federal appellate ruling on voiceprints, the U.S. Court of Appeals here ruled yesterday that such identification may not be introduced as evidence in criminal trials.

"Whatever its promise may be for the future," wrote Judge Carl McGowan for the court, "voiceprint identification is not sufficiently accepted by the scientific community as a whole to form a basis for a jury's determination of guilt or innocence."

The opinion is binding only on federal courts in Washington, but as the first federal appellate ruling on the subject, can be expected to carry "a good deal of weight" with other federal and state courts, according to John A. Terry Jr., chief of the U.S. attorney's appellate division here.

A voiceprint is an electronic process that displays in a pattern of lines for visual analysis the voice sounds of an individual's utterances. The technique, pioneered 40 years ago, first was used as trial evidence in 1966.

Yesterday's opinion could also affect the only conviction obtained from several indictments in recent trials here of police officers charged with gambling conspiracy and corruption. That conviction, of Lt. Delmo V. Pizzati, for conspiracy on Feb. 20, was based largely on a voiceprint analysis.

In the D.C. Court of Appeals, one conviction based on a voiceprint is under appeal. The case involves telephone threats in early 1972 against the president of Federal City College.

The law on voiceprints varies from state to state. Courts in Florida and Minnesota now admit voiceprints, but the New Jersey Supreme Court has ruled them inadmissible.

"There's a general state of indecision as to its value and use," Robert A. Miller, chief of the FBI's radio engineering section, said yesterday. "We use it for investigative guidance. We've never used it (as evidence) because we've never been satisfied we could make a positive identification with it."

In a major federally-funded study of voiceprints, the Michigan State Police concluded in 1970 that so-called "spectograms" are at the least a useful investigative tool.

The U.S. Appeals Court decision yesterday involved the cases of two men tried on charges arising from an alleged shooting of a metropolitan policeman on April 9, 1971. Evidence included voiceprints of the defendants, one of whom was then identified as having made an anonymous call to police that led to the shooting.

Responding to the "policeman in trouble" call, the officer went to a Safeway store in Northeast Washington where he was shot allegedly by two men he had arrested 11 days earlier for disorderly conduct.

Based on the officer's identification of the men, the appeals court upheld their convictions. The jury had not relied on the inadmissible voiceprints alone, the panel said.

U.S. District Court Judge Oliver Gasch had admitted the voiceprint evidence, calling it "clearly reliable," after hearing testimony from experts such as Dr. Peter Ladefoged, a California phonetics professor.

However, the appeals court noted, Ladefoged has also expressed a number of continuing reservations, including problems arising from voice mimicry.

"While portions of the record suggest that spectogram analysis may become a useful tool for resolution of questions of criminal liability," the appellate court ruled, "it is equally clear that techniques of speaker identification by spectogram comparison have not attained the general acceptance of the scientific community to the degree required. . . ."

37-871 O - 74 - 8

APPENDIX L

UNION ORGANIZERS' MOTEL ROOM BUGGING

An important example of wiretapping without the cooperation of the local telephone company came to light in February 1973, in Wallace, South Carolina.

The incident is part of the long campaign of the Textile Workers of America, AFL-CIO, to secure bargaining rights for employees of J. P. Stevens & Company.

A wiretap device was discovered attached to the telephone in the motel room of two Union organizers at Wallace. The FBI was called into the case early by the Union and Southern Bell.

The Textile Workers has filed a $64 million damages suit against J. P. Stevens & Company for its role in the wiretapping of the Union organizers. The National Labor Relations Board has instituted a new civil contempt action against the company.

Confronted with a mass of evidence against it, the company suspended three executives and issued a statement alleging that it does not condone their tactics.

In October 1973, after the Textile Workers had prodded the FBI numerous times, a Federal Grand Jury indicted 2 company officials. After a 4-day trial in the Federal District Court in Greenville, S.C., the 2 were convicted on wiretapping charges. Maximum penalties against each are 5 years in prison and $10,000 fines.

[From the AFL–CIO News, Dec. 22, 1973]

TWO STEVENS OFFICIALS CONVICTED IN BUGGING

Greenville, S.C.—Two officials of J. P. Stevens & Co. face a maximum sentence of five years in prison and $10,000 fines for their conviction in the illegal wiretapping of two labor organizers in Wallace, S.C.

Harold E. Guerry, a Stevens personnel director, and Larry E. Burroughs, a plant safety engineer, were found guilty in federal district court here. But sentencing is being delayed pending court action on their motion for a new trial.

Their conviction came after a four-day trial on the charge they had bugged the telephones of Alfred L. Motley of the AFL–CIO Industrial Union Dept. and Mike Kirvosh of the Textile Workers Union of America while they were engaged in an organizing campaign.

The bug was found by a telephone company worker last January in Motley's motel room in Wallace which was used as the headquarters in the organizing drive at two Stevens plants. Guerry and Burroughs were indicted by a federal grand jury in October.

The company, which has a long record of anti-union activities and labor law violations, attempted to dissociate itself from Guerry and Burroughs after the indictment by announcing the two had been suspended.

In their testimony to the court, however, neither referred to himself as being a "former" employe of Stevens, TWUA lawyers pointed out.

TWUA President Sol Stetin noted following the trial that "J. P. Stevens & Co. lied when it charged that the bugging of a union representative's motel room early this year was staged by the union in order to place the blame on the Stevens company."

"Twelve jurors studied the evidence and came to the conclusion that this Watergate-style incident did indeed happen.

"The pity of it all is that two company officials were used as pawns in J. P. Stevens's unlawful attempt to prevent its workers from forming a union," Stetin declared.

"The company's claim that its two convicted officials were acting on their own was even less credible than the White House claim that the Watergate tapes were accidently erased by a careless secretary," Stetin declared.

When the IUD and the TWUA filed a multimillion-dollar civil damage suit in August charging that the company violated federal and state statutes, Stevens also denied it was involved in the bugging and called the suit a publicity stunt.

Stevens has repeatedly ignored orders by the National Labor Relations Board and the courts to bargain with the TWUA.

The NLRB recently filed new civil contempt actions in federal courts charging the company with failure to comply with earlier court orders.

The NLRB also called off an election at Wallace in September after Stevens illegally fired employees who tried to ask questions at "captive audience" meetings less than two days before the scheduled vote.

APPENDIX M

Medical Information: How Private?

The erosion of privacy rampant in the land has moved into the medical profession; although the physician's examining room is itself inviolate, the ever-present snoopers have devised efficient ways of learning details of citizens' private lives.

The most overt and blatant attack on medical data privacy came within the February 1973 proposal for new rules of evidence in the Federal courts. The proposed rules were transmitted by the Chief Justice of the United States after approval by the Judicial Conference. The Nixon Administration played a major role in the preparation of the proposed rules of evidence.

Proposed Rule 504 was to establish a "psychotherapist-patient" relationship, to become a far narrower category of privileged communication than the "doctor-patient" relationship, which is based on long-standing custom and usage. (See Beirne letter of March 9, 1973, to Chairman Hungate of the House Judiciary Committee's Special Subcommittee on Reform of Federal Criminal Laws for the CWA comments on this proposal.)

In essence, the Beirne opposition came on two grounds: (1), that invocation of a medical privilege would automatically mean that the person was in psychotherapy, and (2), that the entire set of an individual's medical records would be producible in worker injury cases, so that the person's own physician would become a kind of "company doctor."

The Congress wisely rejected many of the proposed rules of evidence, and accepted a set of rules which should prove fair, workable, and in keeping with sound legal practice.

* * *

The Jack Anderson column of May 9, 1972, "blew the cover" off an existing service by which the medical history of more than 12½ million

Americans is kept in a secret data bank, accessible by a computer-to-computer/telephone line arrangement. The Anderson column exposed the existence of the Medical Information Bureau, of Stanford, Conn., which provides a centralized service to 760 life and health insurance companies.

The accuracy of the Anderson column was confirmed by testimony later in 1972 by the director of MIB, Joseph Wilberding. The Senate Banking and Currency Committee's Subcommittee on Consumer Credit has been examining MIB's activities with the intention of eliminating the dangers of abuse. Additional information is contained in the October 1973 issue of "Communication: Today," the Anderson column, and the Senate speech and amendment of Senator Edward Kennedy.

* * *

Americans are being offered the wallet-size "Emergency MD Card," which contains a microfilm reproduction of a person's medical history. This card service is advertised on milk carton panels and elsewhere.

The person who is interested in the service pays a fee of $5, in return for which he receives a blank medical history form to be filled out and returned to the offering company, Medical Identification Systems Inc., of Melville, N.Y. The person who wants the Emergency MD Card is required to furnish his or her Social Security number and to sign the form. The requirement for the Social Security number is insufficiently explained away thus: "Time that would have been spent gathering this information is devoted to saving your life."

Medical Indentification Systems Inc. does not explain what it does with the forms, once they are microfilmed. The Moorhead Subcommittee should inquire of any connections or business transactions between Medical Identification Systems Inc., the sponsor of the Emergency MD Card, and the Medical Information Bureau, which provides services to insurance companies.

March 9, 1973

File:

The Honorable William L. Hungate, Chairman
Special Subcommittee on Reform of Federal
Criminal Laws
Committee on the Judiciary
House of Representatives
Washington, D. C.

Dear Mr. Chairman:

The proposed "Rules of Evidence for United States Courts and Magistrates," recently subject of your Subcommittee's examination, contain numerous questionable aspects.

From the standpoint of Labor Unions, the chief defect appears to lie in Rule 504, the "Psychotherapist-Patient Privilege." If the new Rule 504 is adopted for use in the Federal court system, the result can very well be that an injured worker may find his or her entire set of medical records produced under subpoena---even if most of those records are wholly non-germane to the accident-injury case.

The result thus would be that the worker's own physician becomes a kind of "company doctor."

Under proposed Rule 504, a worker attempting to prevent disclosure of his or her medical records will in effect be proclaiming that the doctor is a psychotherapist. This would call into question the worker's mental condition before, at, and subsequent to the work-related accident. Under the definitions, in 504 (a)(2), the psychotherapist is one who diagnoses and/or treats the patient's mental or emotional condition, including drug addiction. The presumption of emotional illness and/or drug addiction would be inescapable.

If production of a person's entire set of medical records were required under subpoena, the content of consultations between various medical practitioners also would be in the record of the case. Such entries in medical records could include material wholly non-germane, but damaging to the interests of the worker nonetheless.

A corollary objection is that a worker's physician might be obliged to testify as to content of any conversation with the worker, even if the conversation were not related to the injury case.

Many Americans are under the impression that the "doctor-patient" relationship is one of privileged communication. The extent of the general acceptance of that relationship can be seen from this text, quoted from p. 1236 of "Accident Prevention Manual for Industrial Operations, 6th Edition" (1969), issued by the National Safety Council:

> "Although the employer is entitled to know the individual's limitations from a placement standpoint, he should not have specific details of his physical and mental condition. That is, the referral of completed examination reports to lay persons for use in placement is undesirable because it violates the physician-patient relationship, invades the confidential nature of such reports, and untrained lay personnel are unqualified to interpret medical facts into terms of work significance; this is the responsibility of the physician."

It is our position that the proposed Rule 504 can be interpreted too widely, in view of a portion of the proposed Rule 803, "Hearsay Exceptions: Availability of Declarant Immaterial." While Subparagraph (4) of proposed Rule 803 ostensibly limits admissible medical statements to those "reasonably pertinent to diagnosis or treatment," there is the possibility of abuse, if the "doctor-patient" relationship no longer exists.

On behalf of the Communications Workers of America, I urge the rejection of Rule 504, as proposed.

The proposed Rule 509, "Secrets of State and Other Official Information," clearly appears to be an attempt to subvert, by court action, the intent and operation of the "Freedom of Information Act of 1967" otherwise cited as 5 U.S.C. 552. It is unfortunate that the concept of "national security" can be used to suppress information that is merely embarrassing to officials and agencies. This rule also should be rejected, barring more specific

coverage of genuine defense matters. Proposed Rule 509 would require the person seeking information to undertake a burden of appeal. The "Freedom of Information Act" clearly placed the burden on the government to demonstrate why the information sought should not be released. By making the information-gathering process more cumbersome, the government is signaling a return to the days of "secrecy in the public interest," which was the statutory language prior to enactment of the 1967 Act.

We commend the Subcommittee for its diligent examination of the proposed rules.

Sincerely yours,

Joseph A. Beirne.
President

APPENDIX N

HEW's Computer Study

In July 1973, an advisory committee to the Secretary of Health, Education and Welfare published a detailed report, "Records, Computers and the Rights of Citizens," outlining many privacy-related problems resulting from the use of automated personal data systems.

The HEW report, at pp.136-143, lists a number of legislative and administrative recommendations necessary to counter the threats to individual liberties posed by computerized record-keeping operations.

Among the key areas for tighter control is the use of Social Security number (SSN). In recent years many efforts have been made to use the SSN as a "Standard Universal Identifier" or "SUI." When the first SSN was issued in 1936, it was intended and used only for allocating employees' and employers' contributions to the retirement pension system. In the years since then, other Federal agencies have begun the use of SSN's for identifiers--- Internal Revenue Service for tax recording purposes, the Army and other uniformed services to replace the service number system used since World War I days, and the Veterans Administration for benefit program purposes.

Following a policy decision, the Bell System has secured the Social Security numbers of most persons applying for telephone service. In a most matter-of-fact manner, the telephone company business offices ask and in almost all cases get the numbers. The company explanation is that the SSN helps in credit-checking, which leads to a conclusion that credit reporting companies' data banks

also operate with SSN as the major identifier.

The HEW Secretary's Advisory Committee report notes that "... the Federal government itself has been in the forefront of expanding the use of the SSN. All these actions have actively promoted the tendency to depend more and more on the SSN as an identifier-- of workers, taxpayers, automobile drivers, students, welfare beneficiaries, civil servants, servicemen, veterans, pensioners, and so on. If use of the SSN as an identifier continues to expand, the incentives to link records and to broaden access to them are likely to increase..." (p. 121)

The HEW report continues the discussion of the expanding use, or over-use, or even abuse, of the SSN by noting that safeguards are needed, otherwise "...there can be no assurance that the consequences for individuals of such linking and accessibility will be benign. At best, individuals may be frustrated and annoyed by unwarranted exchanges of information about them. At worst, they may be threatened with denial of status and benefits without due process, since at the present time record linking and access are, in the main, accomplished without any provision for the data subject to protest, interfere, correct, comment, and in most instances, even to know what linking of which records is taking place for what purposes." (p. 121)

The HEW Advisory Committee recommended against use of SSN's as the standard identifiers, by legislative and administrative means. The report insists throughout that the challenges raised by computer-based personal data record-keeping should be examined broadly as important issues of social policy rather than as narrowly conceived questions of record-keeping technique and imaginative system design.

The Moorhead Subcommittee has taken this report under close study, in preparation for the hearings.

The Subcommittee should be urged to inquire of "The Good News Publishing Company," of Canton, Ohio, about its advertisements such as the one appearing in Parade magazine of October 7, 1973. In the ad, "Good News" offers a book of advise on Social Security problems and benefits. The coupon for ordering the book contains space for the book-buyer to fill in name, address, and Social Security number. "Good News" promises to send that portion of the order coupon "to the proper government office," presumably the Social Security Administration, HEW.

Does "Good News" make a copy of the "Request for Statement of Earnings" portion of the coupon? For which reasons? To whom would such SSN information be conveyed, and for what purposes would such persons or companies be securing and keeping such information?

advertisement

Parade Magazine
10-7-73
October 7, 1973

How to collect from Social Security at any age!

Would you like to know how much money you have invested in Social Security right to the penny? Then would you like to know how to get the most from that investment including all the brand new Social Security benefits? Now you can do both by using the short easy coupon at the bottom of this page. Here is the way it works. The left half of the coupon will be sent to the proper government office. They will run a check on your account and then send you a report in a confidential sealed envelope. This report will tell you how much of your earnings have been recorded in your Social Security account year by year. There is no charge for this service, not even postage.

The right half of the coupon will be used as a shipping label to send you a copy of a new book entitled, "How to collect from Social Security at any age." If you think that you have to wait until retirement age to start collecting your Social Security benefits, this book will really open your eyes. Here are some of the little-known facts about Social Security you will find out about in this book:

- How to increase the amount of your payment if you are already on Social Security.
- How to collect your share of the brand new Social Security benefits just passed by Congress.
- How to qualify for Social Security disability pensions at any age.
- How to increase your Social Security benefits.
- How to report your Farm income for Social Security.
- How to make your whole family eligible for Social Security benefits, even your youngest children.
- How to replace a lost Social Security card.
- How to replace a lost Social Security check.
- How to get a refund if you have overpaid your Social Security taxes. (Studies show that two out of three people overpay.)
- How to figure out what your Social Security retirement payments should be.
- Should you tatoo your Social Security number on your body?
- What papers do you need in order to file a Social Security claim?
- How ten million people who are only 30 years old, on the average, collect Social Security.
- Should you get a divorce in order to get more Social Security? (a lot of people already have.)
- Should you have two Social Security cards?
- How to get a huge lump sum Social Security payoff.
- How to make sure your employer is not cheating you on your Social Security.
- How you may be cheating yourself out of your Social Security benefits.
- When are the five times you should get in touch with your Social Security office?
- How to work and still get Social Security benefits.
- How to cash in on Social Security even if you've never paid a penny into it.
- How to get hospital and medical insurance for the aged.
- How students between the ages of 18 and 22 can get Social Security cash benefits.
- How to get the special Social Security benefits that are only for veterans.

Although this book can mean hundreds and perhaps thousands of dollars to you, it is priced at only $3.00. Remember, it is not enough to qualify for your Social Security benefits. To get your benefits you must know how to apply for them. The book tells you how to qualify, who to contact—including all necessary addresses, and what to say. This is a 100% no risk offer. If you do not like the book, return it and your $3.00 will be immediately refunded. You will still get the confidential report on your Social Security account.

If you do not take advantage of your new Social Security benefits, you are only cheating yourself, after all, you have already paid for them. It is easy to start getting your new Social Security benefits. Just fill out both parts of the coupon below. Mail the coupon and $3.00 in cash, check or money order to The Good News Publishing Co., 1818 Whipple Ave. N.W., Canton, Ohio, 44708. The book will be sent to you immediately by return mail. Your confidential Social Security report will be mailed to you separately as soon as the government has finished checking on your account. Checks and money orders should be made payable to The Good News Publishing Company.

120

REQUEST FOR STATEMENT OF EARNINGS

SOCIAL SECURITY NUMBER → | | | |

DATE OF BIRTH → MONTH | DAY | YEAR

Please send a statement of my Social Security earnings to:

NAME { MISS / MRS. / MR. } _____

(Print Name and Address in ink Or Use Typewriter)

STREET & NUMBER _____

CITY & STATE _____ ZIP CODE _____

SIGN YOUR NAME HERE (DO NOT PRINT) _____

Sign your own name only. Under the law, information in your social security record is confidential and anyone who signs another person's name can be prosecuted. If you have changed your name from that shown on your social security card, please copy your name below exactly as it appears on your card.

24

Please send me _____ copies of your report "HOW TO COLLECT FROM SOCIAL SECURITY AT ANY AGE" to the address below:

Make check payable to **THE GOOD NEWS PUBLISHING COMPANY**
1818 Whipple Avenue, N.W.
Canton, Ohio 44708

SHIPPING LABEL

NAME _____

ADDRESS _____

CITY _____

STATE _____ ZIP _____

121

DATA BANKS PROBLEMS

Although President Nixon said the time is right for a major initiative to define citizens' rights in the data bank privacy area, the response to be expected will be weak. In the State of the Union address of January 30, 1974, Nixon appeared to call for new safeguards of privacy and basic rights.

The flaw in the Nixon speech was an implicit view that the privacy problem is simply that of ensuring that the machinery, such as computer data banks, "bugs," wiretaps and other snooping aids, are not improperly used. The major defect in this approach is that the technology can be easily used, often without detection. What clearly is needed today, in order to protect the rights of the First and Fourth Amendments to the Constitution, is stringent law which would be analogous to the statutes forbidding the mere possession of machine guns and other automatic weapons.

The last decade of American history has shown conclusively that the existence of a device automatically leads to the use of that device --- and probable abuse.

In July 1973, the Department of HEW released the Report of the Secretary's Advisory Committee on Automated Personal Data Systems, entitled "Records, Computers and the Rights of Citizens." This report explores the many ways in which governments can store vast amounts of data on individuals, without concern for the issues of privacy involved. This HEW report makes a number of recommendations

for legislation and agency regulations.

Rep. Barry Goldwater, Jr., has introduced H. R. 11275, the "Code of Fair Information Practices Act of 1973," to legislate the safeguards described in the HEW report. The Goldwater bill, which includes as co-sponsors liberal Democrats and conservative Republicans, would accomplish 3 basic guarantees for the individual: (1) the right to know the content of computer-stored information, (2) the right to contest the legitimacy of such information, and (3) the right to be informed of all uses of such computer-based files.

The HEW report cites problems in the area of criminal records in computerized systems, making several recommendations to curb the possibility of abuse.

As of mid-February 1974, the Department of Justice did not have a unified position on the corrective legislation.

APPENDIX O

Statement of a CWA Local President on Monitoring

As I understand it, the two reasons the _____ Company finds it necessary to monitor telephone lines is for training and service observing. I cannot testify one way or the other on the benefits to telephone business on service observing. But I can testify to the monitoring aspect for training purposes. I have worked on the test desk for well over 25 years. This job consists of testing all reported subscriber lines, determining where the trouble is located, working with outside men on the poles, etc. My position can be monitored from at least two different locations. One of the positions, I know of, is a small room which supervisors use for their breaks to have coffee. Besides the office coffee pot it consists of a monitoring system for all the telephone lines in the entire test center (all test desk positions, control and dispatch center, repair service positions, and telephones located in the frame room.) All of these positions consist of outside telephone lines as well as inter-company lines in which, in the performance of their job, the employee talks to various subscribers. These subscribers conversations were monitored without their knowledge. Furthermore, there were supervisors, while drinking their coffee, who were listening to conversations on a loudspeaker, of employees conversations who did not even work for them. Many of our members make and receive personal calls. We have always suspected, but could never prove, that their personal calls were also monitored by some supervisor. There were certain remarks made by supervisors which tended to make up believe that personal calls were monitored. But again we had no way of proving it. As President of the union I receive calls on the test desk from members who have problems with the company, from other union officials on

business of the local, and from various district plant managers on company-union problems. On one such occasion, a man returning from upstairs, stopped in the middle of the test center and could hear my conversation. He reported to me that something was wrong because he could hear my telephone conversation while standing in the middle of the test center. I, immediately, hollered real loud and you could hear my voice coming out of a loudspeaker in the 2nd line foreman's office. Needless to say, I raised so much hell with the District Plant Manager about this that he agreed to allow me to receive union calls on my supervisor's telephone which was not on the monitoring system in this office. I have my suspicions that it was monitored from someplace else. As to secrecy of telephone communications in this office, we had none. As to the excuse to monitor for training purposes, in all my years in this job, I was never <u>once</u> taken aside and told that I didn't handle this call properly, etc. The point is the monitoring was done for the sake of monitoring and not for training. Most other test centers are equipt for monitoring in various ways - the same as this particular test center. Any information which I thought was of a personal or confidential nature, I would certainly not speak of it over any telephone line. It is a hell of a feeling to converse on the telephone with the thought in mind that your conversation is being monitored in the back room.

Statement of a CWA Local Vice President on Monitoring

March 17, 1974

Mr. _____
President, CWA Local _____
_____
_____

Dear _____:

In answer to your request of information pertaining to telephone company monitoring systems, let me tell you of what I know about the "service observing system" in _____.

The service observing desk is located in the traffic department in the _____ central office. Two girls operate this desk and their tours are very unusual. They may cover the desk at any hour. Sometimes the desk is manned late at night, sometimes very early in the morning and on occasion not at all. On rare occasions both girls may be working together for the board has two positions. The board is located in a room by itself and the only person in there are the girls who operate the desk.

The service observing system itself is very elaborate. At present the desk can monitor calls in _____ and _____, but I understand that another remote end is being established in _____. Each week a list of working central office equipment is given to the central office repairman. The repairman places observing leads on this equipment and from then on when ever a call is made from one of these lines, the number dialed is printed out on a tape at the observing desk. The observer then operates a key which enable her to monitor that line. She is supposed to only listen long enough to determine if the call went through without experiencing trouble, but there is nothing to prevent her from continuing to listen.

The observer can monitor only one line at a time. If she is monitoring a call from a _____ lead, she cannot receive anything from any of the others. However in _____ there are 20 leads placed each week and in _____, 37. So you see there would almost constantly be a call on one of the leads.

I hope this information helps you in your investigation of monitoring systems.

Very truly yours,

_____
_____

Statement of: Louis B. Knecht,
Executive Vice President,
Communications Workers of America

Before the Committee on the Judiciary,
House of Delegates,
General Assembly of Maryland

Mr. Chairman, my name is Louis B. Knecht. I am Executive Vice President of the Communications Workers of America, a labor union representing one-half million men and women employed in the telephone and other industries. Accompanying me is John Morgan, Administrative Assistant to the President of the union. We both reside in Montgomery County.

We who work in the communications industry are greatly concerned over the actual and possible abuses of the technology now existent. We have been following the areas of privacy and wiretapping or monitoring for a number of years.

We are here today to voice the support of the union for House Bill 1678. As we read it, the bill would add several provisions to the criminal laws of Maryland to restrict monitoring of conversations over telephone circuits. House Bill 1678 includes several good features of House Bill 962, which was vetoed June 1, 1973.

Mr. Chairman, the Omnibus Safe Streets and Crime Control Act of 1968, Public Law 90-351, made important and unwise changes in Federal laws dealing with communications privacy. Title III of the 1968 Act specifically allows telephone companies to monitor telephone conversations "for mechanical or service quality checks." The same Title gives identical powers to the Federal Communications Commission. Those who intercept by this legalized means are allowed in the course of their employment to disclose contents of communications. The legislative intent of that part of the 1968 Act was theoretically to allow monitoring for purposes of service quality observing, not for disciplining employees.

Unfortunately, the law's anticipated safeguards have not proven effective. The current Watergate scandal has shown how many problem areas exist. CWA is attempting to secure repeal of the too-permissive, unwise Federal law and to seek strengthening of safeguards. Further on, I will comment on this activity.

H.B. 1678 sets forth new restrictions on telephone companies, their officers, employees and agents. For more than 50 years, the stated policy of telephone companies has been to monitor in order to evaluate the quality of service. This type of monitoring was written into the 1968 Federal law. However, by a stretching of the legislative intent of that 1968 Act, the telephone companies are continuing to use monitoring for disciplinary purposes. Recording by electronic devices and written notes has been used to form the basis for disciplinary action.

CWA is especially interested in enactment of the proposed Section 557-I, which has several employee protections. Telephone companies would be allowed to continue the practice of monitoring, if necessary to observe service quality. However, all forms of written and electronic recording would be prohibited. The section would protect an employee from having his or her calls recorded. At times, it is necessary for an employee to call a doctor, a lawyer, a clergyman or spouse because of a personal problem. It is possible that the contents of such telephone calls would be included in the employee's personnel file.

Mr. Chairman, we believe service monitoring records are not infallible. We have seen a number of injustices done to employees, and wish to provide a few examples from our files.

A few years ago, a Bell System company allowed installation of a telephone monitoring console in the bedroom of a chief operator's home, in order that the supervisor might monitor without detection. After several employees were dismissed because of the records from this monitoring, CWA fought the case through the State's labor relations agency. After a long proceeding, the company was required to pay back wages and otherwise make amends. The State agency ruled for the employees because

no visual and thus positive observation was possible.

We at CWA often have attempted to imagine the kind of person who would have monitoring equipment installed in her bedroom. And we have wondered whether that chief operator ever allowed her friends to listen in, possibly as a more interesting evening pastime than watching TV.

The written records of monitoring, on prepared forms, contain many areas best described as subjective. For example, the operator can get demerits for "faulty judgment," "faulty start of conversation," or "failed to be helpful." The form contains many other subjective "criteria."

In business offices, the Bell System has used devices other than telephone taps to listen in on conversations between customer and employee. The monitoring can be done through concealed microphones installed in the desk calendar-inkpen unit. CWA has acquired pages from Western Electric supply catalogs, with drawings and descriptions of use given. In the use of this equipment, I would point out that neither party to the conversation would be giving consent to the eavesdropping.

Telephone technology now has advanced to the stage where remote monitoring is possible, with little limitation on location. Equipment in certain central offices can be accessed by the use only of a push-button telephone, on which a certain sequence of digits is punched. In the event some unauthorized person has gained access to the code numbers, he can listen in without detection on the line of his choice. The abuse of such equipment is a chilling prospect.

Another example I will cite is the use of "Voiceprint" technology against a CWA member in California, who was suspected of having telephoned a bomb threat to a recording device in the installation order office. On a cheap recording device, the company secured another sample of this man's voice, and let the "experts" in "Voiceprint" technology analyze the two voice samples. The "experts" were able to "confirm" that our member was the culprit. After long and arduous work by the member's lawyer, the court dismissed the case. A most persuasive factor in the

dismissal was an analysis of "Voiceprint" in a Department of Justice-financed study. An error rate of up to 32% of voice samples was demonstrated in the study.

My final example is the discovery in 1970 that the Civil Defense "hot line" in the offices of Governor Mandel and five other Governors had been "incorrectly wired," the explanations given by some very defensive Federal and Bell System officials. The transmitter unit of each of the "hot line" telephones had been wired around the transmitter cutoff switch, so that each was an open microphone. There were the usual denials of intent to eavesdrop on the Governors.

The Wall Street Journal of March 21, 1974, provided a good roundup of the manner in which company management within and without the telephone industry can monitor employee-customer contacts. I will leave a copy of the article for the Committee's use. Only two weeks ago, as reported in the Washington Post, the FBI discovered and confiscated monitoring devices found in the offices of salesmen of several Baltimore automobile dealers. The dealers are accused of using the devices to eavesdrop on customers who were in those rooms without the salesman being present. The dealers are suspected of learning the thinking of customers regarding car purchases.

If those allegations prove true, I hope the Federal Government will impose heavy penalties on the guilty parties, as an example of the fate awaiting the person who uses wholly illegal means of gaining access to one's thoughts and private discussions.

Mr. Chairman, earlier I mentioned that CWA wants genuine safeguards in Federal wiretapping laws. The union has made a strong case on the subject to the Speaker of the House of Representatives, who soon must make appointments to the National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance. This Commission, provided for in Section 804 of the 1968 Omnibus Crime Control and Safe Streets Act, will begin functioning June 19, 1974, with

its final report one year later. The Commission will examine how well or poorly the nation has been served by six years of monitoring, wiretapping and eavesdropping authority granted by the 1968 Act. Included on that Commission are members already named by the President and the President of the Senate.

Mr. Chairman, amendments to Federal law unfortunately will be long in coming. Therefore, CWA urges enactment this year of H.B. 1678, to make a start on the task of restricting the practice of monitoring.

[From The Wall Street Journal, Mar. 21, 1974]

LISTENING IN.—CONCERNS EAVESDROP ON EMPLOYES' PHONE CALLS; FIRMS DEFEND MOVE, BUT WORKERS ARE ANGRY

(By Jim Montgomery)

ATLANTA.—Larry Marthaler, reservations manager here for Pan American World Airways, flicks a couple of switches on the telephone sets atop his desk and tunes into one of his 20 agents talking with a customer. The agent doesn't know that Mr. Marthaler is listening, or that the conversation may be one of a half-dozen in tapes each month for later review with the agent to point out strengths and weaknesses in his work.

"It's valuable to the individual to hear himself," Mr. Marthaler says.

The agents don't exactly see it that way. Teamsters Union shop steward Betty Moore says it's "kind of a sore subject. Whether constructive or not," she says, the monitoring "intimidates them. . . . If the employes had a choice, they'd vote unanimously to get rid of it."

The employes don't have a choice, but at least they know that they may be monitored. In every state except this one—Georgia— and California, companies and individuals are free to monitor their own telephones without telling the people who use the telephones. Unlike federally regulated wiretapping by law-enforcement officials of other people's telephones, the monitors can do so without a court order.

Telephone companies in every state offer to rent monitoring equipment, which permits listening-in without telltale clicks or background noise. But California requires a beeper to be used on monitored phones. And last August, the Georgia Public Service Commission, which already had required monitors to get licenses, also required them to put a bright orange label on monitored phones and an asterisk beside the directory listing of monitored phones. Here in Georgia, it quickly becomes apparent that:

THE IRS MAY LISTEN

—Rather than make known their monitoring, many companies stop it.

—No matter how noble the purpose of monitoring, employes dislike it.

—And some influential eavesdroppers—the Internal Revenue Service, for example—ignore state regulations.

Georgia's list of licensed monitors ranges from the First Baptist Church of Thomasville, Ga. and the Regency Hyatt Hotel in Atlanta, both of which have stopped monitoring, to Avon Products and the Atlanta police department, which haven't. Currently, there are 72 businesses and five governmental units on the list. They include Delta, Eastern and United air lines; the Davison's unit of Macy's, Rich's and Sears, Roebuck, all department stores, the Atlanta Journal and Constitution newspapers; a variety of answering services, collection agencies and credit bureaus; the Veterans Administration and the U.S. Marine Corps.

Not on the list is the Atlanta office of the Internal Revenue Service, though it secretly monitors more than 100 telephone conversations a day between IRS employes and taxpayers asking for help with their returns. The IRS says it does the same thing all over the country.

Presumably, both the IRS and Southern Bell Telephone are in violation of the Georgia law. It requires a monitor to get a license and prohibits the telephone company from installing monitoring equipment for a telephone user who has no license. The legal issue aside, an IRS spokesman says there's nothing wrong with the agency's monitoring because it is only trying to improve its information service. Besides, he says, callers "never give their names."

DO FEDS NEED A LICENSE?

Southern Bell says it installed the monitoring equipment after being told by the IRS that IRS attorneys held that a federal agency doesn't need a license. The IRS says its lawyers are still considering the license question. (Curiously, however, another IRS office in Atlanta applied for a license in December, then withdrew the application in January because it "no longer anticipated that we will need (the telephone monitoring equipment) for quick quality control.")

Georgia Public Service Commission officials, when informed yesterday of the IRS installation, said they can't find a license exemption for federal agencies in the state law. Noting that two other federal agencies do have monitoring

licenses, the commissioner said its five-man board will review the IRS situation at its next regular meeting on April 2 or possibly sooner at a special meeting. If there appears to be a conflict between state and federal laws, an official adds, the commission will seek an opinion from Georgia's attorney general.

The House Government Information subcommittee plans hearings on monitoring by federal agencies this spring. The subcommittee investigated the government's "telephone snooping techniques," as it called monitoring activities, in 1970, but no federal legislation resulted. In that year the subcommittee found that at least 52 federal agencies permitted monitoring, often without disclosure to callers.

The subcommittee concluded that "until the practice of monitoring is abolished, a citizen will never be able to know for sure to what extent, or for what underlying motive, he is unwittingly sharing his telephone calls with secret listeners." Now, according to Norman G. Cornish, deputy staff director of the subcommittee, "much more sophisticated" equipment is being used in secret monitoring, which he calls "pretty insidious."

Telephone companies resent such criticism. They defend monitoring as an "essential quality-control procedure." The only reason they offer monitoring equipment, they say, is to permit employers to train and evaluate the work of employes who deal with the public by phone.

BUILDING A CASE

The Communications Workers of America and others dispute that. They say telephone companies themselves sometimes use monitoring as a disciplinary tool. Union records in Atlanta show recurrent grievances over employe suspensions and firings that appear to have been precipitated by monitoring. The phone company uses monitoring to build cases against employes it wants to fire or persuade to quit, says Mrs. Edgel Crook, a CWA representative and a long-time telephone operator in Atlanta. Another CWA official says the company steps up monitoring of employes who are conspicuously late or absent. The telephone company says such actions would be contrary to policy, but concedes there may be occasional violations.

Critics of monitoring say the tendency of companies to drop it rather than disclose they engage in it implies sinister motives in the practice. Pacific Telephone & Telegraph's figures show that the number of customers using monitoring equipment is down to 578 now from 1,076 when the California Public Utilities Commission, in 1966, ordered an automatic beep every 15 seconds on monitored lines. In practice, however, the commission seems to have been less than vigilant in enforcing this requirement, leaving that up to the phone companies.

When Georgia required telephone labels and directory signals to identify monitored telephone lines, more than 50 of 143 monitors got their licenses cancelled.

Georgia law permits monitoring "solely for the purposes of business service improvement," which is left undefined. The state public service commission, however, did decide last year that Trust Co. of Georgia overstepped the bounds when it asked for a monitoring license to determine whether employes were using a Wide Area Telecommunications Service (WATS) line for personal calls during business hours. The commission rejected the application.

American Telephone & Telegraph Co. says its affiliates monitor, without the knowledge of callers, "approximately 3.5 million" of the roughly one billion calls the Bell System handles each month. Ma Bell is interested only in its operators' performance, says Paul Loser, an assistant vice president of operations at AT&T, and he says "we don't listen to customers talking to other customers, period." He says also that the Bell System rents monitoring equipment only to employers who agree in writing to use it "exclusively" for employe training and quality control, and who also agree to notify all employes that it is being used.

But critics say that wide misuse of monitoring is indicated by the fact that one guilty party has been the nation's guardian of communications—the Federal Communications Commission. The FCC got some special equipment from Chesapeake & Potomac Telephone Co., a unit of AT&T, in 1970 to use in an attempt to trace information leaks, which proved futile.

After probing the episode in 1972, the House Commerce Committee's investigations subcommittee, chaired by Rep. Harley O. Staggers (D., W.Va), sternly rebuked the FCC for having eavesdropped "without legal authority and in direct contravention of the law and its own regulations." The FCC never conceded wrong-doing, but Dean Burch, then the FCC chairman, who had approved the snooping, promised the House panel that "it will not happen again."

COMMUNICATIONS, WORKERS OF AMERICA,
Washington, D.C., July 3, 1974.

Hon. WILLIAM S. MOORHEAD,
Chairman, Foreign Operations and Government Information Subcommittee, Government Operations Committee, House of Representatives, Rayburn House Office Building, Washington, D.C.

DEAR MR. CHAIRMAN: Because of your subcommittee's continuing interest in the use of monitoring techniques and equipment in telephone systems, I am enclosing a resolution adopted by this union's convention on June 27, 1974, together with the verbatim record of the floor proceedings on that resolution. I would be pleased if you would insert these materals in the record of your hearings of June 11 and 13, 1974, at which it was my privilege to testify.

For your further information, I also enclose a copy of an article from Business Week of June 22, 1974, which deals with the determination by a Bell System company that ". . . a relatively small percentage of telephone customers was responsible for the vast majority of calls for information." Two methods of ascertaining the originating numbers are suggested: First, the use of remote observing equipment, to determine and make records of the calling numbers to Information, or second, a computerized retrieval of the "411" signals sent by telephone instruments in the Cincinnati service area. The latter retrieval could be accomplished in much the same fashion as that of the ordinary customer-dialed long distance ("DDD") call. Perhaps the subcommittee would be interested in learning the basis for the company executive's statement, as an adjunct to the telephone monitoring inquiry.

Sincerely yours,

GLENN E. WATTS,
President.

AN END TO FREE PHONE INFORMATION

Along with "number, please" and the nickel pay phone, free information service for telephone subscribers seems headed for oblivion. Led by Cincinnati Bell, Inc., which for three months has been charging 20¢ for each call made for "directory assistance," most telephone operating companies are likely to impose information charges on subscribers in the next year or two. New York Telephone Co. and Wisconsin Telephone Co. are already making the move.

So far, Cincinnati Bell is the only major telephone company to try the new charge, and the results have been spectacular. In a month, directory assistance calls dropped by 80% from residences and 75% from business. "This thing will become nationwide in one form or another," predicts Richard T. Dugan, president of Cincinnati Bell. "Ninety-five percent of the customers have a better deal—now." In others words 5% of Cincinnati Bell's customers are paying for 95% of directory assistance billings.

LOWER CHARGES

The idea of the information charge is a natural for telephone companies trying to cut labor costs. But none dared try it until analyses of calls for directory assistance proved that a relatively small percentage of telephone subscribers was responsible for the vast majority of calls for information. Dugan calls them "abusers" and claims they are subsidized by the average subscriber. Cincinnati Bell worked out a formula of three free information calls a month with a 20¢ charge for each call in excess. The Ohio Public Utilities Commission went along, in lieu of granting a 25¢ per month rate increase.

New York Tel will cut 30¢ off phone bills and will also offer its subscribers three free directory assistance calls per month. The New York plan, which will take almost a year to put into effect, exempts handicapped customers and pay phones from charges, and there will be no charge for long distance inquiries or when telephone numbers are unlisted at the subscribers' request.

Both Cincinnati and New York will charge for calls to new listings that are not yet published in directories, and that has caused some protest. In Cincinnati,

City Councilman Guy Guckenberger says charging for such new listings "is not fair at all," and he cites a recent Peanuts cartoon inspired by the New York plan: "It's like a grocery store charging to tell you where the peanut butter is."

Cincinnati Bell's Dugan claims that the most serious objections came from businesses that have utilized directory information calls for credit checks and delivery addresses. "I tell them, 'I agree you have a problem, but I don't agree that your neighbor should pay your cost of getting the information,'" he says.

ELASTICITY

In one respect, the change brought a big surprise to the phone company, Dugan admits. "We estimated revenues of $113,000 a month and savings of $12,000, but because there are so many fewer DA calls, revenue is only $19,000 and costs are down $74,000." The big savings come from a 24% reduction in the operator force from 312 in January to a current 237. Although some job switching was necessary, there were no layoffs. Operator jobs have high turnover, and the company made the cuts in its operator force by attrition.

Dugan admits some things about the Cincinnati plan are not ideal, particularly charging for existing numbers that have not yet been published in directories and for failures to locate a number. But, he argues, the three free calls and the lower monthly service charge make up for it. "Essentially," muses Dugan "we are making money by not getting more calls."

CWA 1974 CONVENTION RESOLUTION 36A–74–7

SERVICE MONITORING

Telephone companies of the United States, by their own statements, acknowledge that they have employed the technique of service monitoring for at least the last 65 years. Monitoring is "the company's quality control tool," according to the official policy statements.

The current legal authority for service monitoring was included in the "Omnibus Crime Control and Safe Streets Act of 1968," to clarify the right of a telephone company to examine the quality of service being provided. The key concepts in the 1968 legislation were to allow service observing and monitoring on a random basis solely ". . . for mechanical or service quality checks." Use of information secured by monitoring for discipline was not written into the 1968 Act.

The Bell System in September 1966 began stating in testimony and in other public situations that it does not monitor customer-to-customer telephone conversations. However, the system-wide halt to that practice reportedly occurred on June 1 of that year, after announcement of Senate hearings on the subject of invasion of privacy in telephone systems. Strong interrogation of company witnesses was required to establish the chain of events leading to the discontinuation of the practice for the hearings record.

Observing-monitoring practice, according to company pronouncements, is not to tape-record conversations between customer and company employee. However, there has been a practice of taking notes on monitored conversations, using standard forms, as a first step toward discipline. The forms and techniques are, in the eyes of the companies, to provide the gauge for accuracy and completeness of operators' services and the effectiveness of employees who process trouble calls and business transactions. The following "service indicators" typically are included on the service observation forms:

"Failed to be helpful."

"Faulty judgment."

"Faulty start of conversation."

"Faulty voice."

None of those could be called objective.

Such information in any employee's records is subject to use in disciplinary proceedings. In most instances, the observer is not in visual contact with the employee.

In 1971, the California Public Utility Commission ruled that telephone companies may not legally use information obtained by supervisory monitoring for disciplinary purposes, unless the employees involved were given notice of monitoring. The proceedings before that Commission had established that telephone companies were disciplining employees on the basis of personnel file entries generated by monitoring.

In response to the telephone companies' claim that secret monitoring is needed to keep control over the work force, the California Commission stated: "It is not necessary to sacrifice for ease of employee discipline the principle that, if the privacy of a communication is being violated, notice should be given of the violation of the privacy." The California Commission added that monitoring may be used to determine if employees need retraining.

CWA believes the time is long past due for a tightening of Federal law on the practices of monitoring and service observing. The 1968 Crime Control Act contains an opportunity, in that it provides for establishment of the National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance. The Commission's report and recommendations are due to be presented to the President and Congress in June 1975.

Be it resolved: That the Communications Workers of America urge the National Commission to look specifically into abuses of the 1968 Act's authority, and call on Congress to enact amendments to that law so as to prohibit the use of information obtained by service observing or random monitoring to discipline employees; and be it further

Resolved: That the Union at all levels press for other Congressional and public commission inquiries into the broad area of invasion of privacy, to lead to more effective laws which will severely circumscribe all forms of monitoring and wiretapping to protect the privacy of individuals and employees.

"Be it further Resolved: That in all states, working through the various AFL–CIO Councils, introduce legislation to prohibit any monitoring of telephones without the specific approval of the subscriber or the employee."

Mr. Chairman, the Resolutions Committee moves the adoption of Resolution 36A–74–7. (Applause)

President WATTS. You have heard the Resolution. There is obvious support from the floor.

Microphone No. 1, Delegate Boyce, Local 4108.

Delegate WILLIAM H. BOYCE (Local 4108). Mr. Chairman, I would like to amend the Resolution on the following lines. Line 18, insert the word "reportedly" between the words "practice" and "occurred."

That would make that more meaningful, I believe.

On line 74, insert the words "at all levels" between the words "Union" and "press."

This would have the Locals as well as the International working on this problem.

And on line 75, I would like to insert the words "and public commissions to make" between the words "Congressional" and "inquiries."

That would encourage the Locals, or the states to go to their public utility commissions.

President WATTS. Do you have that written down so I can have it in hand, please?

Delegate BOYCE. Yes, I do.

President WATTS. To be sure that we all have this now, if you will turn to line 18, the motion is to amend to insert, between the words "practice" and "occurred" the word "reportedly."

And then on line 74, between the words "Union" and "press," insert the words "at all levels."

And then on line 75, insert between the words "Congressional" and "inquiries" the words "and public commissions."

Is there a second to the motion?

The motion was duly seconded.

President WATTS. Seconded from the floor.

The Delegate at Microphone No. 1, for the purpose of speaking on his motion. Microphone No. 1.

Delegate BOYCE. Mr. Chairman, fellow Delegates: The Bell System and various other independent telephone companies are not the only companies to employ monitoring, or better known by its real name, telephone snooping techniques. Such nationally known firms and corporations as Pan American, Delta, Eastern, and United Airlines, large department stores, such as Sears Roebuck, Macy's, Rich's, are some of the better known eavesdroppers.

Currently there are 72 businesses and 5 governmental agencies on that list, as reported in the Wall Street Journal, on Thursday, March the 21st, 1974.

The telephone companies in every state are offering to rent monitoring equipment. A.T. & T. says its affiliates monitor approximately 3.5 million of the roughly 1 billion calls the Bell System handles each month, without the knowledge of the customer.

According to Mr. Paul Loser, Assistant Vice President of Operations, A.T. & T., he also stated that the Bell System rents monitoring equipment only to employers who agree in writing to use it exclusively for employee training and quality control and who also agree to notify all employees that it is being used—an agreement they themselves do not ask their own companies to abide by or uphold.

In Michigan we have at this time grievances on monitoring of employees because it is used as a disciplinary tool and has been used to demote an employee. The telephone companies themselves used monitoring as a disciplinary tool. Union records show recurrent grievances over employees suspensions and firings that appear to have been precipitated by monitoring.

The telephone company uses monitoring to build cases against employees it wants to fire or persuade to quit. The tendency of the telephone company to drop monitoring rather than disclose that they are engaged in it implies shady motives in the practice.

In 1966 the California Public Utilities Commission ordered an automatic beep every 15 seconds on monitored lines, and last August the Georgia Public Service Commission required them to put a bright orange label on monitored phones and an asterisk beside the directory listing of monitored phones. However, some of these practices have been left up to the discretion of the phone companies to enforce.

I ask your support on my amendment and the Resolution. Thank you. (Applause)

President Watts. At Microphone No. 3, Delegate Kruske, Local 4108.

Delegate Betty A. Kruske (Local 4108). I'd like to speak in favor of this amendment.

We have seen what monitoring has done in Commercial and Traffic, and now, like a disease, the company is spreading it from department to department. Eventually, they are going to figure out how to monitor trucks.

We can't afford to sit still any longer and let our members be degraded, disciplined, and demoted, suspended, and fired because of the company's practice on monitoring, and because of the loopholes that have been left in the U.S. Code and the state laws that allow the company to do this.

Contact your legislators, your public service commissions, and let's close these loopholes once and for all. (Applause)

President Watts. Permit me to clarify the situation for just a moment.

We have an amendment to the Resolution. The people who are standing at the floor microphone were standing there to speak on the motion. We are beginning to recognize them now, and they are speaking on the amendment. The amendment, though, really does not change the motion, and it appears to me that you are making your points very well on both.

We are going to have to vote twice. We are going to have to vote on the amendment, and then on the question of the Resolution as amended or not amended. I will continue to recognize you in the same way, nevertheless.

At Microphone No. 3, Delegate Gillette, Local 4103.

Delegate Evelyn R. Gillette (Local 4103). Mr. Chairman, Fellow Delegates, and Guests: I rise to speak in favor of both the amendment and the Resolution.

Being a member of the Traffic Department for many years, I feel well qualified to speak against this unfair practice of monitoring, eavesdropping, or, more commonly, spying. Now the Plant Department has started this unfair practice with their line status verifiers and remote monitoring. The information they are receiving from this monitoring is being used for evaluation and threats of disciplinary action.

Let's stop this unfair practice. I urge your support of both this amendment and the Resolution. Thank you. (Applause)

President Watts. Microphone No. 5, Delegate Martin, Local 6012.

Delegate Lloyd E. Martin (Local 6012). I have a question on this line 18. As I understand, it said after "practice," "reportedly occurred." Now can the Resolutions Committee tell me whether this occurred, or reportedly occurred? I think it makes a difference to say if a practice reportedly occurred, or whether it actually occurred. Or did I understand that part?

President Watts. Can the Resolutions Committee answer the question?

Chairman Crabtree (Resolutions Committee). In regard to the question, the statement that your are asking about is testimony taken from the system by the Senate. It is a statement from the hearings, that the company allegedly stated that they reportedly, or they had stopped the practice of monitoring.

President Watts. You are entitled to a second question.

Delegate Martin. This is a fact, then?

President Watts. Well, it is a fact that a representative of the A.T. & T., when testifying before the Congress, stated that they had stopped. Whether or not they have actually stopped, we cannot say with certainty at this momcnt.

At Microphone No. 1, Delegate Dickerson, Local 12143.

Delegate Carol Dickerson (Local 12143). Mr. Chairman, I move the previous question.

The motion was regularly seconded.

President Watts. You have heard the motion to close debate. There is a second from the floor. The motion is not debatable. It requires a two-thirds vote.

Will all those in favor of the motion to close debate, signify by raising their right hand? Down hands. Opposed, by a like sign. Down hands. The motion to close debate is carried.

We are now on the question of the amendment that has been proposed to the Resolution. Will all those in favor of the amendment to the Resolution, signify by raising their right hands? Down hands. Opposed, by a like sign. Down hands. The amendment is carried, and the question is now on the original motion.

At Microphone No. 3, Delegate Shelor, Local 2204.

Delegate Robert P. Shelor (Local 2204). Mr. Chairman, Brother and Sister Delegates: I rise to speak in favor of this Resolution. The term "service monitoring" is a mighty weak excuse the company uses for harrassing our members. It is a matter of record that employees are sometimes monitored for eight continuous hours. This cannot be service-connected and this cannot be tolerated.

Employees are monitored on selectivity. By this I mean if you're not in good with the boss, you will be monitored on until they can find something wrong. This is not service-connected, and this cannot be tolerated. (Applause)

The company has equipment capable of monitoring the quality of service, and there are adequate complaint departments if the customer is unhappy with our service. (Applause) And I believe the public supports our members in the service that they provide.

If the management of the A.T. & T. and other companies are present in the guest section today, then I think we should let them know that we support this Resolution one hundred percent—nothing less. (Applause and cheers)

I urge you to adopt this Resolution. Thank you. (Applause)

President Watts. Microphone No. 1, Delegate Forwood, Local 2100.

Delegate W. G. Forwood (Local 2100). I have a further Resolve to be added to the Resolution:

"Be it further Resolved: That in all states, working through the various AFL–CIO Councils, introduce legislation to prohibit any monitoring of telephones without the specific approval of the subscribers or the employees."

If I get a second, I'd like to speak on it.

The motion was regularly seconded.

President Watts. You have heard the motion. There has been a second from the floor. At Microphone No. 1, the Delegate wishes to speak on his motion.

There is a request to read the motion again. If you will permit me, Woody, I will. The motion is:

"Be it further Resolved: That in all states, working through the various AFL–CIO Councils, introduce legislation to prohibit any monitoring of telephones without the specific approval of the subscriber or the employee."

Microphone No. 1, Delegate Forwood.

Delegate Forwood. I have had some very serious problems on this monitoring, and I have known for a number of years that it has been going on with some of the employees because sometimes the supervisors let little things slip that happened during personal conversations. And it's pretty hard to tie them down, but we know for sure that they are listening to personal conversations, and we have had a couple of very serious grievances in which they used some of the information which was gained from the personal conversation, and the company was upheld at the third step.

So we introduced a bill in the State Legislature for the first time, working through an AFL–CIO Council, and in the rush of business—a bill of this type is serious enough, and the members of the House of Delegates, in a rush, couldn't

give fair consideration. It was referred to the Legislative Council which meets between sessions. There will be another hearing on July 9, in which we will have the opportunity to go down and spend more time.

However, we still have this problem, especially in the small towns. Some of the very men that are the ones that put up the service observing leads are the ones that are assigned to service those very leads. And in the small towns, some of the various people that do the service observing know the people that they are listening to.

I have a District Vice President at the present time, Ray Donnell, whom they told to put a service observer on his own line. We are in negotiations right now because he has requested, as a subscriber, that he is not having any trouble with his telephone, and he doesn't want them to monitor. And also as a District Vice President of the Local, that he feels that they are harrassing him to try to find out what we are going to do.

So I would urge, sincerely urge, everybody throughout all our states in our great Union, to introduce any kind of bills at all on this subject and maybe somewhere we can have some success. And if we introduce enough bills in enough states, maybe they will try to help do some correcting of the action themselves.

I urge you to support it. Thank you. (Applause)

President WATTS. There appears to be no Delegate desiring to speak on this proposed amendment to the Resolution. That being the case, the Chair will put the question.

Will those in favor of the motion to amend, signify by raising their right hand? Down hands. Those opposed, by a like sign. Down hands. The motion to amend has carried. (Applause)

Microphone No. 5, Delegate Brown, Local 4000.

Delegate MABEL G. BROWN (Local 4000). I wish to address my question, through the Chair, to the Chairman of the Resolutions Committee, and to all the Delegates considering the Resolution.

Service observers and service observing assistants are fellow Union members. In addition, there are also many related clerical jobs that are also performed by Union members. However, the Resolution makes no provision for the protection and placement of these members.

I would like to know if any thought has been given as to just what is going to happen to these members.

President WATTS. The Resolutions Committee?

Chairman CRABTREE (Resolutions Committee). The Resolutions Committee did take this under consideration. However, we feel that under the pure context of what the Resolution is proposing, that this would not affect the jobs that now exist on service monitoring as in the pure context of the Resolution.

President WATTS. You are entitled to a second question.

Delegate BROWN. If we are going to take affirmative action to do away with these titles, and I feel this Resolution would have that effect, shouldn't the Resolution be amended to include protection for our telephone Union members?

President WATTS. This, I think, we will classify as a rhetorical question, intended to suggest that the answer is, yes.

Microphone No. 3, Delegate Early, Local 2202.

Delegate DOROTHY S. EARLY (Local 2202). Monitoring, by the company's admission, is the company's quality control tool. What they fail to do is tell us what the name of that tool is.

We in the Traffic Department know it only too well. And if you don't know it, I'll tell you—it's "the axe." Every day, somewhere in our 12 Districts, at least one of our members have their service severed by a hatchet-wielding supervisor using this tool. They tell us they must monitor in order to protect the customer from bad service. They tell us that if an employee listens in on monitored conversations, she is breaking the secrecy of communications.

What they don't tell us is that when they monitor on the operators, they are usually looking for an infraction of what has been previously observed visually, or what has been reported by a fellow employee. What they don't tell us is not only do they listen, they write down every word, and then they discuss it among themselves, as well as the observed party. And then if the action results in disciplinary action, which it usually does, then they talk it over with all steps of the Union representation. They are actually breaking the secrecy of communications by repeating what was said over the telephone.

My question is this: Who is guilty in the greatest degree: the employee who just overhears; or the supervisor who hears, records, and discusses the conversations? (Applause) If the employee is subject to disciplinary action, isn't the management person subject to the same type of action? If they suspend a Union member, shouldn't they also suspend the management person? And if they use their quality control tool to chop off a Union member's income, shouldn't they also terminate the supervisor who has listened, recorded, and discussed the conversation?

At the third step of a grievance in my unit recently, they readily admitted that they sent this girl to an isolated position, had a G.C.O. come in one hour early to a remote place and observe on her in order to try to catch her making a personal call from the switchboard. A friend of hers had said that this is what she was doing.

Well, it was almost a failure as far as the company was concerned—almost. They didn't catch her making a phone call. They did catch her keeping her key open 21 seconds too long on one connection, and 54 seconds on another. And so, here and there, two hours after she returned from a two-months' sick leave, she was terminated and sent home by the company. We lost that grievance because they said they had proof that she monitored.

If this is the case—and this case was sheer entrapment—we should stand together today to say, this must stop. Others have said that this is spreading in other departments of the company as well as Traffic. I guess we have just gotten used to it, and didn't really realize how bad it was until we heard other people talking about it.

Their executioners use the quality control tool and cut the cord on the absentee guillotine to end the career of our Union members in their double-edge axe. I urge you not only to adopt this Resolution, but when you return to your homes, start letter-writing campaigns to your Congressmen to take action in passing laws that will protect not only the public from the invasion of their privacy, but will also protect our members from action taken against them through the practice of so-called service monitoring.

Thank you. (Applause)

President WATTS. Microphone No. 1, Delegate Monger, Local 10805.

Delegate PAUL B. MONGER. (Local 10805). Mr. Chairman, I move the previous question. (Applause)

The motion was duly seconded.

President WATTS. You have heard the motion to close debate. There is a second from the floor.

The motion is not debatable. It requires a two-thirds vote. All of those in favor of the motion signify by raising their right hand. Down hands. Opposed, by a like sign. Down hands. The motion is carried.

The question then is on the Resolution as it has been amended. Will all of those in favor of the Resolution as it has been amended signify by raising their right hand. Down hands. Those opposed, by a like sign. Down hands. The motion is adopted. (Applause)

Mr. WATTS. The Federal Government for many years has been the largest single user of telephone and related telecommunications services, spending several billion dollars each year. Some of that money and the related work effort, we are learning each day, goes into the practices of wiretapping and eavesdropping.

However, it is not necessary to spend large sums of money for equipment necessary to eavesdrop. For example, the transmitter cutoff switch, by which a person may listen in on an extension telephone without detection, is available at around 25 cents a month. Incidentally, I have seen a red copy in this room this morning being used, for legitimate purposes though, as it was originally intended.

Mr. MOORHEAD. Where is that, sir?

Mr. WATTS. Right over here on our left there is a test set that is normally used by telephone craftsmen in their legitimate functions but can be used and improperly abused. That has a cutoff switch on it so that a person being observed or listened to could not tell anyone was on the line. It could be taken down the hall where there is a terminal

37-871 O - 74 - 10

room in this building. With two little clips attached to that terminal, someone could be listening in on the call.

The original purpose of the device obviously was very legitimate. It is an essential piece of equipment in shooting trouble on telephones and something the telephone man uses all the time.

These push-to-talk devices were used—originally their intention was to be used in noisy areas.

And while on the subject of low budget invasions of privacy, I would display the "telephone pickup" available at the Radio Shack stores for $1.19 plus sales tax. Now, this device, incidentally, was purchased just a few days ago by one of our staff employees. It can be plugged into almost any standard recording device, any little recorder that even children play with, incidentally. That is a suction cup and you simply stick that onto a telephone and plug it in and you have a recording device that will record any telephone conversation of both party calling and the person receiving the call without the receiving party knowing that the call is being recorded.

Mr. MOORHEAD. The person to whose phone that would be attached would know it?

Mr. WATTS. Oh, yes. They likely would have attached it themselves, but it would be likely for a third person to attach this to a telephone so it would be unnoticeable by either parties in a telephone conversation.

Now, Mr. Chairman, in our opinion you did the Nation a great service in October of 1972 when you revealed the existence of the White House Domestic Council study on telecommunications used for social needs, otherwise referred to, and perhaps you coined the phrase at that time, as the "Big Brother" study.

In the executive branch, many departments and agencies exercise power over areas in which privacy questions must emerge. CWA has addressed the invasion of privacy question numerous times before, most recently at our 1973 convention. The resolution, which was entitled "The Abuse of Technology: Freedom's Enemy, Corruption's Ally," addressed some recent trends. It is included with the material that we have supplied to this committee.

The telephone industry is a key to inquiries on monitoring because of its developmental work and because much invasion of privacy is accomplished over telephone circuits. The 1970 wiretap of an employee of the Federal Communications Commission was done by questionable means. The tap, installed, we understand, by management personnel of the telephone company, was judged illegal by the Department of Justice. Former White House Counsel John Dean III last year told how the telephone of columnist Joseph Kraft had been tapped with specific knowledge of the exact wires in a telephone cable having been secured in some fashion from the telephone company or a telephone company employee.

Publicly stated policy of the industry is that cable pair information is tightly guarded, and I think normally that is absolutely correct.

The policy of the Bell System of safeguarding privacy is to some degree undercut when incidents like those that I have just described occur. It is entirely possible that the management of a telephone company is placed in the middle of a bad situation when asked to help by an official Government agency.

The request for help in such a circumstance can be perceived as legitimate. We hope that laws and regulations are written to protect all telephone people from being placed in the category of having been misused by apparently proper authority.

Reporters became properly alarmed about the release of their toll records to Government investigators some 6 months ago. Their loud protests will hopefully prevent a recurrence, but we have no assurance.

Four years ago, Mr. Chairman, the Governors of six States found that their "hot-line" civil defense telephones, usually installed in their personal offices, had been wired in such a fashion as to make them "open microphones" by which the sounds could be audited from outside their offices. This "hot-line" system had been installed for a good purpose, to alert Governors in case of imminent disaster. However, the system was capable of gross misuse.

Along that line, there are reliable reports of devices by which an ordinary telephone can be made into an open microphone through which one's conversation can be overheard even when the telephone hand set is lying in the cradle on the telephone otherwise appearing to be unused.

The Washington Post reporter Ronald Kessler reported the existence of the device in 1971 after he attended a symposium in Washington sponsored by the Association of Federal Investigators. As we understand it, the device can be placed at various locations on a particular line, not only at or near the telephone instrument to be tapped. Also available to users of telephone service are remote observing systems, regularly advertised in the weekly trade journal, Telephony. These systems only require a pushbutton telephone and knowledge of appropriate access codes. The observing equipment is accessed through a regular telephone number. It is possible to overhear conversations without detection, to record them, and even on local calls to learn the calling and called numbers. We believe such equipment, especially when used outside the telephone industry, is subject to grave abuse.

Mr. Chairman, our full text cites a number of other areas in which technology can be used to compromise the privacy of the individual. One area is electronic mailing handling, which would be a form of facsimile via computer. This system was tried several years ago in a joint Post Office-Western Union undertaking known as "Mailfax." Computer retrieval would be accomplished without difficulty. This would be more effective for invasion of privacy than the system of "mail cover," by which mail carriers record only the return addresses of mail going to some individual under surveillance.

The relatively new technique of "voiceprint" often entails taking a voice sample over the telephone. Recently courts have tended to reject "voiceprints" as acceptable evidence in criminal cases because the technique is not yet proven.

However, until about a year ago some courts did accept "voiceprints" as evidence. The Federal Government has spent sizable amounts of money through the Law Enforcement Assistance Administration to help develop the technique. Some tests show error rates of up to 37 percent in voice sampling comparisons.

We are concerned over the use of telecommunications technology to store medical information in computers and for the input and retrieval over telephone lines.

The access codes include social security numbers. One such medical data bank is the Medical Information Bureau of Stamford, Conn., which serves some 760 insurance companies. Currently there is a sales effort for emergency medical cards which include microfilms of the individual's data sheet. The individual supplies social security and health insurance policy numbers. Now, CWA has secured samples of these cards and I have some here. We are concerned that the information supplied by the individual to the sellers of these medical cards may also enter a centralized data bank so as to be retrievable without the individual's permission.

Incidentally, on one of these cards there is just a little piece of film that is smaller than a microfilm which has the complete medical record of an individual. It is a phenomenal thing, and most public libraries now have a device that you can just either pay a very nominal fee or no fee to take these kinds of records and supply them into the machine and see them magnified up to their original size.

This is the application for one of these cards that is going out pretty much as junk mail, incidentally, to people. This is the card that an individual gets at a later date and we will leave all of these here for your later inspection. There is a legitimate reason for this, and it can serve a very useful purpose.

On the other hand, without proper regulations, the potential misuse of this kind of device is substantial, we feel.

Now, we share the concerns expressed in July 1973 in the report on "Records, Computers, and the Citizens' Rights," issued by the Department of Health, Education, and Welfare. This study makes recommendations for legislative and administrative safeguards. We would support most of these without hesitation. We are sure that this report is already available to you. We do have one sample copy here, and we would recommend it highly to you for consideration as your subcommittee goes about its work.

We note with interest the recent work of the subcommittee in hearings on legislation to amend the Freedom of Information Act to guarantee the privacy of individuals and to provide access to records concerning themselves maintained by Federal agencies. We support these moves.

We have examined the proposals made by the American Civil Liberties Union's project on privacy and data collection. CWA would certainly support the concepts of the ACLU proposals. However, we would oppose one point, the matter of conviction records. ACLU would urge that conviction records be destroyed after the person has served his or her sentence. On the assumption that the conviction is a proper one, we must brand such a proposal at best unrealistic.

Two centuries ago, before our forebears took to arms, invasion of privacy normally meant entry into private homes by British soldiers and mercenaries. The framers of the Constitution thought that they had quite adequately disposed of the issues of privacy. And in their defense, I must agree that they did accomplish that aim. But the onrush of technology has led to a deterioration of understanding of the spirit in which the safeguards of the Constitution were written into

our most sacred body of law. I believe your subcommittee's work is helpful in leading the Congress to a rebirth of the spirit. Thank you, Mr. Chairman.

Mr. MOORHEAD. Thank you, Mr. Watts. I notice the 24-page statement has taken you 20 minutes. That should be a model for all witnesses before congressional committees.

I have a few technical questions to ask you, because I don't understand some of these terms.

At page 8 of your testimony you talk about "pair numbers." What is the meaning of that?

Mr. WATTS. Well, as you can imagine, in order to be able to determine all of the wires that travel throughout a telephone company system you have to be able to identify them for purposes of being sure you get them to go to the right place, or of finding them if they have trouble. So each pair of wires is identified in some fashion and it is the usual parlance inside the industry to refer to a pair number by which a pair of wires is identified as it goes through all the labyrinth of machinery and ultimately gets to the telephone at the telephone subscriber's premises or at the office. The pair number is usually one that goes back to a frame.

Mr. MOORHEAD. To a what?

Mr. WATTS. A frame, which is really a mass of wires that comes out of the telephone switching equipment and goes into the distribution system of cables under the streets and which ultimately ends up as two numbered pairs of wires, one for a positive side and one for a negative, just in terms of electricity, so they refer to it as numbered pairs.

Mr. MOORHEAD. Is your testimony that if I know somebody's pair number, I could tap that person's phone?

Mr. WATTS. You could more easily tap it. You could at random, I suppose, go and find where the wires begin to go to a person's home or office and with a device not unlike this person's telephone put the two clips on the two wires or onto lugs they come out on and listen until you found the persons' voice you were interested in; or if you knew the number stenciled on the little wooden block by the pairs you could very easily tap into it at that point. That would be a pretty amateurish way because it would be obvious. A person seriously interested would probably go about it in a much more scientific and sophisticated way.

Mr. MOORHEAD. This is the way columnist Joseph Kraft's number was tapped.

Mr. WATTS. Apparently someone who knew the numbers associated with Kraft's telephone made them known to the individals who were to carry out the act of tapping and it was easier for them to go about doing the job they did.

Mr. MOORHEAD. At the top of page 9 you talk about "remote observing systems" by which a person with a pushbutton telephone who knows the proper access code may listen in on conversations.

How would you find the access codes and how do you use this machinery?

Mr. WATTS. In this instance the access codes would have to be known and they would normally be known by the person assigned the responsibility for making the observations. Here again these devices were originally developed for what on the surface appears to be a very

legitimate reason, that is, to measure the quality of service being performed, either by employees of a telephone company or the equipment or in some instances by those persons who use telephone systems extensively in their businesses such as credit bureaus or hotels. It is a piece of equipment that can be purchased or leased. There are very specific instructions that go along with it, and the people authorized to use it would have those instructions available. They would have the code numbers used to dial in a pushbutton or touch-tone type telephone system so they could dial across any line being used anywhere in the system. And without the knowledge of the individual talking on the line, you could go literally across and cut in on the connection itself and listen to everything that was going on.

Mr. MOORHEAD. Thank you, Mr. Watts.

My 5 minutes have expired. I am going to try to keep everybody down to that.

Mr. Gude.

Mr. GUDE. No questions right at the moment, Mr. Chairman.

Mr. MOORHEAD. Mr. Alexander.

Mr. ALEXANDER. Thank you, Mr. Chairman.

Thank you very much, Mr. Watts, for your very splendid statement.

About 4 years ago I had the suspicion that my telephone was tapped in my office here at the Capitol, and I called the telephone company representative at that time to ask if it was so. He said no, it wasn't specifically tapped, that it was electronically monitored for the purpose of establishing efficiency of operation.

Now, Mr. Watts, is that the same thing as a tap?

Mr. WATTS. Well, I suppose it depends on what you are using it for that might cause it to be described as a tap or monitoring. It is exactly the same kind of process that is involved though, and the one that was involved, I assume, if they gave you a pretty quick answer. This surprises me, frankly, if they didn't make some investigation before they gave you an answer. The kind of monitoring that would have been used under what appears to be the circumstances you described is a very sophisticated kind of thing that is very much like this "REMOBS" kind of observing equipment.

Mr. ALEXANDER. This was at a time before Government wiretapping received the notoriety that it has in the last several years.

How does one determine when one's telephone is tapped? Is there any way that a private citizen can determine whether or not his telephone is being tapped?

Mr. WATTS. For the ordinary private citizen, except for them seeking out assistance in determining whether or not his phone is tapped it would be very difficult to make that determination on his own.

However, the telephone companies have a procedure, and if you call the telephone company and express the suspicion that your line does have a tap on it the company has an obligation to investigate the matter and advise you whether or not there is in fact found to exist any kind of a tap.

Mr. ALEXANDER. Should that request be made in writing?

Mr. WATTS. Well, I am not sure about that. They may ask you to make the request in writing, but I would assume that in at least some instances, and I would think that from a Member of Congress, a telephone request would be sufficient.

Mr. ALEXANDER. That is all, Mr. Chairman.

Mr. MOORHEAD. Mr. Erlenborn.

Mr. ERLENBORN. I have no questions at this time.

Mr. GUDE. Mr. Chairman.

Mr. MOORHEAD. Yes, Mr. Gude.

Mr. GUDE. Mr. Watts, in your opinion, have the phone companies been cooperative with the average citizen in regard to concerns about wiretapping?

Mr. WATTS. Yes, in my opinion they have, and to the extent that our testimony sounds critical and is critical, we raise general objections to the simple invasion of privacy by the use of these kinds of equipment in an official capacity of a company. We have generally accepted as a legitimate use for such devices the observing of quality of service, but we draw the line there and say that beyond that point it should not be used to invade the privacy of individuals and certainly should not be used in the field of labor management relations for collecting information for disciplinary action.

But generally I think one would have to agree telephone companies are cooperative to the citizens who feel they have a problem.

Mr. GUDE. The telephone companies respond rapidly and efficiently to citizens' complaints?

Mr. WATTS. I am generally under the impression they do.

Incidentally, since I am a union representative and an ex-employee of the telephone company, acquaintances of mine who are aware of that fact frequently call me and ask me if I can help them find out if their lines have been tapped. I have called the telephone company but have not gotten a response back because I asked them to go to the person asking the question. I have requested an immediate check be made and in general I have had a more or less inadvertent opportunity to ask those who raised the question with me if they got satisfactory advice and the indication was that they did.

Mr. GUDE. Thank you, Mr. Chairman.

Mr. MOORHEAD. Mr. Watts, at page 11 of your statement you say that Bell and other companies let customers use monitoring equipment. Do I take it from the tenor of your statement that you think that this is improper and a public utility such as the Bell System should not permit customers to use monitoring devices?

Mr. WATTS. Well, where we say we let them, what we tend to indicate to you is that under the regulations of either the FCC or at the State or city level the companies provide service under tariffs that have been established. So when other companies use some of the monitoring equipment similar to that which the telephone company uses internally, we believe that where that is done, in some way it ought to be circumscribed so the use would not be for the invasion of privacy. And to some extent it might be agreed appropriate for public privacy and to help some businesses operate more efficiently, that there ought to be proper notification to people that they are being observed.

We have cited several instances: in the State of Georgia, the public service commission requires that where the telephone company provides such a piece of equipment to a subscriber that there must be a public notice of that, and there is a notice in front of the telephone book. You can call the telephone company and get a list of all the subscribers that are renting equipment in the State of Georgia. In the

material we have submitted to you, we have a list of the people in Georgia who are leasing equipment.

Mr. MORGAN. And I believe we have supplied that to the subcommittee. Mr. Chairman.

Mr. MOORHEAD. Thank you very much. You have been very helpful to us.

On that same page, the "Alston Subscriber Dial Service Measuring System, Models 370/389, which includes a visual display and tape recording unit, and the Tel-tone M-240 system."

How can that be used?

Mr. WATTS. That is a remote observing piece of equipment that is manufactured by the Alston Co. and put into use by telephone companies. This is one of the devices we mentioned as being advertised regularly in the publication known as Telephony which is an industry kind of magazine.

When the equipment is installed there is a control area, with a selected number of telephone lines wired to it or adjusted so that they will respond to it. Individuals then can dial over any one of the lines that are associated with it in such a way that they can listen to any call that is being handled by the particular line that they have "dialed up," as the parlance goes, without the individuals talking on that line knowing that they are being observed.

Now, the legitimate aspect would be to determine whether or not the call was answered promptly by the employee and whether he or she was giving proper kinds of answers or information to the calling party.

Obviously, if one wanted to use this for an abusive purpose, took the equipment and set the system up, he could dial up and observe any number of lines. It ranges from a low of 10 up to a couple hundred lines that can be wired-in in this fashion.

Mr. MOORHEAD. One final question, Mr. Watts, on the hung-up phone invention on page 14. I have always thought of wiretapping as tapping into actual phone conversations, which is bad enough. As I understand it, by tapping the phone you can listen in on conversations in the room where the telephone is located, even though it is not over the telephone. Do I understand that correctly?

Mr. WATTS. I understand that is correct. Unfortunately, I am not enough of a scientist or technician to explain how this is done and raise the question myself as to how this is possible. In addition, there are methods of picking up conversation by induction, which is a process involving magnetism, the field of magnetism running through telephone lines, and as it fluctuates you can pick up conversations without making a direct metallic contact between two lines. I assume something of this sort is involved in the process of being able to use a telephone that appears to be idle as a microphone in a room to pick up a conversation.

Mr. MOORHEAD. Mr. Watts, is your schedule such that you can stay with us this morning?

Mr. WATTS. I can, obviously. If not necessary, I would like to move on. If you feel it necessary, I would be most happy to remain.

Mr. MOORHEAD. Our next witness is Mr. Caming of the American Telephone & Telegraph Co. You have made some statements about the company policy which he would be asked to comment on.

Mr. WATTS. I will be happy to stay.

Mr. ALEXANDER. Mr. Chairman, would you yield for one question?

Mr. MOORHEAD. Certainly.

Mr. ALEXANDER. Mr. Watts, I have followed most of your illustrations, but I want to ask you a further question on the illustration with reference to induction wherein the reference was placed in proximity to the telephone line. Is a special electronic device necessary in order to tap a line in that fashion?

Mr. WATTS. This little device for $1.19 is an induction device. It does not touch the wires. It is stuck onto the telephone and it picks up the magnetism that is created as electricity moves through the wires in the telephone itself.

Mr. ALEXANDER. Is it possible to use a laser device or some other electronic equipment to home in on a transmittal line between two parties without even touching the wire and pick up the conversation?

Mr. WATTS. Well, to say that the laser itself specifically as the device is used, I couldn't testify to that. I do know it is possible without touching the wires to pick up the conversations on them in a very sophisticated way and it boggles the mind of the uninitiated.

Mr. ALEXANDER. Is it possible for that to be done from across the street in an office building?

Mr. WATTS. It is so. In fact, I have seen a toy device in New York City where you could point across the street and pick up verbal conversations going on in the room by picking up the vibrations apparently on the windowpane by voices created in the room. If it can be done by a plastic toy, obviously a person who is a real scientist in the room could create very sophisticated devices that could do this.

Incidentally, we have mentioned one of the movies, "The Conversation," which is just replete with all kinds of futuristic devices of accomplishing these objectives. When you think in terms of some of the things we have heard—well, the "Big Brother" study, for example—it just is literally possible in the future to have every home in the United States wired in such a way that it could be observed on a very continuing basis by people if we permit that to happen and it is that kind of thing we hope to protect ourselves against.

Mr. ALEXANDER. Could these types of devices be installed in electrical appliances, in television sets, and matter of that type that were sold in retail outlets?

Mr. WATTS. Without being a real expert, I think I can say yes to that because I know there is a rural telephone system that uses power lines to transmit voice itself, so that you wouldn't have to put up both telephone and power lines, but you can run the telephone system over the power line. That being the case, it seems reasonable to me you could take an electrical device and build into it what in effect would be a microphone, stated in the simplest terms, that would transmit sounds back over electrical wires that could be picked up somewhere out of the area that you had planted this device in.

Mr. ALEXANDER. Thank you, Mr. Chairman.

Mr. MOORHEAD. Thank you very much, Mr. Watts.

We will now hear from Mr. Caming. Then we will ask you to come back to the witness table and the members and staff will direct questions to both you and Mr. Caming.

Mr. WATTS. Good.

Mr. MOORHEAD. Mr. Caming, will you come forward, please.
If you would rise, please.
Do you swear to tell the truth, the whole truth and nothing but the truth, so help you God?

STATEMENT OF H. W. WILLIAM CAMING, ATTORNEY, AMERICAN TELEPHONE & TELEGRAPH CO., NEW YORK, N.Y.

Mr. CAMING. I do, sir.
Mr. MOORHEAD. Thank you, Mr. Caming.
We welcome you to the subcommittee and if you want to summarize your statement the whole statement plus the attachment will be made a part of the record without objection.
Mr. CAMING. Thank you. If you will just indulge me for a moment. As a lawyer I would like to give you as complete an explanation of our position and be as helpful as we can.
Mr. MOORHEAD. We sincerely appreciate that, Mr. Caming.
Mr. CAMING. I am William Caming, attorney in the general departments of American Telephone & Telegraph Co. My areas of primary responsibility have since 1965 included, from a legal standpoint, oversight over matters pertaining to industrial security, service observing, and privacy as they affect the Bell System.
I wish to thank the subcommittee for the opportunity to present the views of the Bell System on privacy of communications and delineate our experiences, principally in the provision of supervisory observing equipment to business subscribers, including Government agencies.
At the outset, I wish to stress the singular importance the Bell System has always placed upon preserving the privacy of telephone communications. Such privacy is a basic concept in our business. We believe our customers have an inherent right to feel that they can use the telephone with the same degree of privacy they enjoy when talking face to face. Any undermining of this confidence would seriously impair the usefulness and value of telephone communications.
Over the years, the Bell System has repeatedly urged that full protection be accorded to its customers' privacy, and we have consistently endorsed legislation that would make wiretapping as such illegal. In 1966 and again in 1967, we testified to this effect before the Senate Subcommittee on Administrative Practice and Procedure during its consideration of the Federal omnibus crime control and safe streets bill. This is still, of course, our position.
We believe that the Federal Omnibus Crime Control and Safe Streets Act has contributed significantly to protecting privacy by, among others, clarifying existing law and proscribing under pain of heavy criminal penalty any unauthorized interception "or" disclosure or use of a wire communication.
On April 26, 1974, I appeared before the Subcommittee on Courts, Civil Liberties and the Administration of Justice of this House's Committee on the Judiciary and discussed our views on privacy of communications and our experiences with electronic surveillance, principally in the area of wiretapping. A copy of our statement is respectfully enclosed as background information.
Turning to your subcommittee's specific inquiries, as we informed you in 1970 the Bell System companies provide, under tariff, facilities

such as push-to-talk telephones and transmitter cutoff keys to customers, including Government agencies, who find it necessary at times to eliminate background noises and distractions (for example, at an airlines reservation desk in a noisy terminal; a secretary taking telephone dictation; during use of a mobile car phone; in a factory; or at a construction site).
Duplicative jacks for switchboard or console positions are also offered under tariff. This enables a subscriber's supervisor or fellow employee to plug into a position while standing next to the attendant manning it, so as to provide assistance in an emergency or otherwise unusual operating situation, or for training and development purposes, or to allow one attendant to relieve another without disrupting a call in progress.
Over the years, the Bell System companies have also been providing to a limited number of subscribers, under tariff, observing arrangements for supervisory and service training assistance purposes. Currently some 4,000 to 4,500 of almost 9 million Bell System business subscribers use these arrangements. They are largely businesses or institutions which receive from, and in some instances place to, members of the public large volumes of calls. Airlines, department stores, public utilities, and Government agencies are among the primary users of such equipment.
Specific requirements, of course, for supervisory observing and service training assistance arrangements, of course, vary somewhat among customers, so that facilities provided locally are arranged to conform to the particular customer's needs. These arrangements incorporate various types of key equipment, such as multibutton key telephone sets, and special switchboard and console positions.
In the main, however, the bulk of these observing arrangements are provided at present as a feature of our automatic call distributing systems, rather than through key systems. These vary in size, depending on the volume of incoming calls to the business. They may range from 60 or less attended positions to several hundred or more in the instance of a few airline reservation centers.
ACD's automatically distribute incoming calls in the approximate sequential order of arrival to the attendant positions in the order of their availability. If at a given time all of the attendant's positions are busy, a recorded announcement will advise the calling party that he has reached the company, that all of its attendants are busy at the moment, and that one will be available shortly. We have often heard that when calling an airlines reservations center.
The waiting call will then generally be randomly distributed to the next available attendant.
Supervisory observing and service training assistance equipment is furnished by the Bell System companies solely to assist business subscribers in better evaluating the quality of telephone service being rendered by those of its employees handling calls placed "to the business." These are not employee calls. The implementation of this policy relies on adherence to intrastate tariff provisions which, in general, impose restrictions and conditions on the provision of this service, such as the following:
Furnished only to business subscribers;

Subscriber shall inform its employees their business telephone contacts are subject to observation;

Service provided solely for purpose of determining the need for training of or improving the quality of service rendered by employees in the handling of telephone calls to the subscriber (not to the employees) of an impersonal business nature;

Limitation of use of service to administrative lines only, in connection with hotel service and service of like nature involving public use;

Observing equipment may not be used for any other purposes, and also inform employees of such use;

Subscriber shall not use service in any manner contrary to tariff or law;

As a condition precedent, to insure compliance, subscriber must agree in writing to use the equipment solely for the purpose stated above—and to fully inform all affected employees.

Thus, by tariff the use of supervisory observing and service training assistance equipment is expressly restricted to routine, impersonal calls to the business. It bears reiteration that there are calls to the business, handled in its behalf by employees as its agents. These are not personal calls to the employees. Personal calls by and to the subscriber's employees may not be subject to observing. Employees usually are afforded convenient access to telephones other than those used for business to carry out their personal calls; these are not subject to observing. In no wise does supervisory observing in conformity with the above strictures constitute an invasion of personal privacy.

Further, such supervisory observing may only be used to evaluate the quality of service rendered by the subscriber's employees (whether they be PBX or Centrex switchboard operators, ACD attendants, or other telephone contact employees) for the sole purpose of determining what, if any, additional training and development is required to insure that the performance of each satisfactorily meets the standards of the business. It is to be borne in mind that the basic work product of these particular employees is telephone service, susceptible to reliable and adequate evaluation only through supervisory observing. These employees are also made fully aware that the performance of their telephone contact duties will be subject to supervision, in part through periodic supervisory observing. The conclusion is inescapable that it is essential to observe such business calls if the supervision, training, and development of the employees is to be effectively and efficiently conducted.

Thus many business users of telephone service whose employees' duties entail the constant handling of large volumes of calls, often on a random basis, regard supervisory and training assistance observing as an indispensable technique for the reliable evaluation of the quality of service being provided to the public. This process not only discloses critical areas in which additional development and training is needed, but also promotes recognition of satisfactory or outstanding performances of duty by individual employees.

It is clearly, in our opinion, in the public interest to have businesses, institutions, and public agencies maintain on a continuing basis high standards of performance, not only in face-to-face contacts, but also when conducting their affairs by telephone—both with respect to the completeness, effectiveness, and courtesy of the service rendered.

Each of the Bell System companies promptly and thoroughly investigates any and every complaint alleging improper use of supervisory observing equipment furnished under tariff, whether we receive such complaint directly or through regulatory or other channels. Whenever the circumstances of any such investigation so warrant, necesary corrective action is promptly taken by the telephone company, to insure that the subscriber's practices are in strict compliance with all applicable tariff requirements.

Over the years, however, Bell System companies have received extremely few complaints or other indications of abuse of this service. This favorable experience appears to reflect, in good part, the responsible approach of the businesses subscribing to this offering, the routine and impersonal nature of the business calls under observation, and the subscriber's recognition of the vital importance of this form of supervision to the successful operation of the enterprise or agency.

In conclusion, I wish merely to assure you that the Bell System continues to be wholly dedicated to the proposition that the public is entitled to telephone communications free from unwarranted intrusion, a position Mr. Watts also eloquently subscribed to.

We are vitally interested in the protection of the privacy of personal communications and always welcome measures and techniques that will strengthen and preserve it. We believe that the foregoing service offerings that I have described in no respect infringe upon such privacy and are in furtherance of the public interest.

I shall be pleased to try to answer any questions of the subcommittee.

Mr. MOORHEAD. Thank you very much, Mr. Caming.

[Mr. Caming's prepared statement before a House Judiciary subcommittee follows:]

PREPARED STATEMENT OF H. W. WILLIAM CAMING, ATTORNEY, AMERICAN TELEPHONE & TELEGRAPH CO., NEW YORK, N.Y.

I am H. W. William Caming, attorney in the general departments of American Telephone & Telegraph Co. My areas of primary responsibility have since 1965 included, from a legal standpoint, oversight over matters pertaining to industrial security and privacy as they affect the Bell System.

I wish to thank the subcommittee for the opportunity to present the views of the Bell System on privacy of communications and delineate our experiences with electronic surveillance, principally in the area of wiretapping.

At the outset, I wish to stress the singular importance the Bell System has always placed upon preserving the privacy of telephone communications. Such privacy is a basic concept in our business. We believe that our customers have an inherent right to feel that they can use the telephone with the same degree of privacy they enjoy when talking face to face. Any undermining of this confidence would seriously impair the usefulness and value of telephone communications.

Over the years, the Bell System has repeatedly urged that full protection be accorded to its customers' privacy, and we have consistently endorsed legislation that would make wiretapping as such illegal. In 1966 and again in 1967, we testified to this effect before the Senate Subcommittee on Administrative Practice and Procedure during its consideration of the Federal Omnibus Crime Control and Safe Streets bill. We said we strongly opposed any invasion of the privacy of communications by wiretapping and accordingly welcomed Federal and State legislation which would strengthen such privacy. This is still, of course, our position.

We believe that the Federal Omnibus Crime Control Act has contributed significantly to protecting privacy by, among others, clarifying existing law and proscribing under pain of heavy criminal penalty any unauthorized interception or disclosure or use of a wire communication.

During our congressional testimony, we said too that we recognized that national security and organized racketeering are matters of grave concern to the Government and to all of us as good citizens. The extent to which privacy of

communications should yield and where the line between privacy and police powers should be drawn in the public interest are matters of national public policy, to be determined by the Congress upon a proper balancing of the individual and societal considerations.

For more than three decades, it has been Bell System policy to refuse to accept in the Yellow Pages of its telephone directories advertisements by private detective agencies and others, stating or implying that the services being offered include the use of wiretapping. In December 1966, during congressional consideration of the Federal Omnibus Crime Control Act's title III proscriptions against unauthorized interceptions, this longstanding policy was expanded to prohibit too the acceptance of eavesdropping copy. This standard, adopted by all Bell System companies, was interpreted from the outset to make equally unacceptable so-called debugging advertising (i.e., advertising stating or implying electronic devices or services will be provided for the detection and removal of wiretaps and eavesdropping "bugs"), on the theory that those who can debug also possess the capability to bug and wiretap.

Our companies continually review their Yellow Pages in an endeavor to insure all unacceptable copy is removed, either by satisfactory rewording or deletion of the offending copy. New advertising is subject to similar scrutiny. The scope of this undertaking becomes apparent from the fact that there are approximately 2,400 Yellow Pages telephone directories, containing some 18 million advertisements and listings.

The removal of unacceptable copy is a never-ending task of large proportions, since many such advertisements are revised, and new ones appear, in each issue. We believe, however, that we have done a creditable job in this area, and we intend to continue such rigid policing as contributive to maximizing privacy of communications.

It may help place matters in perspective if we provide a brief insight into the magnitude of telephone calling that occurs in this country in a single year. During the calendar year 1973, for example, there were approximately 138 million telephones (including extensions) in use in the United States, from which some 188 billion calls were completed.

From the time our business began some 90 years ago, the American public has understood that the telephone service they were receiving was being personally furnished by switchboard operators, telephone installers, and central office repairmen who, in the performance of their duties of completing calls, installing phones and maintaining equipment, must of necessity have access to customers' lines to carry out their normal job functions. We have always recognized this and have worked hard and effectively to insure that unwarranted intrusions on customers' telephone conversations do not occur. We are confident that we have done and are doing an excellent job in preserving privacy in telephone communication.

The advance of telephone technology has in itself produced an increasing measure of protection for telephone users. Today, the vast majority of calls are dialed by the customer, without the presence of an operator on the connection. This has greatly minimized the opportunities for intrusions on privacy. In addition, more than 88 percent of our customers now have one-party telephone service, and the proportion of such individual lines is growing steadily. Direct inward dialing to PBX extensions, automatic testing equipment, and the extension of direct distance dialing to person-to-person, collect and credit card calls and to long distance calls from coin box telephones further contributes to telephone privacy.

Beyond this, all Bell System companies conduct a vigorous program to insure every reasonable precaution is taken to preserve privacy of communications through physical protection of telephone plant and thorough instruction of employees.

Our employees are selected, trained, and supervised with care. They are regularly reminded that, as a basic condition of employment, they must strictly adhere to company rules and applicable laws against unauthorized interception or disclosure of customers' conversations. All employees are required to read a booklet describing what is expected of them in the area of secrecy of communications. Violations can lead, and indeed have led, to discharge.

In regard to our operating plant, all of our premises housing central offices, equipment and wiring, and the plant records if our facilities, including those serving each customer, are at all times kept locked or supervised by responsible management personnel, to deny unauthorized persons access thereto or specific

knowledge thereof. We have some 90,000 people whose daily work assignments are in the outside plant. They are constantly alert for unauthorized connections or indications that telephone terminals or equipment have been tampered with. Telephone cables are protected against intrusion. They are fully sealed and generally filled with gas; any break in the cable sheath reduces the gas pressure and activates an alarm.

With these measures and many others, we maintain security at a high level. We are, of course, concerned that as a result of technological developments, clandestine electronic monitoring of telephone lines by outsiders can be done today in a much more sophisticated manner than has been heretofore possible. Devices, for example, now can pick up conversations without being physically connected to telephone lines. These devices must, however, generally be in close proximity to a telephone line, and our personnel in their day-to-day work assignments are alert for signs of this type of wiretapping, too. Every indication of irregularity is promptly and thoroughly investigated.

Our concern for the privacy of our customers is reflected too in the care with which we investigate any suspicious circumstances and all customer complaints that their lines are being wiretapped. Our companies follow generally similar operating procedures when an employee discovers a wiretap or eavesdropping device on a telephone line. Each company has established ground rules for the small number of these situations that occur, which take into consideration any local statutory requirements. Most frequently, when our people find improper wiring at a terminal, it is the result either of a record error or failure on the part of our personnel to remove the wires associated with a disconnected telephone. Each of these cases is, however, carefully checked. In those few instances where there is evidence of wiretapping, the employee discovering it is required to inform his supervisor immediately, and a thorough investigation is undertaken in every such case by competent security and plant forces.

In a small number of cases, a customer suspects a wiretap and asks for our assistance. Usually, these requests arise because the customer hears what are to him suspicious noises on his line. Hearing fragments of another conversation due to a defective cable, or tapping noises due to loose connections, or other plant troubles are on occasion mistaken for wiretapping. Each company has established procedures for handling such requests. Generally, the first step is to have our craftsmen test the customer's line from the central office. In most instances, these tests will disclose a plant trouble condition. In each such case, the trouble is promptly corrected and the customer informed there was no wiretap.

In cases where no trouble is detected through testing the customer's line, a thorough physical inspection for evidence of a wiretap is made by trained personnel at the customer's premises and at all other locations where his c[illegible]try might be exposed to a wiretap. If no evidence of a wiretap is found, the c[illegible]er is so informed. Where evidence of a wiretap is found, the practice gene[illegible] is to report to law enforcement authorities any device found in the course of the company inspection, for the purposes of determining whether the device was lawful and of affording law enforcement an opportunity to investigate if the tap was unlawful. The existence of the device is also reported to the customer requesting the check, generally irrespective of whether it was lawful or unlawful. The customer is told that a device has been found on his line, without our characterizing it as lawful or unlawful; should the customer have any questions, he is referred without further comment to law enforcement.

New Jersey Bell however, as a matter of policy, informs a customer requesting a wiretap check that only the presence of an unauthorized device will be disclosed. Minnesota by statute similarly limits disclosure to unlawful devices. Should the customer inquire about the presence of a lawful device, he will usually be assured that applicable Federal and State laws require any judge authorizing or approving a court-ordered interception to notify the affected customer within 90 days after interception ceases (or at a later date, if disclosure is postponed upon a good cause showing by law enforcement).

All Bell System companies report the existence of an unlawful device to the customer requesting the check, as well as to law enforcement, and the latter is provided an opportunity to investigate for a reasonable period (generally 24–48 hours) prior to removal of the wiretap.

We might point out that unless the wiretap effort is amateurish, a person whose line is being tapped will not hear anything unusual, because of the sophisticated devices employed. As we previously said, most of the complaints originate because the customer hears an odd noise, static, clicking, or other unusual mani-

festations. As far as our experience discloses, these usually turn out to be difficulties in transmission or other plant irregularities. From 1967 onward, for example, the total number of wiretap and eavesdrop devices of all types (including both lawful and unlawful) found by telephone employees on Bell System lines has averaged less than 21 per month—an average of less than one a month for each of the 24 operating companies of the Bell System. In our opinion, the criminal sanctions imposed by title III (for the unauthorized interception or disclosure or use of wire or oral communications, or the manufacture, distribution, possession, or advertising of intercepting devices), coupled with vigorous law enforcement and attendant publicity, appear to have contributed significantly to safeguarding telephone privacy.

In the area of court-ordered wiretapping, it is the policy of the Bell System to cooperate with duly authorized law enforcement authorities in their execution of lawful interceptions by providing limited assistance as necessary for law enforcement to effectuate the particular wiretap. We wish to stress that the Bell System does not do the wiretapping. The assistance furnished generally takes the form of providing line access information, upon the presentation of a court order valid on its face, as to the cable and pair designations and multiple appearances of the terminals of the specific telephone lines approved for interception in the court order.

The term "cable and pair" denotes the pair of wires serving the telephone line in question, and the cable (carried on poles, or in conduit, or buried in the earth) in which the pair reposes. A "terminal" is the distribution point to which a number of individual pairs of wires from the cable are connected, to provide service in that immediate area. A terminal may in a residential area be on aerial cable suspended from telephone poles or on a low, aboveground pedestal, or be found in terminal boxes or connecting strips in the basement, hall, or room of an office building or apartment house. The pair of wires of each telephone serviced from a particular terminal are interconnected at that terminal with a specific pair of wires from the cable, so that a continuous path of communication is established between the customer's premises and the telephone company's central office. The terminals vary in size, depending upon the needs of the particular location. To provide optimum flexibility in usage of telephone equipment, the same pair of wires may appear in parallel in a number of terminals, so that the pair can be used to service a nearby location if its use is not required at a particular point. Thus, the term "multiple appearance" denotes the locations where the same pair of wires appears in more than one terminal on the electrical path between the central office and the customer's premises.

In the instance of law enforcement authorities of the Federal Government (and of those States enacting specific enabling legislation in conformity with the amendments to § 2518(4) of title III of the Federal Omnibus Crime Control Act effective February 1, 1971), the court order may "direct" the telephone company to provide limited assistance in the form of the "information, facilities, and technical assistance" necessary to accomplish the wiretap unobtrusively and with a minimum disruption of service. Upon the receipt of such a directive in a court order valid on its face, our cooperation will usually take the form of furnishing a private line channel from terminal to terminal (i.e., a channel from a terminal which also services the telephone line under investigation to a terminal servicing the listening post location designated by law enforcement). Additionally, the above described line access information will be furnished for the specific telephone lines judicially approved for interception.

On occasion, assistance in the form of private line channels is furnished to Federal authorities in national security cases. This assistance is only rendered upon specific written request of the Attorney General of the United States or of the Director of the Federal Bureau of Investigation (upon the specific written authorization of the Attorney General to make such request) to the local telephone company for such facilities, as a necessary investigative technique under the Presidential power to protect the national security against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities. For reasons of security, we are not informed in such cases of the specific nature of the national security matter under investigation.

In cooperating in court-ordered and national security cases, we endeavor to provide the very minimum assistance necessary to effectuate the particular wiretap. Under no circumstances, do we do the wiretapping itself; that is the exclusive province of the appropriate law enforcement officers. Nor do we furnish

end equipment to be used in connection with a wiretap, such as tape recorders or pen registers. Nor do we design or build wiretap or eavesdrop devices for law enforcement authorities. Furthermore, our telephone companies do not train law enforcement personnel in the general methods of wiretapping and eavesdropping, nor do we provide telephone company employee identification cards, uniforms or tools, or telephone company trucks.

In conclusion, I wish to assure you that the Bell System continues to be wholly dedicated to the proposition that the public is entitled to telephone communications free from unlawful interception or divulgence. We are vitally interested in the protection of the privacy of communications and always welcome measures and techniques that will strengthen and preserve it.

The foregoing reflects our experience in the areas of wiretapping and electronic surveillance since the passage of title III of the Federal Omnibus Crime Control Act in 1968 and our continuing concern for maximizing the privacy of communications.

I shall be pleased to endeavor to answer any questions that the subcommittee may have.

Mr. MOORHEAD. Mr. Watts, will you now come back to the witness table?

The first question I would like to ask you, Mr. Caming—you heard Mr. Watts' testimony——

Mr. CAMING. Yes, sir.

Mr. MOORHEAD. Are there any technical statements—not philosophical—that Mr. Watts made about bugging and related fields that you have knowledge of in your corporate position that you wish to correct—technical matters—not how the device is used?

Mr. CAMING. Thank you, Mr. Moorhead.

I would not necessarily want to correct any of the statements of Mr. Watts. I would say perhaps I would describe them differently.

Mr. MOORHEAD. Give an example of where you would be different.

Mr. CAMING. Without going into too much specification, it is a question of background interpretation and understanding of each of the complicated questions that are the subject of your inquiry.

For example, reference was made to remote observing equipment. This is the so-called telephone equipment that we have recently introduced for service observing purposes and is currently used by some 12 of our companies in some of our offices to overhear and observe on calls made of a routine nature to the business office and to the plant repair service bureaus at present.

Now, I would be very pleased, without wishing to overburden the committee, to give you whatever information in connection with that you might desire. I can, if you so desire, describe briefly how it operates and, two, how it in no wise impinges upon privacy and perhaps the overall conclusion might be that it is as secure or perhaps more secure.

In that regard, we now use, as we have for so many years, as one of our primary criteria, the impact upon privacy. As you can appreciate, we, too, are sensitive to the public considerations which have been on an increasing level, certainly since the midsixties when Senator Long and members of the House—Senator Edward Long—launched various investigations concerning invasions of privacy.

So we do not do anything lightly with a million or so employees. There are, of course, some aberrations from our policies, but they are in each case very carefully investigated and quickly corrected.

The Tel-tone is one example where there is no real concern. If you would like, I can briefly describe the operation.

Mr. ALEXANDER. Would the Chairman yield a second?

Mr. MOORHEAD. Yes. I was going to suggest maybe we get that description in writing rather than take up the time this morning.

Mr. ALEXANDER. Just one inquiry, Mr. Chairman. Since Mr. Caming has agreed to describe these devices to us, I wonder if it would be helpful if he could bring all this type of equipment in here and illustrate it for us.

Mr. CAMING. Mr. Alexander, as an attorney I would not categorize myself except as a secondhand expert on the subject.

What I would say about the Tel-tone would be very brief——

Mr. ALEXANDER. Mr. Caming, I was asking the Chairman a question.

Mr. CAMING. Sorry.

Mr. ALEXANDER. Would it be possible to have that equipment illustrated? I think it would be very helpful to see how all these devices work.

Mr. MOORHEAD. Is the equipment suitable to be brought in here and attached to that phone over there?

Mr. CAMING. I would have to confer with our people as to whether it is. Basically it is used for service observing whereby the unit is, say, affixed to a number of our plant repair offices, and the equipment is accessed through your dialing from one of our secure service observing locations a telephone number to the particular unit you wish, and then a tone is sent back from the unit. That is all there is to it. Within 5 seconds the service observer must send back a two- or four-digit security code. That is all there is to it. Once that is done the equipment is accessed. It is just a small unit.

We have, I believe, or can furnish the staff necessary manuals and I believe Mr. Cornish, you may have some of those, in connection with Tel-tone. That is about all there is to it. It is just a small unit which has the capability, once it is activated to preselect at random from a large number of trunks one of the incoming calls to a plant repair office or to a business office. It is just a very simple box. There is nothing particularly sophisticated about it in the sense of appearance. Does that help?

Mr. MOORHEAD. When you say the equipment is accessed, you mean you can listen in on the conversations?

Mr. CAMING. Yes, just as our service observers in service observing can and do randomly access a certain number of plant repair service calls, business calls and the like.

Mr. MOORHEAD. Mr. Erlenborn?

Mr. ERLENBORN. I have no questions, Mr. Chairman.

Mr. MOORHEAD. Mr. Alexander.

Mr. ALEXANDER. Mr. Chairman, I appreciate very much the opportunity to hear Mr. Caming this morning, and I appreciate your cooperation. I realize you are an attorney and I wouldn't expect the illustrations to be demonstrated by you but by some of the technicians with the company with which you are associated.

I have become alarmed during my 6 years in Washington at the number of people who believe that they are bugged even if they aren't bugged. People in my neighborhood think they are bugged even if they aren't bugged. I believe I am bugged. I don't know whether I am or not. I hope if I am that someone enjoys the conversations as

much as I do with them. I think people out in the heartland of our country are increasingly more alarmed about Government spying on their businesses and persons, and in fact, one individual that I talked to in Arkansas not long ago made the statement that he believed that every American is on a potential party line with their Government. Now, when that sort of attitude prevai in this country, I think it is time for Government to do something about it and I think this committee is on the right track.

Thank you, Mr. Chairman.

Mr. MOORHEAD. Thank you, Mr. Alexander.

Mr. Gude.

Mr. GUDE. Thank you, Mr. Chairman.

What type of a timetable does the phone company have in regard to responding to citizen complaints or inquiries concerning wiretapping?

Mr. CAMING. Mr. Gude, I might allude to the fact that I included as part of my statement the statement I made before the other House subcommittee of the Committee on the Judiciary, in which there is a description of the operative procedures under which we do respond.

We respond as quickly as possible. Each one of these requests for assistance in the area of wiretapping is immediately processed. The first step, if I may go on, Mr. Gude, is to have our plant central office test electronically to determine whether what a person takes to be a wiretap may in fact be a plant trouble. This actually, in our experience, has been the case in most situations where people hear something that they believe constitutes wiretapping. For example, a crackling noise, talking in the background, certain disturbing surges. In such cases that investigation is carefully made through the plant central office. In most instances, in our experience, and we average about 10,000 of these requests a year across the land in the Bell System, most of these immediately turn out to be ascertainable plant troubles. They are immediately corrected and the customer promptly notified what it was and that it was corrected.

Now, if that is not found to be a plant trouble that can be cleared, as the expression goes, Mr. Watts, I believe, then it is immediately turned over to the security group that each company constitutes, and a very careful and full inspection is made under their general supervision, either directly by them or in concert with plant craft forces to check the outside wiring between the telephone itself and the central office; and second, to also check the inside wiring and facilities, including the telephone and all the terminals with, of course, the consent and at a time convenient to the customer.

Now, if I may, I thought I would give you the exposition one step further. What do we do when we find one? If we find nothing, of course, we so notify the customer, and also ask that any further indication be immediately reported. This is a check made by competent personnel. If we do find a device somewhere on the stretch, we are, of course, at that stage of finding it not able to determine whether it is a lawful or unlawful device. I say lawful, for example, one under a court order. Our procedure then calls for security upon finding a device, say at a pole or at a terminal some distance away, to have our files checked to determine whether we have a lawful—a record of a lawful court order having been presented to us by a State or local or Federal authority for court-ordered wiretapping.

Assuming we do not, we then check with the appropriate local Federal authorities, like the FBI, and also some central point in the State-local level which has been prearranged, to determine whether there is a wiretap on that line that is lawful but that has not been brought to our attention, since there is no requirement of law that they do, and often it may not be necessary for law enforcement to require our cooperation in order to effectuate a particular tap.

Assuming they say no, we know nothing about it, this would then appear to us to be an illegal wiretap. In such case we would normally accord law enforcement, if they so desire, a very short period, perhaps 24 to 48 hours, to investigate and endeavor to capture the culprit, the point being that if you find a device but don't catch the wiretapper, you have accomplished relatively little. After that period, the device is removed and usually taken in tow by law enforcement.

The customer is informed that there was an illegal device—I am sorry—that there was a device on his line. We use the term "device" because we do not wish to characterize it one way for lawful devices and another way for unlawful devices. As you gentlemen undoubtedly know, the Crime Control Act provides in section 2510(8) that applications and court orders for wiretapping are under seal and therefore cannot be disclosed. If it is a lawful wiretap, we will notify law enforcement we have found this device, what do you want us to do about it. This assumes it is not trouble inducing. If it was, it would be removed anyway, but assuming it wasn't, they will probably tell us to remove it, although there are a few cases, I have been told, where they may decide to keep it on the phone, because it sometimes facilitates surveillance of organized crime of people going in and out. But generally it will be disposed of in accordance with the proper law enforcement instructions of the authority having put it there under court order.

Now, we do not lie to the customer. We are in somewhat of a dilemma as to what we should do. And there has been a great deal of objection from law enforcement in many areas of the country, that we are precluded by the law from disclosing the presence of the device. We recognize we cannot characterize it as an unlawful device. So we tell the customer we have found a device, and if you have any question discuss it with law enforcement. We do that whether it is a lawful or unlawful device so as not to tip our hands.

With respect to national security devices, and I am sure that questions come to mind, there, too, our assistance is not necessary for placing it. We have until now not found to my knowledge a device which has been admittedly a national security device. I say admittedly, because they may say no, that is not ours, or yes, that is ours but—and also if the man is a competent wireman who places the device and takes enough time, it is exceedingly difficult even for the most competent expert to find certain very well placed wiretaps.

But what we would do, I have speculated, and this is hypothetical, is one of two things. I might say we would tell the customer. As mentioned in my statement, there are two exceptions. In the State of Minnesota, we may not by statute disclose the presence of a lawful device in any sense, and in New Jersey by policy. What we say is that the application and order is under seal. Accordingly, we are unable to disclose the presence of such application or order pursuant to court order. So we will therefore only disclose to you unauthorized wiretaps that we may discover. In such a case the question is often prompted when we say we found no device, they say what about a lawful one. We point out we do not disclose it in those States but assure them under the Crime Control Act itself, section 2510(8), there is a specific requirement, not that the prosecutor, but that the trial judge is directed to disclose to the intercepted party and such other parties as in his discretion he may feel it advisable to notify within 90 days after termination of the tap, or any later date, if postponed by the court, to notify such parties that a lawful wiretap was placed on their line from period so-and-so to so-and-so, and that interceptions were accomplished thereunder.

That is a long way around, Mr. Gude, to answering your question.

Mr. GUDE. So as it stands, if a complaint is made by a customer or user of a telephone, they are notified if a tap is discovered, whether or not it is illegal?

Mr. CAMING. That is our uniform and recommended policy, and that is correct.

Mr. GUDE. If a citizen uses a telephone in a hotel or some similar public place, can he be assured of the same type of security he would have when using a telephone in a private home?

Mr. CAMING. Yes, to the extent of limitations placed upon our offerings, we can provide that assurance.

Under our tariffs or administrative practices, we do not provide the supervisory observing equipment I described to hotels or motels or other similar communications areas where a guest might access the public network for a telephone conversation. In such cases, we only provide observing of what we denominate an administrative character; that is on nonguest telephones. So that a person calling, say, from one of the Washington hotels can be assured that there is no supervisory observing by the management of the hotel.

Now, that telephone call would be subject to random statistical service observing or official service observing described in a letter to this committee on 1970. But I might stress there is no monitoring or any observing of any of the conversations of any of the calls that we engage in.

Mr. GUDE. So outside of observing for the purposes of marketing surveys or the level of customer service, a citizen who uses a telephone in a hotel or similar place can be assured of the same security he has in a private home?

Mr. CAMING. That is correct.

Mr. GUDE. Thank you, Mr. Chairman.

Mr. MOORHEAD. Thank you, Mr. Gude.

Mr. Caming, you have stated, particularly on pages 1 and 2 of your testimony, the interest of the Bell System in preserving privacy. Mr. Watts, on page 9 of his testimony, says—

> The Bell System employs "remote observing systems" by which a person with a push button telephone who knows the proper access codes may listen in on conversations without detection.

Does Bell do that and is that consisent with the interest stated in preserving privacy?

Mr. CAMING. May I comment, Mr. Moorhead?

Mr. MOORHEAD. Yes. That is why I am asking you, sir.

Mr. CAMING. What we are talking about there is, I believe, that Mr. Watts had adverted to the fact that in 12 of our companies at this time we use Tel-tone equipment, that I mentioned earlier that you access through a code that is held most securely and requires a complex range of dialing to send it back, as I adverted, within 5 seconds.

Now, in many respects our service observing practices might bear just a brief comment to give you the background to understand this in perspective.

As you know, we conduct official service observing from certain locations which are kept under very tight security and I might say at any time that members of the committee or its staff might desire to see any we would be very pleased to have you visit them.

Now, these facilities are for the purpose of random statistical observing on equipment and equipment malfunctions as one of the principal quality controls of the Bell System. Since our product is telephone service there is no other way to check on its efficacy and evaluate its performance in the public interest.

Now, these rooms are very closely guarded and our most relial and experienced and trained employees are placed there under supei vision to insure there is maximum consideration of privacy. In fact, in over 60 to almost 70 years now there has never been a case that a service observer in the Bell System, and I think this is a tribute to our employees and Mr. Watts' constituents, there has never been a case of any service observers being charged with violating their duties to protect the privacy of their equipment and operations.

Now, these offices generally have up to now been hardwired to random trunks. You know, a trunk is one that may contain a 100 wires leading into it and then one line at a time can access the trunk and then the others access other trunks. So we have had our service observers and they have through hardwiring been able to observe on various operations such as business offices and plant repair bureaus where people call and want their phones fixed.

Now, in this connection the hardwiring has imposed a number of limitations on the efficacy of this as a quality control tool because you have to dedicate a pair; it is expensive to do so and you cannot necessarily reach all parts of a State. A number of our States and some areas that Mr. Alexander may be more familiar with than I in the heartland which are rural and not too heavily populated, we have not been able to observe the service to the degree we can in more concentrated areas because of the inability and tremendous cost of doing so.

In addition, we often have very small service observing bureaus in some of the more suburban and rural areas. In this connection they may be just two-man bureaus and there is not the constant close supervision you have in major cities. There may be supervisory visits only two times a week rather than constant daily supervision.

This new equipment has the following advantages. In one sense it is more secure in arrangement because it will permit centralized location of service observers; therefore, they will be the same locked room in which access is confined to authorized personnel but they will be under close, constant daily supervision. This is a very important plus from the viewpoint of privacy.

It is also a very effective quality control measure. It will permit us to access every part of the State and to reach more locations for checking on the quality of the service. It will also permit, by concentrating the force, instead of having only two or three in one area, better utilization of the areas, for schedules, sickness and the like. It will also, and importantly, permit a more uniform interpretation of our measurement plan, and therefore a better administration of the quality control program when you have fewer units to be coordinated.

It will insure, and this is a very important consideration, a better random selection. In this case, the unit that I mentioned has built in it, although it is not apparent, just a box, a preselector that insures that each call observed is randomly selected from among these trunks in a completely random nature which is more efficient than the current one, and of course the more random the quality of this service the better the results that can be obtained.

It does also have some economies attached to it.

Now, we had some concern because the code, which is a very carefully guarded two-digit or four-digit code that accesses when the tone comes back after you dial the unit to activate it. The code itself is closely guarded and in the hands only of the service observers. It is under lock and key when not in use. Now, this code can be changed with regularity, and it is our policy at this time, and this is being—in fact, I had it rechecked just yesterday in contemplation of my appearance—changed at intervals of 2 weeks or less, and that is going to be our target. This closely guarded code can be changed.

The change is going to be very simple. The service observer has a touch tone button type of television—sorry, I heard that noise in the background and the word television immediately came into mind when the light came on and I was off screen.

If I may restate that. The service observer in the locked office who will change the code does it in the following fashion. She has a touch-tone dialer with buttons, and I will comment on that just very briefly after this. She punches say four digits for the new code she selects or that has been designed for her to select at the next period of time. At such time she has already cont cted the plant people at the particular location, say in the northeast part of Washington. So there is a plant repairman there at the unit and it is very simple to do. She tells them to turn the screw on, say, button No. 1 which she has punched and he does. It is a variable resistor potentiometer, a word I just reviewed the other day, and when he turns it, he just keeps turning it blindly until a light flashes and then he stops. He does not know what the frequency is he has selected and then he does that, then, for the next. So it is a very simple, quick method that can be done in a couple of minutes and completely changes the code, which is a matter of great concern to us to insure privacy.

Second, the original Tel-tone, and some of the literature that has been distributed states that access can be made from any touchtone telephone if you have stolen the code. It doesn't say if you have stolen the code, but that inference is you must know the code. We were concerned with this, so that last year, and this has just been introduced within the last couple of years, we decided to introduce a new touch-tone dialer, the 1066 touchtone dialer, which has four additional buttons that do not appear on the ordinary touchtone telephone and they are used for the code. So you have 14 or 16 buttons to the 16 power, whatever mathematically that may turn out, as the possible

combination. This is now being put in—I am not sure it is yet in all locations, but it is being put in on an accelerated basis. For example, I did ascertain in the C. & P. area covering Washington, they did have 1066's for all of their locations.

Now, even if you could break into the secure locations or otherwise obtain the security code for that 2-week period, that is all you would have it for, it wouldn't be worth anything thereafter, and if you could manage to get hold of a 16-button touchtone dialer, what would be the net result? You would merely access at random impersonal business calls of customers to the business office and to plant repair service. I submit that these calls would be at most of vicarious interest: to hear who disputes a particular bill or feels that their telephone service is exceedingly poor on their new equipment and they want something better. That is about all you would overhear. So for these reasons, the economies of scale, the more secure arrangements, the greater coverage it will afford to service and the improved quality control that we can provide have led us to the feeling that this is an improvement and one that we are proud of. This is basically the remote observing equipment that Mr. Watts alluded to in his statement.

Mr. MOORHEAD. Thank you very much, Mr. Caming.

I presume you gentlemen would be willing to answer questions we would submit to you in writing?

Thank you. I will yield to any member for questions that can't be put in writing.

Mr. Daniels?

Mr. DANIELS. No questions. Thank you.

Mr. MOORHEAD. Anyone else?

Mr. STETINER. For Mr. Watts, Mr. Chairman. The example used in your testimony as an appropriate place for the type of device that you pointed out is an automobile repair bodyshop. The subcommittee has information there are literally thousands of these in use in Government circles. What would be the appropriate setting of these? In the normal administrative executive office situations?

Mr. WATTS. Normally I wouldn't think so under those circumstances, but I am sure in this building there is probably a machine room or repair shop where it might be desirable to have one, so that by releasing the buttons cut the transmitter out and the side noises of the telephone would be eliminated and you could hear better. The potential abuse is obvious in that you could use that same telephone device as a wiretap, cut out the transmitter and reduce the possibility of being detected as a wiretap.

Mr. STETTNER. In one of the appendices you have a picture of service observing equipment that is mounted on a bracket on a desk in a telephone business office. The date on that picture indicates it is pretty ancient equipment. Are there any other types of equipment used, in a similar type circumstance in a business office, for supervisory monitoring of the way employees deal with customers?

Mr. WATTS. I think the exhibit that you are referring to probably was a calendar on an inkwell or something of that sort which is really an antique in techniques that are being used. I don't believe they are being used any longer, not since Mr. Beirne waved one in a congressional hearing some years ago to demonstrate how the customer and the employee could be listened to as far as conversation was concerned.

I don't believe that particular calendar device and the inkstand are being used any longer. The area is wired in such a way that the conversation between the employee and the customer coming into the public area to talk to that employee can be monitored from another area.

Mr. STETTNER. Is the customer on notice?

Mr. WATTS. No.

Mr. STETTNER. The employees are not on notice?

Mr. WATTS. The employees are on notice that they can be monitored almost anytime.

Mr. CAMING. May I comment, Mr. Moorhead?

Mr. MOORHEAD. Yes, Mr. Caming.

Mr. CAMING. If it may be of any help, the use of desk microphones and the like in business offices was used in the 1960's or up to the 1960's as one of the ways of measuring the quality of service rendered in a business office face-to-face. After the Long committee hearings of the Subcommittee of Administrative Practice and Procedure in 1965 and 1966, we had occasion, and that was my early advent into this position, to reexamine the use and at that time it was being used in virtually none of our offices. It had pretty well phased out.

In 1968, if I recall correctly, the use of such equipment for such observations was phased out of our contact measurement plan for observing face-to-face contact.

I recently had occasion, just Friday last, to check on this point, and I had been informed that to our knowledge, and I spoke to the assistant vice president among others of the business offices at our headquarters, that that is not used in any of our offices.

I would like to make one other comment if I may, just to clarify Mr. Watts' statement. To my knowledge, there is no covert way in which face-to-face contacts are observed in the business offices at this time by any wire arrangement. There is supervisory observance. It is both visual, supervisors in the room observing service representatives dealing with members of the public, and there also is some in the area of remote observing on those who are in telephone contact. But to my knowledge there is no face-to-face.

Now, Mr. Watts may have additional knowledge on that.

Mr. WATTS. I don't have any personal knowledge to the contrary, although I have been misinformed if it is not. I will do some checking to see about my information.

Mr. STETTNER. As to the videophones that are used in business offices?

Mr. CAMING. I am talking about the normal contact where a customer comes into the office and talks directly to an employee.

Mr. STETTNER. If the customer walks into the business office and picks up a videophone in the general area and speaks to a service representative, is that telephone marked in any way to indicate that it is subject to service monitoring?

Mr. CAMING. No. I don't know, unless there are a few locations within the United States where there may be picture phone equipment that that is done.

Normally when one walks into a business office it is like walking into a bus terminal. One doesn't pick up the phone. One deals directly with the person on the other side of the counter.

Now, I do know in Chicago, for example, where picture phone has been used on an experimental basis that we have attempted to encourage use. Now, whether it includes use of the picture phone in the business office rather than talking to a person across the counter I have no personal knowledge.

But it would be no more than one or two offices that would do that, if any.

Mr. STETTNER. Thank you.

Mr. MOORHEAD. Mr. Alexander?

Mr. ALEXANDER. Mr. Chairman, one question.

Mr. Caming, as I understand it, your statement is that the reason for service observing systems being sold are principally for the determination of need for training and, two, improving the quality of service rendered by employees; is that correct?

Mr. CAMING. May I understand, because these terms are used so interchangeably, Mr. Alexander, that I, for self-serving purposes perhaps, clarify.

Mr. ALEXANDER. I am quoting from page 5 of your statement.

Mr. CAMING. The reason I said that you had referred to service observing and we refer to that as supervisory observing as done by telephone personnel.

Mr. ALEXANDER. What is the difference?

Mr. CAMING. Well, the difference is that in service observing by telephone company personnel at certain observance locations, this is done on a purely random statistical basis. There is no knowledge recordwise of the calling or the called party or any indication of any particular employees involved. It is purely to determine the character of the index of the office or group.

Now, supervisor——

Mr. ALEXANDER. What do you mean by determine the character of the index or group? I am trying to decide in my mind what the reason for this is.

Mr. CAMING. Certainly.

For example, there will be service observing say in the traffic department on calls to directory assistance for information. There will be service observing on what we call direct distance dialing outgoing trunks and incoming trunks to determine whether a call that was made went through or met with equipment blockages, say at the first switching station, whether it was misdirected, whether there was a matching loss, for example, your call reaches a point say where there should be an idle line to the particular number you call but there is a mismatch of the equipment so it doesn't get in.

Mr. ALEXANDER. Would it be fair for me to conclude that the principal purpose for service observing systems being sold is to measure the quality of service?

Mr. CAMING. Yes.

Mr. ALEXANDER. Is that what you are saying?

Mr. CAMING. Well, I was talking about what the telephone company does and we call that service observing.

Mr. ALEXANDER. Right. Now can we stop right there for a moment?

Mr. CAMING. Sure.

Mr. ALEXANDER. I have some data here which indicates that your need for determining the quality of service through the sale of service observing systems has increased dramatically since 1970. It appears that the Bell System sold 7 of those systems in 1970, 83 in 1971, 159 in 1972, and 1,125 in 1973, for a total sales systems of 1,417. Does the data match up with the information that you have?

Mr. CAMING. Mr. Alexander, I believe there is a complete misunderstanding, sir. First, if I may, just so that we understand we are talking about the same thing, otherwise I may be misleading, when I was using the term "service observing," I was just talking about something done by the telephone company with secure offices. We do not sell that or provide that service. My statement deals with furnishing equipment to business subscribers for supervisory observing and service training purposes. That has nothing to do with our service observing practices.

Normally this is provided under tariff. We do not sell these systems, and I am not quite sure what we are talking about as a result.

Mr. ALEXANDER. Well, we are talking about manufactured equipment sold to the Bell System.

Mr. CAMING. Oh, sold to the Bell System. I thought you said sold to our customers.

Mr. ALEXANDER. For the purpose of service observing systems.

Mr. CAMING. I believe that has nothing to do with my statement but rather something that Mr. Watts had adverted to, that we may have purchased, and that may be, from Tel-Tone Corp. a number of these remote units since we have found that it is in the public interest to use those in our official service observing, and we are expanding our use of that equipment for the reasons I have described. But this is for our own purposes. It is not furnished to subscribers and was not mentioned in my statement at all nor adverted to.

Mr. ALEXANDER. Why has your need for service observing increased from the purchase of 7 units in 1970 to 1,125 units in 1973?

Mr. CAMING. I think that can be readily explained, Mr. Alexander, when you see the universe that we are dealing with.

In 1970, after very careful determination, and we had been working through some other systems to improve the quality control of our service observing to reach, as I had mentioned, more remote areas of the States to insure closer supervision, we had been, through our Bell laboratories, looking at various systems and attempting to develop some such as our service evaluation system to permit greater access to a larger universe of offices. Now, at that time it was felt that the Tel-Tone equipment, which I had mentioned, would provide at least at this stage, the satisfactory results that we had desired. As a consequence, in 1970, the first sets were tried on an experimental basis.

Now, you must appreciate that these units are small units. They cover only a certain number of——

Mr. ALEXANDER. Without interrupting you, could you tell us how many units that each of these systems can service?

Mr. CAMING. I don't know that offhand, but I may have some order of magnitude.

Mr. ALEXANDER. Mr. Chairman, these are facts that can be established, if he wanted to submit that later for the record.

Mr. MOORHEAD. Let's go off the record for a moment.

[Off the record discussion.]

Mr. MOORHEAD. Before we proceed, I just want to say to Mr. Eger, Mr. Joyce, and Mr. Gentile that the subcommittee will meet again at 2 o'cock to hear your testimony. I am sorry we couldn't get to you this morning. I wanted to get it all finished but it just didn't seem possible.

Thank you very much.

Mr. Alexander.

Mr. ALEXANDER. Mr. Chairman, when the gentleman finishes responding to my last question, I have no further questions.

Mr. CAMING. Thank you, Mr. Alexander.

Each one of these units covers a small number. For example, I was looking at some figures as to the minimum of trunks covered. If you have 1 to 10 trunks, that is a different plant repair group; and a large number of trunks are furnished to each plant repair office; and each business office might have a large number of trunks. There are 1,800 repair service centers to be observed, each having a large number of trunks.

Now, as to our business offices, we also have at the present time at the end of 1973, and I was looking through my figures, we do have a large number of business offices. I don't have the figures immediately at hand on that.

Mr. ALEXANDER. Mr. Chairman, could the gentleman submit that for the record?

Mr. CAMING. We will be glad to submit how many plant repair bureaus and business offices we do have. [See p. 177.]

Mr. ALEXANDER. Thank you very much.

Mr. CAMING. In other words, the number of units purchased, considering the number of offices involved, for example, like we had 30 plus billion dollars worth of equipment and each of these units is a small unit, purchased by the thousands or less, is not an order of magnitude for the operation that has to be accomplished.

Mr. ALEXANDER. Thank you very much.

Mr. MOORHEAD. Could you also tell us about this difference—on page 5 you talk about supervisory observing equipment furnished to businesses. That is not the equipment you were talking to Mr. Alexander about, was it?

Mr. CAMING. No, the equipment that is furnished is mainly like automatic call distributors, which you may not——

Mr. MOORHEAD. What I want the figures on is the number of monitoring devices within a business, the kind you describe on page 5.

Mr. CAMING. Well, we have—yes—we have, as I mentioned at the top of page 5, the bulk of the provisioning of this equipment is in the form of automatic call distributing equipment and they range from 60 to several hundred, for example, Eastern Airlines.

Mr. MOORHEAD. What I am interested in is the way a supervisory person can monitor the call of a nonemployee to check up on the proficiency and job performance of that employee.

Mr. CAMING. Fine, if we are using as an illustration the automatic call distributing system, which is the most frequent, that has a monitoring capability. In other words, a call comes in at random from the outside.

Mr. MOORHEAD. Is that subject to these requirements that you list on page——

Mr. CAMING. Oh, yes, these are all subject to these requirements. The different types of equipment are merely to give you a description of the types of equipment we furnished, all of which are furnished under these type tariff preconditions.

Mr. MOORHEAD. And every piece of equipment that you furnish is subject to these listed limitations?

Mr. CAMING. That is our policy on the furnishing of observing equipment that it not be furnished except under those—certainly—in fact, we recommended and made this statement as early as 1966 in reply to the August 11, 1966, questionnaire to the Subcommittee on Administrative Practice and Procedure, and we did outline at that early date that these conditions which are set forth herein are our policy, and I recently had the matter reaffirmed by a telegram sent out by our marketing people.

Mr. MOORHEAD. This is a matter of company policy, not law?

Mr. CAMING. This is purely a matter of company policy due to our concern for privacy.

Mr. MOORHEAD. Do you furnish this equipment to the U.S. Government?

Mr. CAMING. As a customer we do furnish it to certain agencies of the U.S. Government.

Mr. MOORHEAD. Do you put the same limitations on the Government as you do on other customers?

Mr. CAMING. They stand in the shoes of all of our other customers as far as the normal provision of services.

Mr. MOORHEAD. Do you, with any customers, or customers in general, and the Government in particular, make any check to see if the customer is living up to these limitations?

Mr. CAMING. I might in this instance mention to you by way of illustration, because I thought it would be of interest to the subcommittee, that we were asked, for example, to provide certain observing facilities at one of the airbases in Massachusetts, and we——

Mr. MOORHEAD. This would be one of the types described on page 5?

Mr. CAMING. Well, to permit them to do certain types of communication security monitoring, communications monitoring on their facilities.

Mr. MOORHEAD. Monitoring of their personnel?

Mr. CAMING. Yes, and calls to them. They are talking about calls, both their private line facilities on the base, private networks and also calls that might come into their networks.

We provided under the following written preconditions, that the lines to be monitored are provided for the transmission only of official Government business. In other words, we provided only for those lines, not for personal calls, and that all users be notified of their conversations being subject to such communication security monitoring in accordance with the appropriate DOD directives which we mentioned.

Second, that whenever any recordings should be made by the military during such monitoring that they will conform with the FCC requirement for a periodic beep tone.

Third, that they will keep this equipment and our interface—and they actually supplied in this case the equipment and we merely provided the wiring that would interconnect to their lines, in other words,

they provided the terminal equipment in this case. The military often do. But they said they would keep all of this equipment under proper safeguards, to be accessed only by authorized military personnel having a need to know in that connection and that last, all applicable tariffs, both interstate and intrastate relating to the customer-provided communications equipment would be complied with fully.

Now, this is our normal requirement when we supply this or are asked to assist in the provision of any assistance or wiring for observing purposes.

Mr. MOORHEAD. Can you supply for the record the number of such monitoring devices that you have furnished to Federal departments and agencies?

Mr. CAMING. I believe we could. It may take some time. We have already provided the committee with such information in the metropolitan area, I believe, of Washington, D.C. Would you like it on a more expanded basis?

Mr. MOORHEAD. I think Washington, D.C. will do.

Mr. CAMING. We have already provided that information to your subcommittee; Mr. Phillips, is that correct?

Mr. PHILLIPS. That is right.

Mr. MOORHEAD. Thank you.

Mr. Cornish.

Mr. CORNISH. Thank you, Mr. Chairman.

These comments and questions are directed to both witnesses.

I am especially interested in the service observing devices also. As we understand it, these are used by Government and private companies to determine the quality of service being rendered to customers. Now, that sounds like a very worthwhile objective. But I would like to ask both of you whether you have ever known Americans to be reluctant to complain to the telephone company or to the Government about poor service, discurteous employees, and the like?

Mr. WATTS. I haven't known them to be reluctant to do that, no.

Mr. CAMING. Mr. Cornish, reechoing Mr. Watts' strong affirmation of our strong lack of reluctance to grouse, given to our Congressmen at times, although there is very little occasion to do that—it must be recognized that the purpose of the supervisory observance would be not to merely gather information as to the volume of complaints, but to attempt to ascertain the nature of the complaints with precision so as to cope with them to evaluate as a form of supervision the type of service being rendered, for example, whether proper information was afforded, say, by an airline reservation clerk, whether further training and assistance of the individual was required.

Now, these would be the basic reasons, remembering that the obtaining of this equipment is at some expense to the particular company and they would not undertake it lightly unless they felt that this was necessary for supervisory and training assistance purposes.

Mr. CORNISH. Can you see any reason why any particular Government agency would need 21 service observing systems?

Mr. CAMING. If I may, I think perhaps it might be helpful in our discussion if perhaps we could call this supervisory observing. We do not use the term service observing as such, merely as semantics, perhaps. But this is supervisory assistance which is provided to customers.

Mr. CORNISH. You can call it anything you want. We all know what equipment we are talking about. It is the same thing.

Mr. CAMING. I want to clarify we are talking about it with respect to our customers.

I would say, Mr. Cornish, in all fairness this is a question that the particular Government agency would have to address itself to. I don't think we can say whether or not a particular large facility of the Government which handles huge volumes of calls might or might not have need for that many systems. I could say that a number of Government agencies like other major institutions have the type of call and communication with the public that might require, as far as effective supervision of the service rendered, such observing equipment. But this is not a judgment for the telephone company to make, and I respectfully defer to the heads of the various Government agencies concerned.

Mr. CORNISH. By way of comparison, it is my understanding the Department of Justice has 3 of these devices, and yet another Government agency that we know of has 21.

Mr. CAMING. Perhaps there isn't enough occasion to call the Department of Justice, I don't know.

But really, I would be very pleased to respond, Mr. Cornish. It is just that I am not in a position to know the internal requirements of the particular agency.

Mr. CORNISH. I think you can see what I am suggesting, and that is the purpose of these devices is to determine the quality of service, I think it can be done by other means such as by complaints from citizens. You may not get the precise nature and details of the call, that is quite true. But you do identify, it seems to me, the primary problem involved.

Mr. CAMING. If I may comment, I would respectfully state that that has not been our experience, that we have used a service attitude measurement plan as a supplement to various forms of observing and we do get, as you say, the overall complaint pattern. But the information is not of the nature required for effective supervision and training assistance, particularly with respect to individuals, which is the purpose of this thing.

I am of a firm opinion personally that this form of supervision of these telephone communications is the only adequate way to supervise to determine the individual training, to recognize good performance as well as bad, and to provide necessary assistance, sometimes on a short-range basis. You have a complete range of problems that could not be ascertained merely from the customer's standpoint. It is a question of not only serving the customer to his satisfaction but serving the customer in the best possible way, a responsibility that the Government, as well as any other agency ascertains. There is no other way of examining a product, that is, saying if it is in an assembly line, perhaps if you look at the line and the cars look good as they come by and customers come back and say you did a lousy job, that that would be an adequate form of quality control. At least that has not been our experience or of the major users we have talked to, say in the airlines.

Mr. CORNISH. Let me interject there, if I may.

Certainly as time goes on our citizens have more and more business, in quotation marks, with their Government just by the nature

of the animal. It is becoming more complex and we find ourselves in that situation.

Now, I ask you, in your relationships or contact with the Government of the United States relating to your personal business, do you want those telephone calls monitored for any purpose without your knowledge?

Mr. CAMING. I would say that, since you asked it from my personal standpoint, that I would have no reluctance whatever, that these are calls to the business, to the Government agency. I am not calling anyone personally, as in a sense of a call to an employee to ask them to have dinner.

Mr. CORNISH. But you are discussing your personal business.

Mr. CAMING. But I am discussing it with the agency concerned and I am desirous of having it administered and my questions answered as fully and as responsively as the Government agency can. If the purpose of having a supervisor observe in order to provide better service on a call that is routine and impersonal to start—for example, my tax return refund did not come. If that quality control observation of the particular individual would uncover the fact that perhaps he needed more training in order to administer to my needs, and since it was an impersonal call, well, there is no question of privacy in my conversations at all, vis-a-vis a particular employee. In fact, most of those calls come in at random and don't get any particular employee—I would have no reluctance at all. I would think it would be a responsible, management way of assuring that the best possible service is administered by the Government agencies to me.

Mr. CORNISH. What if you were calling to ask the IRS whether a certain deduction on your income tax was a proper and legal deduction and were so advised that it was not? You would not care to have that information go any further than that, would you?

Mr. CAMING. Well, it would not go any further——

Mr. CORNISH. What you asume, Mr. Caming, with all due respect to you, is that these are all well-intentioned people doing this for well-intentioned purposes. What I am suggesting to you, and that has been amply shown by the events of the last several years, is that in many cases this innocent information and well-intentioned people are not innocent and well intentioned.

Mr. CAMING. As you can appreciate, and I think as the subcommittee can appreciate, I am not able to comment upon that. I can only say that that has been our general experience and remember the Government agencies are just one segment of the 4,000 units.

Mr. CORNISH. But this is the element we are primarily interested in.

Mr. CAMING. I understand that.

I am saying that has been generally our experience that there has been no abuse that we have seen over two decades as far as being brought to our attention. There is no way, as the chairman would understand, that would permit us to critique the performance of any individual absent some indication of impropriety. There has been none and therefore I am not in a position to speculate, Mr. Cornish, as to whether or not there is such abuse. I think you can appreciate my position.

Mr. CORNISH. I can appreciate your position, but just let me ask you this final little tidbit. It wouldn't be catastrophic to the country if service observing was halted by Federal agencies, would it?

Mr. CAMING. I would think that the question of whether supervisory observing equipment is to be used for supervisory and training assistance purposes—by Federal agencies—is for Congress to determine upon the balancing of individual and societal considerations. We, of course, have full confidence in the wisdom and ability of Congress to achieve the best possible result in the public interest as they see it. This is for the Congress to determine, and I am sure Mr. Watts would subscribe to the fact that our basic concern is privacy of communications.

We do recognize that the use of observing equipment has proved invaluable to many people. For example, I was over at Delta just so I could see what an operation looked like in this area, and the subcommittee, if you so desire, we would be very pleased to have you see an operation like this.

Mr. CORNISH. Mr. Caming, if it is a question of privacy or checking of quality of service, let's recognize that might be a gray area; don't you think it would be the better part of wisdom to come down on the side of privacy?

Mr. CAMING. I think you must recognize first, as my statement tried to say, I had hoped eloquently, perhaps not persuasively to all quarters, that we cannot feel in any respect whatever that the supervision in this area is any incursion into privacy, that—if properly used in accordance with the strictures, of course, that I have mentioned in there—that it is a form of supervision just as there are other forms of supervision, including visual. We have a number of forms of supervision, in the traffic room we can plug in next to an operator. That, too, is a form of supervision.

But I would think that basically you are talking about impersonal, routine calls to a place of business. It is not calls to the employees, and there is no invasion of privacy of the caller because he isn't talking to anyone. He wants something from the business, and he is willing to talk to an employee representing the employer.

Now, if the employer feels in order to give him better service that a second supervisory employee should also participate in that conversation, I do not think it invades privacy. However, as I said originally, there is the recognition that Federal agencies have a perhaps overriding responsibility that Congress may wish to examine in the context of other responsibilities and adjust the question of privacy. Perhaps like Caesar's wife, you must not only be faithful, but you must have the appearance of fidelity. In that case we will subscribe to any desires Congress may have.

Mr. MOORHEAD. You quoted from an agreement that you had with the Air Force in a particular monitoring installation. Do you have agreements with each customer who gets this monitoring equipment and particularly do you have an agreement with each Government agency as you install it?

Mr. CAMING. These are with reference to the field. Normally, these were operations at military bases and the like where we might be asked to, you know, provide facilities or wiring.

Mr. MOORHEAD. Mr. Caming, my questions don't seem to be clear to you. I just said do you have an agreement? You said no, you do not have.

Mr. CAMING. I am sorry. I meant that type of agreement isn't the one we would normally get.

Mr. MOORHEAD. Would you have another type of agreement for an installation, say, like the State Department?

Mr. CAMING. I believe the tariffs of the C. & P. Co. do require the subscriber to agree to the terms along the lines outlined on pages 5 and 6 in my statement, and I will be glad to have that checked and that information furnished to the committee.

Mr. MOORHEAD. So if I picked a particular installation at random we could get from you the agreement that was signed?

Mr. CAMING. I believe that is the tariff and administrative requirement of the company. I hesitate, because like any other large institution, this is the policy and these are the recommendations, whether in the particular case you select we had actually done it is something we would hope would be the case. But this is the definite policy and this is what it should be when we provide observing equipment. Therefore, when you ask for the State Department and we have provided them with observing equipment, if our tariff requires, we agree in writing, such as notifying, they agree to use it for lawful purposes, et cetera. I will agree and have it confirmed and have your staff so notified.

Mr. MOORHEAD. You said you didn't believe it was an invasion of privacy if these strictures were followed?

Mr. CAMING. What I meant was whether or not there was an agreement in writing, the equipment does not lend itself to any form, you might say, of illicit wiretapping. If you do that, I think you do it with more sophisticated methods, but these are clearly our conditions and policy. As I say, we recently reiterated and the C. & P. Co. should be following that policy which I believe reflects its task.

Mr. CORNISH. If we could demonstrate that some Federal agency was in gross violation between the agreement of the telephone company and that agency, what action would you take?

Mr. CAMING. When we have any indication of an impropriety or violation, we would then investigate. If we find it is so we would take corrective action. If it was very flagrant and there was a possibility of recurrence after its disclosure, we would probably suspend or terminate service and our tariffs so permit, and we would take the necessary action. For example, if the agency said they would not cooperate, they would not agree in the future, or if their conduct had been so flagrant that it appeared unlikely that they would comply in the future we would merely remove the equipment. Unquestionably that is our practice.

Mr. CORNISH. Are you aware of the wide publicity given to the observing of calls made by the IRS by taxpayers seeking tax information? I think a very prominent article appeared in the Wall Street Journal and perhaps some other publications.

Mr. CAMING. I am aware that the local office of the IRS, which receives a large volume of calls from the public, does engage in using the supervisory observing equipment, but I have seen no evidence of impropriety.

Mr. CORNISH. Well, the impropriety, if I may suggest it, is that the callers do not know, or did not know until the publicity came out in the press, that their calls were being sampled thusly.

Mr. CAMING. I would respectfully submit that that is not an impropriety, that as the law is constituted at present, one party to a conversation may overhear without the consent of the other party, and

I refer to section 2511(2)(c) of 18 U.S. Code. The present condition is we have the employees of the subscriber know of it. There is no requirement in our tariffs that the other party be advised.

In fact, that would utterly defeat the purpose of proper supervision, and if an employee knew that a particular call was being observed they would not necessarily be getting the reliable normal barometers of performance that is the purpose of this.

Mr. CORNISH. I can only quote one of the distinguished witnesses before the subcommittee today, namely yourself, and that is we believe our customers have an inherent right to feel that they can use the telephone with the same degree of privacy they enjoy when talking face-to-face.

Mr. CAMING. I agree with that, and I do not think that calls to a business which are calls to the business, and when they are willing to speak to any member of the business who is an employee representing it, that conversation does not constitute any invasion of privacy since they initiated it. To have a second employee participate for supervisory purposes—for example, as the Supreme Court said, *Rathbun* v. *U.S.* in 1957, if one employee held out the headset and had a second employee listen to it for assistance purposes without telling the caller, that clearly does not constitute an invasion of privacy of the caller. The caller has no concern, in my opinion, whether one or two employees of the particular company service him.

Mr. CORNISH. That is for telephone assistance. We are talking about highly substantive personal matters that are being discussed with the Internal Revenue Service.

Mr. CAMING. Let me say what we are talking about in the instance of an employee of the Internal Revenue Service answering the telephone at random, usually on an automatic call system, at A one time or B, that that conversation is no more violated if a fellow employee also participates, both representing the same employer. And for supervisory purposes, the caller is not apprised so that the employee called is not aware of it and therefore a normal review of his performance is obtained, remembering that the employee is aware of the fact he is subject to this.

Mr. CORNISH. I won't carry this on forever, but what if the second IRS employee is an auditor and he is providing that assistance and he is making little notations, and I am not suggesting this was ever done, he is making little notations on who this caller was to double-check that return when it came in because of the nature of the conversation?

Mr. CAMING. I would submit that the first employee would also be making these notations to check the return.

Mr. CORNISH. I am not so certain he would.

Thank you, Mr. Chairman.

Mr. MOORHEAD. Mr. Phillips?

Mr. PHILLIPS. Thank you, Mr. Chairman.

Mr. Watts, in his statement, referred to the testimony that John W. Dean III, ex-White House Counsel, gave before the Senate Watergate Committee last year, in which he said that a 28-year-old ex-Bell System employee who went to the White House staff "utilized his associations at C. & P. Telephone Co. to learn the pair numbers of the tele-

phone lines of syndicated columnist Joseph Kraft in order to install wiretaps."

Mr. Caming, can you tell me, did C. & P. conduct any investigation based on Mr. Dean's testimony to determine which, if any, C. & P. contacts may have given this information to the White House staff member to enable him to accomplish this illegal wiretap?

Mr. CAMING. I can assure you, Mr. Phillips, that a matter of such public knowledge was very carefully and thoroughly investigated. Even if it had been brought to us by private complaint, it would have been investigated surely and swiftly, but you can be assured it was doubly done. I was one of the many people on the horn to the appropriate people to find out what were the facts.

To our knowledge, the investigation was a thorough one and competent and clearly with good intentions. We were not able to ascertain that information.

I might parenthetically state that the disclosure of cable and pair information by any employee for any reason other than that in accord with company policy, such as pursuant to a court order authorizing wiretapping under a Federal or State law, is a violation of the secrecy of communications which we indoctrinate our employees in both at the time of hiring and also periodically, usually once a year or more frequently, and such breach can and has led to dismissal.

Now, if we had found the employees involved, and they had been guilty of a flagrant impropriety, appropriate disciplinary action would have been taken. We were unable to do that in this case, as you understand. The potential is such that we could not run it down without further leads.

I might also say that CWA has always, over the years, and before I held this position, I was general labor counsel in long lines from 1957 to 1965, and they have always been most concerned and cooperative in the area of violations of the secrecy of communications, and I think Mr. Watts very eloquently expressed the concern of the CWA and we have always found them cooperative in attempting to uncover facts in a situation of this character. None of those were successful in this particular situation, unfortunately.

Mr. PHILLIPS. During the course of that investigation, can you tell us if the ex-Bell System employee referred to in Mr. Dean's testimony was interrogated? Was that part of the investigation?

Mr. CAMING. Offhand, I cannot respond to that of my own knowledge. I believe he was interrogated or talked to. I don't think—at least it was discussed with him, and I believe from my recollection, and you must forgive me, Mr. Phillips, there have been so many revelations from Washington that I have to keep large files to keep them on separate tracks, but to my knowledge, Mr. Davis denied that information publicly, and I believe it was discussed with him. It would have been the normal and usual and understandable thing to do, and I believe there was no indication of any impropriety disclosed.

Mr. PHILLIPS. Do you know if he was subjected to a polygraph examination?

Mr. CAMING. That would have to be by some other group. The Bell System, with the endorsement of CWA, does not normally use polygraph detectors. Second, we are not a law enforcement body, so if we talk to you, for example, we don't interrogate you, we ask to discuss it with you in depth, and we do not use the polygraph.

Mr. PHILLIPS. I asked the question because last week we held 2 days of hearings on the use of polygraph equipment.

Mr. CAMING. We do not use the polygraph.

Do you know of the use of any of it, Mr. Watts?

Mr. WATTS. No.

Mr. PHILLIPS. You referred on page 2 to the Federal Omnibus and Safe Streets Act and you mentioned the heavy criminal penalties for disclosure or use of wiretap communications. Do you know if there has been any conviction under that provision of the act?

Mr. CAMING. Yes; I believe there have been a number of prosecutions. For example, one comes to mind of Gordon Novell, and I was going to make a very bad pun, Mr. Chairman, and say it was a very novel name.

Mr. MOORHEAD. The Chair should rule you out of order.

Mr. PHILLIPS. Was this a conviction?

Mr. CAMING. This was a conviction, also, of a private detective in Seattle, Wash., and there have been a large number of prosecutions reported in the newspapers. I would think the FBI would have statistics on them.

Mr. PHILLIPS. Thank you very much, Mr. Chairman.

[Questions submitted to Mr. Caming and CWA and the answers thereto follow:]

SUBMISSIONS TO ADDITIONAL SUBCOMMITTEE QUESTIONS

The questions are restated exactly as written in the enclosure to Mr. Caming.

References in the attached answers to transcript pages (e.g., "T. 37–41") denote pagination of the reporters' stenographic minutes (unrevised and unedited) of the Hearing of June 11, 1974, entitled "Telephone Monitoring and Other Surveillance Practices," before the Foreign Operations and Government Information Subcommittee (hereinafter called the "subcommittee").

Question 1. Information furnished to the subcommittee by one national supplier of service observing equipment systems shows total sales of 1,778 units in the five years from 1969 through 1973. Of these, 1,242 were sold in fiscal year 1973. The Bell System companies purchased 1,417 of the 1,778: moreover, in that last year, the Bell System purchased 1,152 units of the 1,242 units sold by this supplier which is not the Western Electric Co. What explanation is there for this major acquisition of service observing equipment from outside sources in recent years?

Question 2. Are these outside manufactured service observing and monitoring systems procured for use by operating companies or for commercial subscribers?

Question 3. What manufactured equipment is generally used in commercial subscriber installations using service observing equipment?

Question 4. What is there about these outside manufacturers' systems that makes them a preferred item for internal use by operating telephone companies?

Due to their close interrelationship, the foregoing questions are being treated jointly for purposes of response. They were generally discussed by Mr. H. W. William Caming during his appearance before the subcommittee at its June 11, 1974 hearing (hereinafter referred to as the "hearing"). [T. 60–64, 36–39, 46–54]

During the hearing, the request was made for information as to the number of business offices and plant repair bureaus within the Bell System. [T. 63] There are currently some 2,450 business offices (so-called record offices) which handle incoming customer telephone calls. Many of these offices are very small, but of the larger ones (that is, those handling more than 2,500 incoming telephone calls per month), about 85 percent, some 1,350, are currently observed upon. There are also some 730 so-called public offices; these business offices are not subject to service observing since their contacts with customers are face-to-face, rather than by telephone. There are also approximately 1,800 repair bureaus in the Bell System at this time. About 1,530 of these bureaus, some 85 percent, are currently observed upon.

The service observing equipment purchased by Bell System companies from an outside supplier to which question is raised is manufactured by the Tel-Tone

Corp. of Kirkland Wash. This equipment has been in use by some Bell System companies since 1970, when it was first installed on a trial basis. Within our operating companies, this particular equipment is used by, and is limited to, official service observing organizations, solely for the purpose of compiling company service measurement statistics. Tel-Tone equipment is not furnished by Bell System companies to business subscribers for supervisory observing, employee training assistance, or other purpose; nor is it used internally by our operating companies for purposes other than official service observing.

Tel-Tone's capabilities of remotely accessing numerous, widely dispersed offices and bureaus from a centralized, secure location, with security features to preclude access to the equipment by unauthorized persons, uniquely lend themselves to use by telephone companies in service observing. Inasmuch as the Bell System did not manufacture standard equipment possessing these capabilities, outside procurement from Tel-Tone Corp. was undertaken.

These specific capabilities are generally not required by business subscribers engaging in supervisory observing and service training assistance with equipment furnished by the telephone company. Such observing is usually performed on the site, that is, on the business subscriber's premises or close thereby, and it normally encompasses only the operations of a single unit, group, or department. Accordingly, the equipment furnished continues to be standard equipment, in general manufactured by the Western Electric Co. Specific requirements for supervisory observing and service training arrangements of course vary somewhat among subscribers, so that facilities provided locally are arranged by each Bell System Co. to conform to the particular subscriber's needs. These arrangements incorporate various types of key equipment, such as multibutton key telephone sets (for example, 6-button sets) and Call Directors (for example), of 12, 18, 24, or 30-button sets) and special switchboard and console positions. Many of these supervisory observing arrangements are provided at present as a feature of the automatic call distributing systems (ACD), rather than through key systems. ACD's vary in capacity, depending on the volume of incoming calls to the business. They range from 60 or less attended positions to several hundred or more in the instance of a few airline reservation centers. [T. 30]

Official service observing is the principal quality control measure of the Bell System, and we know of no adequate substitute for it. Its sole purpose is to enable management to evaluate statistically the overall quality of telecommunications service rendered to its customers. The observed calls are selected on a completely random sampling basis, with no method of identifying beforehand the calls to be observed. Customer-to-customer conversations are not observed, and every reasonable precaution is taken to safeguard customers' privacy. The service observing practices the equipment involved, and the locations where the observing is physically performed promote and ensure such privacy. [T. 47–49]

The Bell System is constantly seeking to improve the quality control results obtainable from its official service observing, in part by extending in a secure fashion each operating company's observing capabilities to as many of its widely dispersed offices as practicable throughout the territory it serves. We have also endeavored to centralize service observing locations to further increase security, promote efficiency, and achieve greater uniformity of results. Equipment like Tel-Tone, with remote, secure service observing capability, significantly enhances our ability to attain these objectives.

After carefully evaluating its performance during a trial period commencing in 1970, we concluded that the Tel-Tone equipment appeared to offer a high degree of efficiency and security. This equipment has, accordingly, been installed and used in increasing numbers throughout the Bell System to observe randomly incoming customer calls to business offices and repair bureaus and thereby statistically measure, from a quality control evaluative standpoint, the overall service performance of the observed units. [T. 61–62]

Tel-Tone equipment has a number of features which enhance its security, including the following:

Knowledge of the security access code (a 7- or 10-digit accessing telephone number) is necessary to gain initial access to the equipment.

An additional security access code must then be dialed (in response to a returning audible tone) within a specified number of seconds, with proper interdigit intervals, or the call will be automatically disconnected.

Incoming calls to the business office or repair bureau are then selected for observation on a totally random basis. [T. 49–53]

As an added security measure, we have introduced and are installing a special dialer that produces frequencies which cannot be duplicated on a conventional

Touch-Tone® telephone. These dialers and security codes are kept in secure quarters, and access to them is confined to authorized service observing personnel. In addition, it is our policy to change regularly the security access code on a random basis. Further, our service observing people are reliable, well-trained individuals and to our knowledge, not one has violated secrecy of communications in almost 70 years. Of course, any disclosure of the security access codes would be a serious breach of the secrecy of communications regulations with which all employees are familiar. Violation of these rules can lead to dismissal. [T. 48, 50–53]

Tel-Tone equipment is not amenable to use as a wiretapping device. Even if one gained unauthorized access to our observing equipment, he would only access lines receiving wholly random, routine business calls to the company at its business offices or repair bureaus. It bears reiterating that customer-to-customer conversations are not observed through the use of this equipment or in any other fashion. [T. 53]

We have been pleased with the more comprehensive and effective quality control results available to the operating companies through the use of Tel-Tone. Among the advantages gained from the use of this equipment have been the following: We have been able to extend our customer service measurements to more locations. Greater uniformity in administration of our service observing has been realized. Better utilization of the work force has been effected. A completely random selection of the calls being observed continues to be achieved. Significant cost savings have resulted. Greater security has been provided through closer supervision of centralized service observing forces. [T. 49–50]

Question 5. To what extent are recorders installed as an integral facet of the service observing and monitoring systems when installed for: (*a*) operating telephone companies? (*b*) commercial subscribers?

(A) OPERATING TELEPHONE COMPANIES

No Bell System company, with but a single limited exception, uses recording equipment in connection with either official service observing or supervisory observing; all such observing is "live" (*i.e.*, nonrecorded).

Customer-to-customer conversations have never been recorded in the Bell System.

Through the midsixties, official service observing in one instance—of incoming customer calls to plant repair bureaus—was generally performed in the Bell System, for quality control customer service measurement purposes, through recording. A so-called beep tone (originated by a tone device automatically producing a distinctive "beep" tone, repeated at intervals of approximately fifteen seconds to indicate to the parties to a call that their conversation is being recorded) was always used when such calls to the telephone company were recorded. An electromechanical selector chose for such observing a random sampling of the customer calls coming in over repair bureau trunks.

However, the Bell System's experience with this method of service observing (by recording) of calls to repair bureaus was not wholly satisfactory. Consequently, the operating companies gradually eliminated such recording and now engage only in "live" service observing, generally from centralized locations, of incoming customer calls to their repair bureaus. In one company, service observing of customer calls to a number of its smaller repair bureaus is still performed through recording (with a beep tone); the remainder of its repair bureau observing is "live." It is anticipated that such recording will be phased out within the next 6 to 12 months.

(B) COMMERCIAL SUBSCRIBERS

Bell System companies do not provide recording equipment to any business subscribers, including Government agencies, for supervisory or service training assistance purposes.

At the specific request of the Department of Defense (DOD), Bell System companies have furnished a limited amount of recording equipment for use in connection with the operation of certain critical military private line telecommunications networks situated within the continental United States [*e.g.*, Air Force Strategic Air Command Primary Alerting System (SAC PAS); Joint Chiefs of Staff Alerting Network (JCSAN); Air Force Command Post Alerting Network (COPAN); and Aerospace Defense Command Network (SAGE)].

This recording equipment is not provided to DOD military organizations for service observing or supervisory observing purposes. It is furnished solely for

tactical and operational purposes . . . to monitor, and recall and verify to the extent necessary, tactical operations undertaken and operational decisions made by the military on their high priority private line networks.

Question 6. Are there any discernible trends in recent years as to the type of commercial subscribers for whom the telephone companies are installing such equipment: (*a*) Private sector customers? (*b*) Public sector customers? (1) Federal agencies? (2) State agencies? (3) Other government entities?

Answer. In both the private and public sectors, the trend generally continues, as it has over the years, for a limited number of large volume users to subscribe, under tariff, to observing arrangements for supervisory and training assistance purposes. As Mr. Caming said at the hearing, it is estimated that some 4,000 to 4,500 of almost 9 million Bell System business subscribers use these arrangements. They continue to be largely businesses. Government agencies and other institutions which regularly receive from, and in some instances place to, members of the public large volumes of calls. Airlines, banks, hospitals, department stores, newspapers, radio and television stations, credit bureaus, telephone answering services, public utilities, and Government agencies (e.g., Internal Revenue Service, Veterans Administration, General Services Administration, and the Metropolitan Police Department of the District of Columbia) are still among the primary users of such equipment. [T. 29–30]

Question 7. Is it possible for commercial or government agency subscribers to telephone service to purchase and arrange for installation of service observing equipment, without obtaining it from a telephone company?

Answer. Yes, it is possible. If the customer-provided terminal equipment is, however, to be connected to the message telecommunications network by direct electrical connection, the business subscriber is required by tariff to obtain from the telephone company the proper connecting arrangement to protect the network from harmful voltages and signals. All interconnection arrangements must comply within minimum protection criteria set forth in applicable tariff provisions and administrative practices.

These interconnection arrangements for customer-provided terminal equipment are required to insure technical compatibility with the message network and thereby preclude harm to members of the general public, telephone company service employees, the quality of service provided, and the complex network itself.

Question 8. Under what circumstances would an operating telephone company not act favorably on a commercial subscriber's request for installation of full-scale service observing equipment (automatic call director, service observing, recording, etc.)?

* * * * * * *

Question 16. In what instances have Bell System operating telephone companies refused to install service observing equipment?

Answer. The operating companies of the Bell System will reject a business subscriber's request for installation of supervisory observing and service training assistance equipment if the subscriber refuses to comply with any of the terms and conditions of the offering or gives other indication that the intended use will be contrary thereto. If, for example, the subscriber indicated its intention to use the equipment for purposes other than determining the need for training or improving the quality of service rendered by its telephone contact employees, or gave any indication of intent to extend the observing to employee lounge telephones used for personal calls, such proposed use would be unacceptable. Likewise, if the subscriber declines to inform affected employees that their business telephone contacts would be subject to supervisory observation, its requests for service will be rejected.

We have only been able to ascertain one instance in which an operating telephone company was obliged to refuse to furnish supervisory observing and service training assistance equipment to a business subscriber. In May 1973, an Indianapolis company, which offered specialized industrial training courses, declined to agree in writing to comply with the terms and conditions of the offering. As a result, Indiana Bell Telephone Co. refused to furnish the requested observing equipment.

Parenthetically, as stated in our answer to question 5.b., the operating companies of the Bell System do not furnish recorders to business subscribers for service observing, supervisory observing, or any other purpose (except limitedly to components of the Department of Defense for the previously-described purposes of tactical and operational use over private line networks). Subscribers

can connect their own terminal voice-recording equipment to the message telecommunications network . . . but both Bell System interstate and intrastate tariffs expressly require any such recording to be accomplished only by means of a direct electrical connection through a Telephone Company-provided connecting arrangement containing a so-called beep tone (i.e., a recorder tone device producing a distinctive "beep" tone, repeated at intervals of approximately 15 seconds to indicate to the parties to the conversation that recording equipment is in use). Some intrastate tariffs, however, exempt from the beep tone requirement police and fire departments and other municipal agencies recording incoming "emergency" calls with their own equipment.

Question 9. What strictures or obligations are imposed by the Bell System on commercial or government subscribers requesting installation of remote service monitoring capabilities?

Answer. As stated in our answer to questions 1–4, observing by business subscribers for supervisory and service training assistance purposes is usually conducted on the site, i.e., on the same (or close by the) premises of the employees being observed, rather than from some quite remote distance. The observing normally encompasses only the operations of a single unit, group or department and is generally situated within the working area of the affected employees or reasonably close thereby.

Identical strictures are imposed upon all business subscribers, including Government agencies, irrespective of where the observing takes place . . . whether within the same physical area as the affected employees (so that the observer can be seen by them), or remotely (i.e., out of line-of-sight of the employees).

All business subscribers, without exception, are obliged to comply with the previously-described restrictions and conditions imposed on this service offering by applicable administrative practices and tariffs. These strictures are uniformly imposed, whether the on-site observing is performed remotely from or within view of the employees being observed. [T. 31–33.]

Question 10. Does the installing operating telephone company require the subscribers to notify employee-users of telephones being monitored that the practice is going on? Does the telephone company do it itself and if so, how?

Answer. As previously stated, applicable intrastate tariffs and administrative practices of the operating companies of the Bell System require business subscribers, including government agencies, obtaining observing arrangements for supervisory and service training assistance purposes to commit themselves to notifying affected employees that their business telephone contacts are subject to observing.

It is not Bell System policy to have the local telephone company itself notify the subscriber's employees. Rather, to insure compliance, each business subscriber is to execute a letter agreement which includes the condition that affected employees will be fully informed by the subscriber such observing. Further, the purposes of the observing are such * * * supervision, training, and development of individual employees * * * that they are all generally aware their telephone business contacts are subject to periodic observing. [T. 31–33.]

Question 11. What responsibility does an installing telephone company accept to insure that the equipment is being used properly by the subscriber?

Answer. Each of the Bell System companies promptly and thoroughly investigates any complaint alleging improper use by a business subscriber of supervisory observing equipment furnished under intrastate tariff, whether such a complaint is presented directly to it or received through regulatory or other channels. Whenever the circumstances of any such investigation so warrant, necessary corrective action is promptly taken by the telephone company, to ensure that the subscriber's usage and practices are in strict compliance with all applicable requirements imposed by administrative practice or tariff. Flagrant or continuing violations (e.g., willful failure or refusal to give the requisite notification to affected employees) would be grounds for suspension or termination of such service.

Over the years, however, Bell System companies have received extremely few complaints or other indications of abuse of this service offering. This favorable experience appears to reflect, in good part, the responsible approach of the businesses, institutions, and Government agencies subscribing to this offering, the routine and impersonal nature of the business calls under observation, and the subscriber's recognition of the vital importance of this form of supervision to the successful operation of its enterprise or agency. [T. 33–34.]

Question 12. The report by the telephone staff committee of the New England Conference of Public Utility Commissioners proposed several courses of action on the matter of service monitoring. Would your company subscribe to the need for each, i.e.—

(*a*) Institute and pursue a program designed to fully acquaint subscribers, by bill inserts and other media, that service observing was practiced?

Answer. The Bell Telephone companies would be willing to introduce a program to acquaint subscribers, by billing inserts and other media, with its official service observing practices. We do not, however, believe such a program is necessary and are concerned that it might be counterproductive. Publicity of this nature could be readily misunderstood and create unwarranted apprehension among our customers that the privacy of their telephone conversations was being invaded. Such an impression would be unfortunate and misleading, for as we have previously stated, customer-to-customer conversations are never observed. The sole purpose of service observing is to evaluate statistically the overall quality of telecommunications equipment and service rendered to our customers by random sampling a minute proportion of calls for customer service and contact performance measurement purposes. The privacy of our customers' conversations is always fully protected.

Furthermore, all Bell System companies conduct a vigorous program to insure every reasonable precaution is taken to preserve privacy through physical protection of telephone locations and plant and thorough instruction of employees. Only authorized personnel have access to the closely-guarded service observing locations and records, and these locations are kept locked at all times when not in use. Employees who perform service observing duties are chosen from our more experienced people. They are persons of demonstrated reliability—selected with care, thoroughly trained, and closely supervised. They, like all employees, are regularly reminded that as a basic condition of employment they must adhere strictly to company rules and applicable laws in the area of secrecy of communications. They are required to read a booklet describing their responsibilities and what is expected of them. Violations can lead to discharge. In, however, almost 70 years of service observing in the Bell System, we know of no instance where a service observer has ever violated the company rules designed to protect the privacy of our customers' conversations. [T. 47–48.]

Official service observing is performed solely for the purpose of providing Bell System management and the appropriate regulatory bodies with their principal source of statistical information regarding the overall quality of service being rendered to the general public. In no wise does service observing conducted in accordance with the strictures and safeguards uniformly applied throughout the Bell System constitute an invasion of personal privacy.

Question 12. * * * Would your company subscribe to the need for each, *i.e.*—

* * * * * * *

(*b*) Bring service observing and monitoring practices directly under regulatory scrutiny by covering it in the General Regulations of tariffs filed with commissions?

Answer. Over the years, Bell System observing practices have been under legislative oversight and regulatory scrutiny on an ongoing basis. In 1966, for example, they were reviewed by a committee of the National Association of Regulatory and Utility Commissioners, and a recommendation was included in NARUC's 1967 annual report that each of the state utility commissions review the service observing policies and practices of the operating telephone companies under its respective jurisdiction.

The question of whether the official service observing practices, prepared by A.T. & T. and uniformly administered throughout the Bell System, satisfactorily comport with privacy of communications has been extensively reviewed, by the Federal Communications Commission and by the various State regulatory bodies (e.g., California, Connecticut, Georgia, Maine, Massachusetts, New Hampshire, New York, Rhode Island, and Vermont).

On September 14, 1966, Mr. Hubert L. Kertz, A.T. & T. vice president—Operations, testified on behalf of the Bell System before the Subcommittee on Administrative Practice and Procedure (of which Senator Edward V. Long was then the chairman) of the U.S. Senate Committee on the Judiciary concerning the vital importance of service observing as a quality control measure and the manner in which it was conducted. Also, on September 8, 1966, and December 8, 1966, A.T. & T. furnished detailed written responses to a series of questions posed by Senator Long relating to service observing.

Thereafter, in section 802 of the Federal Omnibus Crime Control and Safe Streets Act of 1968 [18 U.S.C. § 2511(2)(a)], Congress recognized that service observing and random monitoring for mechanical or service quality control checks was a necessary incident to the rendition of telecommunications services, and expressly authorized such practices. Commenting on this portion of the act, the Senate Judiciary Committee in Senate Report No. 1097 (April 29, 1968) said on page 93:

"Service observing is the principal quality control procedure used by these (communications common) carriers for maintaining and improving the quality of telephone service."

These examples of regulatory and legislative oversight of our observing policies and procedures demonstrate that they are under careful and continuing scrutiny and that general tariff regulations relating thereto are not needed.

Question 12. * * * Would your company subscribe to the need for each, that is——

* * * * * * *

(*c*) Automate the service observer's key, by a relay or some other method, to cut off at the time the caller is connected to the party called?

Answer. It bears reiteration that service observing does not include any listening to customer-to-customer conversations. Each official service observer is rigorously trained and fully instructed to remove herself or himself from an observed connection between customers as soon as the called station or party is connected. Service observers are carefully supervised and their work output closely reviewed to insure they strictly adhere to such instructions. The large daily number of observations that must be taken and noted, and physical indicators such as cords, display panels, and the visual lamp signals at each observer's position (indicating whether an observer is still on a connection), also significantly contribute to precluding any improper conduct. The observers of course understand that severe disciplinary measures will result from any violation. As previously mentioned, however, in almost 70 years no official service observer has, to our knowledge, ever violated instructions by improperly intruding upon customer conversations. [T. 48]

To provide additional assurance, service observing positions throughout the Bell System are generally equipped with a semiautomatic exclusion feature, which further minimizes the official observer's presence on the connection. As soon as the brief required data is noted, the observer immediately disconnects from the circuit at the effective start of customer-to-customer conversation by pushing the requisite key. The observer cannot thereafter reenter that connection, unless the observer is automatically restored by the equipment to the audible portion of the connection by the customer recalling the operator through appropriate signaling (flashing the switchhook) or the customer hangs up at the conclusion of the conversation.

Furthermore, the Bell System is currently concentrating on the research, design and development of a so-called service evaluation system. Through new or modified equipment and arrangements, the proposed system will result in fewer, more centralized service observing locations and increased mechanization, including expanded use of computerized techniques to obtain, automatically, requisite service measurements. We anticipate that such a system will produce even greater uniformity in administration, more effective utilization of the work force, significant cost savings, and increased security through closer supervision of centralized service observing forces. Also through such increased mechanization and computerization, the human evaluation of the quality of service will be further reduced.

Question 13. Furnish copies of the written agreements made between the Bell System operating telephone companies and those Federal agency subscribers in the Metropolitan Washington, D.C. area for whom service observing equipment has been installed, showing the strictures imposed on use of the equipment by the subscribers.

Answer. Attached hereto as attachments 13–A et seq. are copies of written agreements with Federal Government agency business subscribers in the metropolitan area of Washington, D.C., relating to the provision of observing arrangements for supervisory and training assistance purposes. [These agreements are in the subcommittee's files.]

Question 14. For comparative purposes, furnish copies of the written agreements made between the Bell System operating companies and representative commercial subscribers in this same area, where similar telephone service is being furnished.

Answer. Attached hereto as attachments 14–A et seq. are copies of written agreements with representative business subscribers (other than Federal Government agencies) in the metropolitan area of Washington, D.C., relating to the provision of observing arrangements for supervisory and training assistance purposes. [The copies are in the subcommittee's files.]

Question 15. Furnish sample copies of the written agreements used by other major operating telephone companies of the Bell System which have installed service observing capabilities for the Internal Revenue Service, the Veterans' Administration, and the Social Security Administration in other parts of the country.

Answer. Attached hereto as attachments 15–A *et seq.* are sample copies of written agreements used by other operating telephone companies of the Bell System, relating to the provision of observing arrangements for supervisory and training assistance purposes to business subscribers. [The copies are in the subcommittee's files.]

Question 16. See pp. 180–181.

Answer. See pp. 180–181.

* * * * * * *

Question 17. Notwithstanding the presence of an automatic call distributor in a service observing system installation, is it not a relatively simple matter to then selectively transfer some of the incoming calls to a specific supervisory monitor console position, thereby negating the alleged "random access" which ensures privacy?

Answer. Several models of Bell System-furnished Automatic Call Distributing Systems (ACD) contain, as an optional feature which a business subscriber may order, the capability of transferring incoming calls from an attendant's position to the console position of his (or her) supervisor.

If such a feature is included, the ACD will still automatically distribute the incoming calls in the approximate sequential order of arrival to the attendant positions in the order of their availability. If at any given time all of the attendants' positions are busy, a recorded announcement will still advise the calling party that he has reached the company, that all of its attendants are busy at the moment, and that one will be available shortly. The waiting call will usually then be randomly distributed to the next available attendant. This random distribution process is the same, irrespective of whether the ACD has the above-described transfer capability feature.

When the transfer capability is present, any attendant receiving an incoming call through random access can, if the attendant so desires, signal the supervisor and transfer the call to the supervisor for handling by the latter. This supervisory function is wholly unrelated to the supervisory observing function, inasmuch as the supervisor receiving a transferred call is directly involved in handling, rather than observing, the call in progress. Further, the presence of this transfer capability does not affect the "random access" manner in which calls are distributed by the ACD to its attendants.

RESPONSES OF GLENN E. WATTS, PRESIDENT, COMMUNICATION WORKERS OF AMERICA TO WRITTEN QUESTIONS SUBMITTED BY THE FOREIGN OPERATIONS AND GOVERNMENT INFORMATION SUBCOMMITTEE

Question 1. "Your example of a situation where a transmitter cutoff switch or push-to-talk switch would be appropriate was an automobile body shop. What more typical situations are there in Federal agency offices or other facilities where such devices would be appropriate?"

Answer. In Federal agencies, other examples would be Command and Control Centers, because of the security requirements to prevent background conversations from being intercepted; Federal Aviation Agency tower and control rooms; Coast Guard search and rescue operations headquarters, under emergency conditions; composing and press rooms of the Government Printing Office; boiler rooms and machine shops of agencies, because of the noise levels. All of the foregoing examples show a morally neutral use of the "push-to-talk" switch or transmitter cutoff, since the issue of privacy is not existent.

Question 2. "What alternative means of giving notification to callers that their conversations were subject to monitoring would you recommend as being most effective and most practical?"

Answer. 1. License of users of such equipment, with the holders' identities publicly available in company tariffs; 2. Identify the users of such equipment in the telephone directories, as is done in Georgia pursuant to statute; 3. Recorded message to callers, telling that their conversations with the personnel in "X" department are subject to monitoring; 4. The person accepting the call, such as a service assistant, would begin the conversation with a statement telling that the call is subject to monitoring; and 5. A variation of the "Beep" tone required for recorder use, to indicate that monitoring is in progress.

In 1966, the telephone staff committee of the New England Conference of Public Utility Commissioners conducted a study of the service observing practices of New England Telephone & Telegraph Co. and Southern New England Telephone Co., which serve the six States lying east of New York. That 1966 study stated that service observing extended through all departments, and was conducted on a centralized basis in four locations—Boston, Lawrence, Springfield, and Providence. The 1966 staff study recommended that the companies be required to undertake a program to inform the public that their calls were subject to monitoring, and to bring the monitoring practice under the regularly published tariffs filed with the State utility commissions. In that six-State area, the monitoring originated about 1910, and was extended to plant repair service in 1928.

Question 3. "Have CWA employees been surveyed concerning service observing and monitoring, and if so, what are the consensus views?

Answer. CWA has conducted four nationwide surveys of members on the broad area of "job pressures," which includes various methods of observing employees at work. The job pressures studies, conducted by committees established by the executive board, were in 1968, 1969, 1970, and 1973. The idea to study job pressures originated at the June 1967 convention of the union.

Attached is a copy of a chronology of events, taken from a report to the executive board. The full reports of the job pressures committees are held on a confidential basis, with the distribution limited to approximately 20 top officials of the union whose duties involve various aspects of bargaining.

A CHRONOLOGY OF EVENTS

At the 29th Annual Convention in Kansas City, June 19 through 23, 1967, Delegate McCoy P. Garrison Jr., president of CWA Local 2204, made the following motion:

"Mr. Chairman, I move that this convention mandate the executive board to conduct a study of the undue pressures being applied throughout the Bell System to traffic operating employees and of appropriate measures to alleviate such pressures."

Delegate Garrison supported his motion as follows:

"Our traffic operators rate high on the list of those employees under constant pressure to meet unreasonable and uncalled for indexes set forth by the company, not the customer. Operators are under constant pressure to meet certain computed indexes which will only be raised once they have met the objective.

"The pressures applied to these employees has led to unnecessary absence because of nervous sickness or nervous breakdowns, widespread use of tranquilizers and a large turnover in the traffic operating force.

"Constant supervision through monitoring devices, such as supervisory consoles and recording devices, plus constant monitoring and direct supervision by the management create a condition which parallels the sweatshops we have fought against for so long. Ways must be found to create a more desirable and healthier atmosphere for our traffic operators under which to work."

It was then understood during subsequent convention discussion that job pressures studies would include all departments of both Bell System and non-Bell telephone companies.

Soon after the convention, President Beirne appointed a job pressures study committee consisting of:

Clara Allen, New Jersey director (chairwoman).
Robert Butland, president, Local 1022.
McCoy Garrison, president, Local 2204.
Faye Holub, president, Local 6312.
Bertha Van Sittert, president, Local 6323.
Ellis Crandell, president, Local 9409.
Myrtle Robertson, secretary, Local 3372.

The first job pressures survey was conducted in April, 1968. The survey was sent to all CWA local presidents. Although this survey contributed a vast wealth of qualitative information, it did not measure the pressures and employee attitudes

on a quantitative basis, nor did it give information on a district or company basis. It was determined that more detail was needed.

The second job pressures survey was taken in March 1969. The committee devised and distributed two questionnaires designed with similar objectives, but to have different approaches. One questionnaire was sent to all local presidents having questions geared to the amount of grievances processed in various problem areas. The other questionnaire was sent to a randomly picked sample of union members employed by the telephone industry having questions which pertained to their attitudes and experience on the job.

On June 4, 1969 the results and conclusions were sent to the CWA Executive Board by the job pressures committee. A week later Louis B. Knecht gave a preliminary and confidential report of the findings to the executive board.

At the 31st Annual Convention, June 16 through 20, 1969, Clara Allen, chairwoman of the Job Pressures Committee, reported the results and conclusions of the surveys, as follows:

"We have verified by an extensive and thorough study that job pressures do exist in the telephone industry. A significant 63 percent of CWA local presidents and 45 percent of local members surveyed attested to this fact by responding to questionnaires that consisted of eight or more pages. This response far exceeded the normal 12 to 15 percent response of the average two-page political survey.

"In order to obtain measurable factual information, an enormous amount of planning and fieldwork was necessary. For this and their very willing cooperation and assistance in compiling the statistical data, the committee is truly grateful to the CWA Development and Research Department.

"An in-depth study involving two separate surveys was conducted to obtain the statistical data necessary for the committee to arrive at their conclusions.

"The first survey, sent to local presidents, explored a multitude of problem areas. The second survey was more precise so that there could be actual measures of working conditions. This second survey consisted of two questionnaires; one was sent to all local presidents of telephone locals, and the other was sent to 11,000 local members. The response of this final survey overwhelmingly bore out the analysis developed in the early survey.

"The outstanding example of the problems that exist is the company's absentee control program. The committee found that fear is generated from the excessive disciplinary action taken by management against employees who have been ill. Approximately 40 percent of the locals reported having suspensions due for absentee control. There is also an alarming rate of dismissals and promotion denials. As expected, the individual survey revealed that absentee control is a larger problem with the females than the males. This survey also confirmed that the fear of disciplinary action encourages employees to take unpaid days off rather than reporting in sick.

"It is now evident that "index systems" or "work measurements" are one of the more serious problems and also the focal point of most other job pressures. The committee, supported by the statistical data, concludes that such systems do not adequately determine normal workloads and personnel requirements. Furthermore, the poor design and administration of the index system now present in the Bell System encourages "beefing up" the normal rate of production by various dishonest methods, thus resulting in unfair competition. An alarming four-fifths of the local presidents felt that unfair competition was promoted by the existing index system, and an overwhelming majority felt that the results of such a system was reported inaccurately to top management. According to our sample, one out of every four females was disciplined last year resulting from the index system.

"Working supervisors very materially affect the honest reporting of work measurement. The results of their production distort the figures, making an understaffed work location "look good."

"Management's various practices of job observation have caused gross irritation among our members. Three out of every five females surveyed responded that such job observation creates an uncomfortable or harassing atmosphere. The committee recognizes the need for a means to evaluate job performance; however, the existing administration and methods of job observation are not only harassing in the extreme, but are degrading to the employee and must be changed if employee morale is to be improved from its present low state.

"The main issue developed in the area of overtime stems from the company's irresponsible handling of overtime assignments. It appears that short overtime notifications plague male workers more than female workers; however, the committee points out that the scheduling of sixth-day overtime in the traffic department is a problem that is growing rapidly.

"Both individual members and the local presidents expressed an attitude of mistrust toward the company's use of personnel records. It appears that the company has been neglecting to inform employees when items are to become part of their records, and members are not always given the right to review their records. Almost one-half of the locals stated that they felt the entries made into personnel records are unfair.

"The adequacy of company training programs was severely criticized by both the local presidents and the individual members. Over three-fourths of the locals gave poor ratings to such training programs. Also, more than a majority reported that management expects too much too soon from newly trained employees.

"There is significant evidence that the number of employees is insufficient in most cases to provide adequate service to the customer. This naturally throws a greater workload on the employees and a heavier burden on firstline management.

"In concluding this report, the committee emphasizes that the stature of the telephone industry in the public eye is in critical danger. When asked how they would recommend a company job similar to theirs to a friend outside the company, two-thirds of the employees that responded failed to rate their job as a good one."

On October 2, 1969, President Beirne appointed a Job Pressures Implementation Committee to determine what action could be taken to alleviate the work pressures existing in the telephone industry. The committee members included Clara Allen, New Jersey director; Patsy L. Fryman, CWA representative, district 4; and, Victor Crawley, area director, district 6;

At an executive board meeting held on March 13 and 14, 1970, the Job Pressures Implementation Committee report was reviewed, in depth, and acted upon as follows:

(1) The executive board accepts in principle the recommendation of the Job Pressures Implementation Committee.

(2) All responsible officers will immediately act to put into effect those matters which can be handled and will alert those staff involved in job pressure matters to step up activity in their field.

(3) The president is directed to use his office in keeping the companies and the locals aware of the executive board's grave dissatisfaction with working conditions in the industry.

An action chart was devised consisting of five points, as follows:

(1) Send proposal to A.T. & T. for each company to participate in an informal meeting with our people to discuss job pressures. Propose also an ad hoc committee of vice presidents of the companies to meet with a three-man committee of the union to informally discuss job pressures in the industry.

(2) Vice presidents to review pressures in each company in the district with staff. Vice presidents should be prepared with existing information on reported pressures in district and union.

(3) Vice president to set up a meeting between himself and company representatives to talk about job pressures in the particular company. A report of the conversations to be sent to headquarters.

(4) Vice president to endeavor to arrange a meeting between all staff involved in job pressure matters, with as many management people as will come. Meeting to be informal. Report of conversation to be sent to headquarters.

(5) Vice presidents to assign someone in each district to become expert in this question. Said person will make certain that adequate records of reported job pressures as well as action taken to correct such pressures are kept. Person need not be a staffman; it could be done by a local officer or even a competent clerical employee.

At the 32d Annual Convention in Cincinnati, Delegate George Vogelsang, CWA Local 8490, made the following resolution:

"The Federal Communications Commission is conducting inquiries in the broad subject of quality and grade of the telephone and telegraph services offered to the Nation.

"The Commission, in existence 35 years, has not to date evolved a set of standards to define what is the ideal of telephone and telegraph service.

"Telephone service all over the Nation has been in crisis in varying degrees. New York City has been the most troubled area to date. The New York Telephone Co. has been in a crash program of installing facilities to meet the demand. This union and the company have worked shoulder to shoulder in the temporary assignment of plant personnel from other areas.

"The Western Union Telegraph Co. has been curtailing its office hours as well as its delivery service all over the Nation, while at the same time it is asking the Commission to approve higher tariffs. The company also is indicating its wish to abandon the public message service entirely, by its move into "mailgram" service, in conjunction with the U.S. Post Office.

"It is all too simple to rely on stereotyped reasons for the service problems; too easy for management to decry union practices; too easy for the union to accuse the company of putting profit first and service to the public second. Solutions to these problems, as with most other problems of 1970, are far too complex for simple disposition.

"The telephone companies themselves seem to have difficulty in identifying the cause of service quality breakdowns. One executive seemed to blame the personnel—most of them represented by this union—as a major cause in the deterioration of service.

"The trend in the industry has been to resort to assignment of excessive overtime; the threat of demotion; suspension or even discharge for failure to work extra hours; foreshortened or eliminated training periods for new employees; adoption of vicious absentee control programs, including the use of supervisors to check on personnel who are ill; and various other avoidable job pressures.

"Another telephone executive flatly admitted that his company had failed to pay attention to the service demand projections made by its own engineers and economists 5 years ago. The management dismissed the projections then as unrealistic. Now, when the company is in its crash program of adding facilities, it is encountering extrahigh interest rates for the money it must borrow, and extraordinary expenses in payroll for the employees who are paid hourly rates.

"Telegraph service is less and less reliable, but more and more costly. Although Western Union has been allowed to collect a surcharge for physical delivery of messages, it often sends the messages through the mails.

"The Federal Communications Commission did not invite the collective bargaining agent of the employees to take part in the inquiries into service quality.

"As a result, the information now being supplied to the Commission is that which the companies involved wish to provide. The standards are those set up by the companies.

"*Resolved*, That this 32d Annual Convention of the Communications Workers of America urge the Federal Communications Commission to (1) solicit the views of all bargaining agents of the employees regarding quality of service; and (2) develop, adopt and enforce its own standards; and be it further

Resolved, That this union urge the Commission to expand its service quality inquiry so as to include the very important human factors, such as job pressures and excessive overtime, which must necessarily affect the services provided all customers, in the telephone and telegraph industries."

The resolution was adopted unanimously.

On November 24, 1970 a survey questionnaire was prepared by the development and research department containing 41 questions relating to the quality of telephone service and on-the-job pressures. It was sent to a 1 percent random sample of CWA's membership in the telephone industry, approximately 3,000 members throughout the United States.

A report was prepared from the survey data by the development and research department. The results were compiled and utilized by the legislative staff in CWA's intervention in Docket 19129 (FCC Investigation of A.T. & T. tariffs) in May 1971.

At the 34th Annual Convention in Los Angeles, Delegate Eleanor J. O'Neill, CWA Local 5009, made the following motion:

> Mr. President, I move that the convention reaffirm the job pressures program; that the committee be reactivated and local representatives be added; further that the program be reviewed and updated and its goals be accomplished by the 1973 convention.

To implement this motion President Beirne recommended that the committee be reactivated and consist of:

Clara Allen, New Jersey director (chairwoman).
Victoria White, member, Local 2022.
Allen W. Kempf, president, Local 5575.
Marie King, secretary-treasurer, Local 6016.
Bertha Van Sittert, president, Local 6323.
Ellis Crandell, president, Local 9409.

The Job Pressures Implementation Committee still consists of Clara Allen, Patsy Fryman, and Lonnie Daniels.

Mr. MOORHEAD. Thank you.

Thank you both very much for your very eloquent and helpful statements. We know that it is a very difficult area.

The subcommittee will now recess until 2 o'clock this afternoon.

[Whereupon, at 12:30 p.m., the subcommittee recessed, to reconvene at 2 p.m., the same day.]

AFTERNOON SESSION

Mr. MOORHEAD. The Subcommittee on Foreign Operations and Government Information will please come to order.

Today's and Thursday's public hearings by the subcommittee are part of a longstanding and continuing investigation by Congress into the problems of invasion of privacy. At these particular sessions we are focusing on the use of telephone monitoring and telephone surveillance devices by the Government, especially as they affect the people of the United States.

The subcommittee will consider mainly the magnitude and propriety of the monitoring of exchange of information among Government agencies and between those agencies and the public. We firmly believe when a citizen contacts a Federal agency by telephone he should know whether his call is being monitored and recorded and if so, why.

As our first witness this afternoon the subcommittee would like to hear from John Eger, Deputy Director, Office of Telecommunications Policy, accompanied by Charles C. Joyce, Jr., Assistant Director for Government Communications.

STATEMENT OF JOHN EGER, DEPUTY DIRECTOR, OFFICE OF TELECOMMUNICATIONS POLICY; ACCOMPANIED BY CHARLES C. JOYCE, JR., ASSISTANT DIRECTOR OF GOVERNMEINT COMMUNICATIONS

Mr. EGER. Good afternoon, Mr. Chairman.

Mr. MOORHEAD. Won't you sit down?

I will not administer the oath until there is a quorum present.

You may proceed as you wish, read your entire statement or summarize it and we will put the entire statement in the record, as you personally prefer.

Mr. EGER. Thank you, Mr. Chairman.

Because of the statement's brevity, I would like to read it if the chairman pleases?

Mr. MOORHEAD. Fine, we will be delighted to hear it.

Mr. EGER. I am here today with Mr. Charles Joyce, OTP's Assistant Director for Government Communications. I welcome this opportunity to testify before the Foreign Operations and Government Information Subcommittee, and I particularly wish to commend you, Mr. Chairman, the other members of this subcommittee and your staff for the fine work which you have done over the years relative to telephone monitoring and other surveillance practices within the Federal Government.

In 1961, this subcommittee issued a report which criticized the lack of regulations governing monitoring practices and recommended

broad principles which OTP generally supports and which guide OTP's own use of transmitter cutoff switches. For the present hearings, you asked that we discuss the nature and use of telephone monitoring equipment by this Office. OTP does not permit telephone monitoring without the consent of all parties to the conversation. When such consent is given, secretaries may come on the line, and transmitter cutoff devices are useful for reducing background noise. As we reported in response to the GAO survey, three transmitter cutoff switches are installed on secretarial telephone consoles in the director's office. The total rent for fiscal year 1973 was $90; we expect that to be about the same for fiscal 1974.

In addition to OTP's use of the telephone listening devices, you also requested that we summarize the results of the privacy study about which Clay T. Whitehead, Director of OTP, testified before this subcommittee last July. He stated that the Office had undertaken a study of the adequacy of present law and regulation to protect the privacy of individuals in their electronic communications and the security of the systems carrying them.

The study was conducted by Prof. R. Kent Greenawalt of the Columbia University School of Law in New York City. Professor Greenawalt is a distinguished legal scholar with broad experience in the field of privacy protection. His study, entitled "Privacy—Its Meaning and Its Legal Protection," is in the final stages of preparation, Mr. Chairman, and should be available for release in the near future. This subcommittee will, of course, receive a copy.

By way of a brief summary, the study deals with the concept of privacy, the issues regarding its legal protection, and various problems of special concern to OTP and to the Domestic Council Committee on the Right of Privacy. Although the concept of privacy is multifaceted, the study concentrates on privacy as an individual's control of information about himself. The reason for this is that control over information about oneself is a prerequisite for the development of individuality, intellectual growth, creative activity, emotional release and the maintenance of relationships with others.

Professor Greenawalt noted that while there are various significant nonlegal restraints on invasions of privacy including physical barriers, indifference, and ethical restraints, legal protections by far are the most significant restrictions.

A person can lose control of information about himself when information is obtained against his wishes from him or from some area in which he expects privacy, when information is obtained from the original recipient of information against the wishes of both subject and recipient, and generally when information is willingly disclosed by the original recipient against the wishes of the subject.

Among the various legal rules dealing with the acquisition of information from the subject or from areas in which he expects privacy are the law of search and seizure and the privilege against self-incrimination. The first embodies a kind of balancing approach, in theory applied in advance by a disinterested official, the "probable cause" standard defining when the public interest in search overcomes the individual's interest in privacy. By contrast, the privilege against self-incrimination totally insulates some areas from inquiry. The search and seizure approach has been applied to electronic communi-

cation surveillance; the main responsibility for reviewing present law in this regard lies with a national commission created under the applicable 1968 act.

In identifying areas in which there may be a need for further legal protection, Professor Greenawalt's study shows that much information is disclosed by individuals to obtain benefits, such as a job or credit, and there is a need to inform individuals more fully how information is used and to review the need for how much information is gathered.

With respect to the acquisition of information from unwilling original recipients, what is needed is more effective physical protection of record systems from outsiders and from insiders who act with illegitimate purposes. Careful review is also needed of the dissemination policies of original recipients, private and public. Information may be passed on without very strong justification and contrary to the understanding of the subject of the information. The tort right of privacy unfortunately protects only a limited class of disclosure, and systematic legislation and administrative regulation is required to deal with the threats to privacy posed by comprehensive manual and computerized record systems.

While the study states that many of the most dire predictions about computers have not been realized, there is a need to regulate the pervasive record systems that now play such an important part in people's lives. There should be more effective review and control of the kinds of information that are gathered; better efforts to inform subjects of the uses of information; more careful scrutiny of exchanges of information among different record systems. In addition, there should be clearly defined rights of notice, access and challenge to insure accuracy, and to undercut secret files except where clearly needed.

Finally, and of most immediate interest in the context of these hearings, the study identifies the area of monitoring or recording by a participant to a conversation as one of the most murky aspects of the privacy problem. Indeed, Professor Greenawalt has stated that the proper boundaries of such recording and effective enforcement of existing restrictions are among the most significant problems for the protection of privacy.

As we continue to evaluate Professor Greenawalt's study, we intend to give particular attention to the question of participant monitoring within the Government. We shall, of course, work closely with this subcommittee, as we have in the past, to respond to the possible need for further legal safeguards to deal with such monitoring, including the adequacy of the present Department of Justice guidelines in this area.

This concludes my statement.

Mr. Joyce and I are prepared to answer any questions you may wish to address to us.

Mr. MOORHEAD. Thank you very much, Mr. Eger. I think your statement is excellent.

I like your definition of privacy—with the importance of privacy as you have expressed it at the bottom of page 2—"prerequisite for the development of individuality, intellectual growth, creative activity, emotional release, and maintenance of relationships with others." That is an excellent statement. But I am perturbed when I see that statement

on page 2 and then turn to page 5, where I understand you to say that monitoring or recording by a participant to a conversation is one of the most murky aspects of the privacy problem. It seems to me that is a clear invasion of the privacy, not a murky one, if I define murky to be unclear.

Mr. EGER. Until such time as it is finished and coordinated between ourselves and the Privacy Committee and other interested agencies, I can't be definitive. However, when Professor Greenawalt talks about its being a murky area, I think he has in find that there are Supreme Court decisions which say there isn't a constitutional invasion here. We recognize it flirts with some of the fundamental concepts inherent in constitutional principles, and indeed the fabric of our society. There are good arguments on both sides. As compared to some of the other more abusive or offensive violations of the rights of privacy, even as broadly used as that term often is, this particular term of monitoring does raise some problems which are murkier, perhaps, than other forms.

Mr. MOORHEAD. Maybe I am hazy on the word "monitoring." I include in that to mean wiretapping or picking up the extension phone.

Mr. EGER. Yes sir.

Mr. MOORHEAD. And you still consider that to be murky?

Mr. EGER. Yes sir, I think it is.

Mr. MOORHEAD. Murky in the case of the law as it now exists, or murky as to whether it should be considered an invasion of privacy?

Mr. EGER. Certainly murky as to the law which now exists, Mr. Chairman.

Mr. MOORHEAD. I would think that monitoring, by whatever means, is an invasion of an individual's privacy—he loses control over information about him if he is revealing something on the telephone or other device and that is being monitored by someone else—it seems to me a clear case following under your excellent definition.

Mr. EGER. As broadly as one wishes to define privacy, the development question is first, whether it is such an offensive invasion that you wish to define it as an invasion of privacy; and second, what does one do about it? In your home or mine, when two people pick up the phone at the same time, with one on an extension who listens for a minute, that is monitoring, and one might say that is an argument in favor of taking some sanctions against my wife or my daughter, for example. I see the principle there. The question is what do we do with it. To that extent I have to agree with the chairman.

Mr. MOORHEAD. It may be that what we do about it is murky, but it seems to me just as clear as can be that this is an invasion of privacy. It may be a permitted invasion of privacy under court order or something like that, but it is clearly to me an invasion of privacy as you define it. We start with a fairly clear proposition of what it is, and then the murky part begins with what do we do about it. Your definition was so good and then I was a little disturbed about that.

Do you consider that OTP has any responsibility, say, to advise the President on how telecommunications can be used to invade privacy and how it should be restrained?

Mr. EGER. Absolutely, sir. I think it is our responsibility, and there are a number of other agencies with responsibility in this area as well. Our office considers this very high in our order of priorities and with respect to the particular subject of this hearing, that is, participant

monitoring, we intend as one of our acts to investigate further what, if any, recommendations for safeguards we should consider.

Mr. MOORHEAD. I understand you have three of these transmitter cutoff switches in your agency.

Mr. EGER. Yes sir, we do.

Mr. MOORHEAD. Used properly—when you inform people—it does make it easier to make recordings, or at least you don't have the noise in the background of the monitoring telephone?

Mr. EGER. Yes sir.

Mr. MOORHEAD. Does not that device also make it easier to monitor without the subject knowing he is being monitored?

Mr. EGER. Unquestionably it would, sir. Certainly it is easier than going to an extension telephone and cupping one's hand over the transmitter if one were desirous of monitoring that way.

Mr. MOORHEAD. That would be the purpose of the transmitter cutoff if it were to be used, as I say, without the subject knowing about it?

Mr. EGER. I think that is certainly one of the uses of the transmitter cutoff, Mr. Chairman.

Mr. MOORHEAD. If you found some department or agency having a disproportionately large number of these cutoff switches, would you think that that was a signal that would cause OTP or whoever else might have the responsibility to say "wait a minute," is that a signal that they may be using it for improper monitoring?

Mr. EGER. I don't know. We have no idea what other offices are using transmitter keys, push, talk, listening circuits for. Fortunately, through this committee we are gaining information about how other Government agencies are using them. That is one factor we will have to crank——

Mr. MOORHEAD. The one factor being a disproportionate number?

Mr. EGER. Whether it is a large number or not, I can't answer that question today.

Mr. MOORHEAD. We are going to have that particular department up here to testify. I think it will be very brief testimony. You might want to stick around.

Mr. EGER. I certainly will stay around this afternoon, and we will have coverage in these hearings as we have in the past, because we are very interested in the work the subcommittee is doing. It is very helpful to us.

Mr. MOORHEAD. I ask you because you are in the Office of Telecommunications Policy, you may have some technical information that can help us.

What is the KDZ instrument? Do you know that?

Mr. EGER. Mr. Chairman, I am a lawyer by training, not an engineer. I will have to ask Mr. Joyce if he knows what that refers to.

Mr. JOYCE. Mr. Chairman, I am an engineer by training, but I don't know what that refers to.

Mr. MOORHEAD. Well, I have a definition, "service observing equipment associated with a call director appears as a separate button on the telephone." Does that help us along?

Mr. JOYCE. No, sir. I heard the distinction between service observing and supervisory observing, but I am afraid I can't address that question.

Mr. MOORHEAD. Mr. Cornish?

Mr. CORNISH. Yes, thank you, Mr. Chairman.

Mr. Eger, I notice on page 1 you state the Office of Telecommunications Policy does not permit telephone monitoring without the consent of all parties to the conversation.

Mr. EGER. That is correct.

Mr. CORNISH. That goes beyond mere notification. What if someone said well, I don't want my telephone monitored. You just notified me that it is being monitored. What would you do in that case, halt the monitoring?

Mr. EGER. No, Mr. Cornish, it would never even get started. What I meant to convey is that if for some reason we wish the secretary to take notes, we would ask the other party on the line, do you mind if my secretary gets on to take notes? If the answer is no, obviously we do not have consent and therefore we do not monitor it.

Mr. CORNISH. You are using consent with the full implication and meaning of the word?

Mr. EGER. Yes, notification and authorization.

Mr. CORNISH. Would you suggest this be the practice throughout the entire U.S. Government where telephone monitoring is?

Mr. EGER. That is a question I can't answer at this time for other agencies. Again, we have only three cutoff keys. I didn't know how they were used. I didn't know my secretary had one until Friday. But I can't address that question because I don't know about other agencies and hopefully we will hear about how they use them and how valuable they are so we can apply balancing tests at some appropriate time.

Mr. CORNISH. Were you here this morning when I was discussing the taxpayers calling into IRS offices for tax information?

Mr. EGER. Yes, I was.

Mr. CORNISH. And that there were certain numbers of those calls monitored. Would you suggest that might be an instance where a person would be notified and also asked for his consent?

Mr. EGER. Professor Greenawalt addressed that, and again I haven't gotten into it in any great depth, but he suggested that perhaps there should be notification and the opportunity to be heard. You know, the twin peaks of fundamental due process ought somehow to be worked into this kind of monitoring, whether it is participant monitoring or consent of all the parties.

Mr. CORNISH. I think there are certain elements in your statement that are really excellent.

Thank you.

Mr. EGER. Thank you, Mr. Cornish.

Mr. MOORHEAD. Mr. Daniels?

Mr. DANIELS. No questions, Mr. Chairman.

Mr. MOORHEAD. Mr. Phillips?

Mr. PHILLIPS. Just a couple, Mr. Chairman.

Mr. Eger, as part of your overall responsibility in this area that you referred to earlier, was OTP consulted by the White House concerning the decision to tape record private conversations in the Oval Office?

Mr. EGER. Mr. Phillips, I can't speak to that question. I have only been with the office 4 months now, so I simply can't answer it. It may be that Mr. Joyce has personal knowledge of that.

Mr. JOYCE. I have no personal knowledge of OTP's being consulted. It certainly didn't come to me.

Mr. EGER. I should say, and I read some of the testimony of Mr. Whitehead and some of the fine questions posed to him during his first appearance here about what the functions and responsibilities of the Office of Telecommunications Policy are, that I think it is highly likely we would not have been asked, because we do not usually render ad hoc advisory opinions, nor operate or control any of the systems at all, and even though we are in the Executive Office of the President, the President's communications are governed and ordered by the White House communications agencies. I believe that is correct.

Mr. PHILLIPS. Could you check and see if someone in the agency who might have been there at the time this decision was made? I think it would have been either late in 1970 or early 1971. But this was asked in the context of the study that you had mentioned that had been commissioned, and also your comments about the whole question of privacy and the role which OTP is playing, an important role, in assuring a greater emphasis and awareness of this whole privacy problem as it affects Government agencies.

It would seem to me that certainly there would be an invasion of privacy of those individuals whose conversations in the oval office were taped without their knowledge or consent and this is certainly not the policy that you have been enunciating as it affects your agency and any other agency.

[A response to the above paragraph follows:]

OFFICE OF TELECOMMUNICATIONS POLICY,
EXECUTIVE OFFICE OF THE PRESIDENT,
Washington, D.C., June 17, 1974.

HON. WILLIAM S. MOORHEAD,
Chairman, Foreign Operations and Government Information Subcommittee, Committee on Government Operations, House of Representatives, Washington, D.C.

DEAR MR. CHAIRMAN: During our testimony on June 11, Mr. Phillips of your staff asked if OTP was involved in the decision to tape record conversations at the White House, and suggested that we submit a response for the record.

I have been able to verify that OTP was not consulted on that matter, and was unaware of the recording until it became public knowledge.

Sincerely,

JOHN M. EGER.

Mr. MOORHEAD. Do any other staff members have questions?

Mr. STETTNER. No, Mr. Chairman.

Mr. MOORHEAD. Well, thank you very much.

[Questions submitted in writing to the OTP and answers thereto follow:]

Question 1. What criteria have been furnished to the General Services Administration against which that agency might measure representations of other agencies that their "operational needs" require transmitter cutoffs, service observing equipment, and so forth?

Answer. OTP has not furnished to the General Services Administration any criteria regarding the use of transmitter cutoff switches or service observing equipment. OTP commissioned a study by Professor Kent Greenawalt of Columbia Law School on the legal protection of privacy. Professor Greenawalt describes participant monitoring as perhaps the most confused area, both legally and philosophically, in the whole field of privacy. OTP is going to do further investigation in this field and will in addition recommend to the Domestic Council Committee on Privacy that it examine the area.

Question 2. Does the Office of Telecommunications Policy assume that the General Services Administration has responsibility for and has developed criteria, of its own initiative?

Answer. The primary responsibility of the General Services Administration is to procure the goods and services needed by Government agencies on terms most advantageous to the Government. It is not the responsibility of the General Services Administration to determine requirements. While the General Services Administration should not conduct any procurement which violates Government policy, it is not the responsibility of GSA to develop such policy, at least in the telecommunications area. Notwithstanding this, GSA procurement regulations issued in 1968 state that the use of transmitter cutoff switches and other monitoring devices is not permitted. However, agency heads are permitted to exempt their agencies from this prohibition, and to delegate the authority for such exemption within their own agencies. This in effect leaves to the agencies the authority to determine whether such devices are required.

As stated in response to question one, OTP will consider whether there is a need for overall policy guidance in this field; and if so, which agency or agencies should provide the appropriate guidance.

Question 3. What is the nature of any limitation on the authority delegated by OTP to the General Services Administration to prescribe in the Federal Property Management Regulations operating practices relating to the monitoring of telephone conversations?

Answer. OTP has not delegated to GSA any authority relating to the specification of operating practices for telephone monitoring.

Question 4. Does the Office of Telecommunications Policy assume that agencies' requests to the General Services Administration for installation of such equipment would be questioned (i.e., critically challenged) beyond requiring that such requests be made in writing?

Answer. At present, if the agency heads or their delegates submit the required determinations, there is no basis for GSA to question agency requests for the installation of monitoring equipment. We understand that GSA requires that these determinations be made in writing.

Question 5. What agency (OTP or GSA) should be concerned with the matter of excessive numbers of such equipment and/or service being obtained, where agencies deal directly with operating telephone companies because in that location General Services Administration has not established a centralized switchboard operation?

Answer. At present, we assume that only GSA would be concerned whether, as required by its procurement regulations issued in 1971, the head of the procuring agency or his authorized designee had determined in writing that the monitoring device was essential to the effective execution of agency responsibilities or was required by operational needs, and the agency had retained this determination in its files.

Question 6. What are the views of the Office of Telecommunications Policy on the concept of "teleservice centers" and the widespread introduction of service monitoring equipment in these centers, in terms of their potential and actual invasion of privacy of those calling in?

Answer. Clearly, assuming that both notification and authorization are requisite in any participant monitoring situation, the problem of providing adequate notification is more vexing in the case of service monitoring than in most other forms of participant monitoring. OTP is examining the question of service monitoring in telephone service centers as part of its broader concern with participant monitoring.

Question 7. Does the Office of Telecommunications Policy support the decision by the Secretary of HEW to discontinue service monitoring at its teleservice centers and recommend similar action be taken by those other agencies operating numbers of similar teleservice centers?

Answer. The Office of Telecommunications Policy has not reviewed the use of service observing by HEW, nor the reasons for its discontinuance, and therefore has no comment on this action at this time.

Question 8. What reservations would OTP have recommending Government-wide adoption of its own policy that monitoring of telephone conversations not be permitted without the consent (i.e., notification and authorization) of all parties to the conversation rather than the mere notification, which is now the policy of many Federal agencies?

Answer. As we indicated in our testimony, transmitter cutoff devices are used only at the top executive levels in OTP, and then only with the consent of all parties to the conversation. Where transmitter cutoffs are used in other Federal agencies at the Executive level, we would assume that similar reasons for their use prevail, and that the application of the same policy might well be appropriate.

However, before recommending governmentwide adoption of this policy at all levels, we would want to be more familiar with other types of situations in which these devices are used and the justification therefor. It may turn out that some distinctions will have to be made between applications in which the consent of all parties should be obtained, and those where it is not in the public interest to do so.

Question 9. Summarize for the subcommittee those actions taken by OTP, in consonance with responsibilities and authorities set out in Executive Order 11556, dated September 4, 1970, as these relate to:

(*a*) Consultation with agencies to insure that their conduct of telecommunications activities is consistent with the policies and standards of the Director, OTP (section 1(b)).

(*b*) Coordinate the telecommunications activities of the executive branch and formulate policies and standards therefor, including . . . privacy . . . (section 1(e)).

(*c*) Conduct and coordinate economic, technical, and systems analyses of telecommunications policies, activities, and opportunities in support of assigned responsibilities (section 1(j)).

Answer. The attached programs and activities reports describe the broad range of OTP's activities. The activities which are most pertinent to the responsibilities listed in question No. 9 are summarized below.

In late 1972, OTP developed and promulgated a set of management procedures (OTP Circular No. 11), requiring all Federal Government agencies to submit their frequency plans to OTP well in advance, with the objective of insuring a critical review of frequency spectrum availability for Government communication-electronic systems prior to the commitment or expenditure of public funds. OTP's experience with the application of these procedures has confirmed emphatically that the procedures are appropriate and can meet the desired objectives.

In matters related to management of the Government's use of the radio frequency spectrum, OTP is assisted by Interdepartment Radio Advisory Committee (IRAC). The IRAC is composed of representatives of 16 Government agencies having major communication-electronic operations, plus a liaison representative from the Federal Communications Commission.

OTP also established in 1972, the Council of Government Communications Policy and Planning. This council, chaired by OTP's Director, currently includes policy level representatives from the Departments of State, Treasury, Defense, Justice, Commerce, and Transportation and from the General Services Administration, the National Aeronautics and Space Administration, and the Central Intelligence Agency. The Council provides a consultative forum for OTP and Federal departments and agencies with the most significant telecommunications system development and operational responsibilities.

In October 1973, OTP established a formal planning and coordination process (OTP Circular No. 12) called the Government communications planning program (GCPP) which was designed to achieve many of OTP's objectives through the day-to-day activities of the operating departments and agencies. The objectives of the Government communications planning program are: First, to identify all the communications activities and resources of the Federal Government; second, to determine the needs for effective information exchange among the various departments and agencies; third, to promote economy in the Government's use of communications, through sharing of facilities, elimination of duplication, and effective use of commercial services; and finally, to encourage the use of communications to improve productivity and enhance coordination of Federal Government activities.

In June of this year, OTP established guidelines (OTP Circular No. 13) designed to clarify the normal Federal role as a user, rather than a provider, of telecommunication service. The policy emphasizes the need to place maximum reliance on the private sector in providing telecommunications services to the Federal Government.

With respect to OTP's privacy-related efforts, it has been proposed recently to the Domestic Council's Committee on the Right of Privacy that OTP's GCPP be used to assure that personal privacy rights are given systematic consideration in the planning, coordination, and procurement of Federal data communications systems. This recommendation was developed by an interagency task force, chaired by OTP's Assistant Director for Government Communications. The need for such systematic review was demonstrated recently by the events relating to GSA's plans for FEDNET, which progressed undetected until just before release

of the formal request for proposals to industry. OTP analyzed the communications component of FEDNET and, after full consideration of various aspects including the economic and privacy implications, recommended a complete reorientation of that communications program. OTP continues to be concerned with FEDNET and is monitoring closely Federal procurement of telecommunications equipment associated with ADP operations to prevent other FEDNETS from advancing so far undetected.

Another privacy-related activity, discussed in our answer to question No. 1, is an OTP-commissioned study by Prof. Kent Greenawalt of Columbia Law School. OTP is presently studying his recommendations and we expect some of them to result in action by OTP, and some to result in further recommendations by OTP to the Domestic Council's Committee on the Right of Privacy.

Mr. MOORHEAD. We will take a brief recess for approximately 5 minutes while we go and vote, then we will call Mr. Gentile.

[A short recess was taken.]

Mr. MOORHEAD. The Subcommittee on Foreign Operations and Government Information will please come to order.

The subcommittee would now like to hear from Mr. Gentile of the Department of State. Would you come forward. Nice to see you again, sir.

STATEMENT OF G. MARVIN GENTILE, DIRECTOR OF SECURITY, DEPARTMENT OF STATE

Mr. GENTILE. Thank you, sir.

Mr. MOORHEAD. The subcommittee has received a letter from the Department of State, dated June 11, 1974, and signed by Assistant Secretary Linwood Holton, who is Assistant Secretary for Congressional Relations.

Without objection, this letter will be made a part of the record.

[The letter follows:]

DEPARTMENT OF STATE,
Washington, D.C., June 11, 1974.

Hon. WILLIAM S. MOORHEAD,
Chairman, Foreign Operations and Government Information Subcommittee of the Committee on Government Operations, House of Representatives, Washington, D.C.

DEAR MR. CHAIRMAN: The Secretary has asked me to reply to your letter of May 14 requesting the Department's experience and views on telephone monitoring practices.

The Department recognizes that occasionally there will be circumstances in which telephone monitoring may contribute to the more efficient conduct of official business. It, therefore, permits the practice, as long as it is held to a necessary minimum. Further, our written procedures require that the other party be apprised in advance that the conversation is being monitored and, if tape recorded, the beeper warning signal must be used as required by Federal Communications Commission regulations. I enclose a copy of the Department's most recent notice on this subject.

During fiscal year 1973 the Department had a total of 606 transmitter cutoff switches, including "push-to-talk" and listening-in circuits. The total costs involved amounted to $13,328.40. The Department also has four recording devices used to monitor certain calls in the Operations Center and, as required, the beeper is used to notify the other party the call is being recorded. Our experience has been that these procedures, especially in the Operations Center, are particularly useful when accurate reporting of details is paramount.

I hope this information will be helpful to the subcommittee in its consideration of these matters. If I can be of any further assistance, please let me know.

Cordially,

LINWOOD HOLTON,
Assistant Secretary for Congressional Relations.

Enclosure: As stated.

DEPARTMENT NOTICE TO KEY PERSONNEL, STATE, AID, ACDA, SEPTEMBER 23, 1970

MONITORING OF TELEPHONE CALLS

All employees should be periodically reminded that monitoring of telephone calls should be held to a minimum. When it is necessary to monitor telephone calls, the following practices will be observed:

a. Telephone conversations shall not be recorded by recording devices unless advance notice is given to the other party and the device is connected in accordance with the Federal Communications Commission regulations.

b. Advance notice must be given whenever a secretary or any other person is placed on the line for any purpose whatsoever.

Mr. MOORHEAD. Now, Mr. Gentile, do you want to say anything to us in amplification of that letter?

Mr. GENTILE. No, Mr. Chairman, I will just amplify the letter which I know is short.

Mr. MOORHEAD. The reason we asked you to come up here, as revealed by my comments to Mr. Eger, is we noticed the State Department has, for example, more than half of all the KDZ transmitter cutoff switches in the entire Government. Our information is that there are 614 throughout the Government, and of the 614, 427 are in the Department of State. This signals something. What is the meaning of that?

Mr. GENTILE. Well, I don't think those are all KDZs, are they, sir? I am lost in the definitions of all these various terms. This is the cutoff switch as I understand it?

Mr. MOORHEAD. Basically these are the buttons on the telephone that you press; we call it a monitoring button where a secretary can be on taking notes from the conversation her supervisor is having with whomever called in or whatever the supervisor called and these are extensive throughout the Department. Mr. Gentile, why would the State Department need such a disproportionately large number of these cutoff switches?

Mr. GENTILE. It may be a question of habit, sir. I notice in our 1970 presentation there were 835. We did a survey within the Department over 1 year ago.

Mr. MOORHEAD. When did you have 835?

Mr. GENTILE. This was lumping all these categories of cutoff switches that are used on phones.

We did a survey back about a year and a half ago to reduce this number, and as the letter from Mr. Abshire states, we have a count now of 606. So we still have a considerable number, Mr. Chairman. There is no question about it; these are used in the day-to-day business of many senior officers, as I said, basically to have the secretary be able to take down notes of commitments made. I think it is used in the work a lot of the officers are doing with the various embassies around town in handling the questions they have asked. The secretaries can write down commitments, appointments, and promises made. The secretaries can use this to record these commitments that come through in these conversations.

Mr. MOORHEAD. Also on the KDZ, which seems to be a service observing equipment, the same pattern emerges. There are 25 of these devices throughout Federal Government agencies in the Washington metropolitan area, and 21 of the 25 are in the State Department.

Mr. GENTILE. This is a term that is unfamiliar to me. I am really not sure of what this involves. I have a call in to the Department now trying to find out what it is. Earlier I checked after hearing the telephone

company's comments today on supervisory observing equipment, and the telephone man, the supervisor at the State Department for C. & P. Telephone, indicates to his knowledge there is no supervisory observing equipment in use at the State Department.

What the KDZ actually is I don't know. I have a question in my mind that it could be systems involved in the operations center in the Department. There are four big consoles in the operations center with a battery of telephone lines coming in, and they have a facility to shoot those out to 10 or 12 phones in areas we use to set up task forces on a kidnapping problem or a special problem involving a foreign-type catastrophe. This may be what this refers to. I am having a check made, and I will certainly furnish the committee, if we don't get it before the meeting is over, what that 21 consists of.

Mr. MOORHEAD. The same pattern emerges with the TCH or hand-operated transmitter cutoff switch. There are in Federal Government agencies in the Washington metropolitan area 273 of these, and 148 of the 247 are located in the State Department.

Mr. GENTILE. Again, I must say I have never seen a toggle switch or hand-operated cutoff switch. I would like to take those statistics and get them broken out, and get a more definitive answer to the committee, which I am sure we can do.

Mr. MOORHEAD. As I understand it, the transmitter cutoff, if it is not being used properly—that is, to monitor without letting the person know—that the advantage is that you don't hear noise of somebody else on the line so that secret monitoring is carried out much more readily.

Mr. GENTILE. Yes, unless the person who has the secretary doing this tells the person who called that the secretary is on, there is no way of knowing that person is on.

Mr. MOORHEAD. In our office, we often put somebody on the phone telling the people we are calling in, but we don't have any fancy switch to cut off her transmissions, and we don't have any trouble getting the notes taken.

The primary advantage of these cutoff switches is for secret monitoring, but you say you do not do that?

Mr. GENTILE. I think one of the problems we have is that most of the secretaries are in the outer offices where visitors are. Conversations are going on, and the senior officer who is having a conversation in the other room would be getting the background noises from the secretary's room. This would be embarrassing if you are talking to a foreign official and he hears all this background noise. He wouldn't know who else was in the same room at the same time.

Mr. MOORHEAD. Again, I am not talking to foreign officials. If you have somebody else on the phone, it is in an office with other people. Congressional offices are not noted for their quiet serenity. You have so many of these devices, it makes one wonder if you are living up to your directive attached to the letter, which incidentally, without objection, will be made a part of the record.

Mr. GENTILE. Yes, sir.

Mr. MOORHEAD. I don't know whether you are living up to that directive. The good Lord knows how many people there are in the State Department, that some are not living up to that directive, and these devices make secret monitoring much more feasible.

Mr. GENTILE. Certainly you are right, Mr. Chairman. There is no way you can do a survey to determine how many people are or are not abiding by our notice.

Mr. MOORHEAD. Thank you, Mr. Gentile.

Without objection, the tables to which I referred, the first being titled "Quantities of Various Types of Transmitter Cutoffs" and the second titled "Monitoring Practices and Devices Used by Federal Government Agencies," will be made a part of the record.

[The material follows:]

QUANTITY OF VARIOUS TYPES OF TRANSMITTER CUTOFF SWITCHES OBTAINED BY FEDERAL GOVERNMENT AGENCIES[1] FROM TELEPHONE COMPANIES IN THE METROPOLITAN WASHINGTON AREA

	KDZ	BS8	PT7	KDX	PL8	TCH	ATQ	Total
State, Department of	21			427		148		596
ACTION Agency	1							1
Agency for International Development				87		45		132
Civil Aeronautics Board				3				3
Agriculture				23		3		26
U.S. Court of Claims					1	1		2
Export-Import Bank				1		12		13
Farm Credit Administration						2		2
Federal Home Loan Bank Board						1		1
General Accounting Office						1		1
General Services Administration			1	2		5	5	13
HEW, Department of			26	12		9		47
U.S. Information Agency			3			3		3
Inter-American Development Bank						3		6
Interior, Department of			1			2		3
Interstate Commerce Commission						2		3
Justice, Department of			1	2		13		16
National Council on Indian Opportunity	1			1				1
National Labor Relations Board				5		12		17
National Security Council				3				3
Office of Economic Opportunity				10				10
Office of Management and Budget			2	17	1			20
Office of Telecommunications Policy			1	9	5	3		57
Overseas Private Investment Corporation			5					
Small Business Administration			3					
Transportation, Department of	1	2	10					
Total	25	74	614	6	273	5	997	

[1] Partial list of agencies in the area who procure this category of service on a monthly basis.

COMPUTER CODE

DEFINITIONS

KDZ—Service observing equipment associated with a call director appears as a separate button on the telephone.

BS8—Same as the KDZ with the addition of an amplifier.

PT7—Transmitter cut off switch located in the handle of the handset push to talk.

KDX—Transmitter cut off switch located in the receiver cradle of the telephone (switchhook) or button on telephone.

PL8—Same as PT7 except push to listen.

TCH—Hand operated transmitter cut off switch (toggle switch).

ATQ—Operator headset equipped with a transmitter cut off switch located in spring cord.

MONITORING PRACTICES AND DEVICES USED BY FEDERAL GOVERNMENT AGENCIES

Agency	Monitoring permitted		Transmitter cutoffs		Speaker phones		Listening in circuits	
	Incoming	Outgoing	Number	Annual operating costs	Number	Operating cost	Number	Annual operating cost
General Accounting Office	A–1	No	No					
Office of Management and Budget		Yes	Yes	4	$133.20			
National Security Council				F–1 14	87.60			
Central Intelligence Agency		Yes	Yes	309	9,549.00			
Office of Telecommunication Policy	A–1	No	No	3	90.00			
Office of Consumer Affairs	A–1	Yes	No					
Office for Drug Abuse Prevention	A–1, 2	Yes	Yes			(1)		
Agriculture	A–1	No	No					
Commerce	A–1, 2	No	No	1	3.00			
Department of Defense	A–1			16,102	85,012.40		1,878	$14,010.00
Health, Education, and Welfare	A–1, 2	No	No					
Housing and Urban Development	A–1	No	No					
Interior	A–1, 3	No	No				1	
Justice		Yes	Yes	(2)				
Labor	A–1	No	No					
State		Yes	Yes	606	1,110.75			
Transportation	A–1, 2, 3	No	No	248	1,323.86			
Treasury	A–1, 2	No	No	19	423.00			
Action				3	108.00			
Atomic Energy Commission	A–1, 2, 3	No	No	306	1,466.00			
Civil Aeronautics Board	A–1, 2	No	No			3	$270.00	
Cost of Living Council		No	No					
Environmental Protection Agency	A–1	No	No					
Export-Import Bank of the United States	A–1, 2	No	No					
Farm Credit Administration	A–1	No	No	13	39.00			
Federal Communications Commission	A–1	No	No	1	3.00			
Federal Deposit Insurance Corporation	A–1	No	No	4	7.20			
Federal Home Loan Bank Board	A–1	No	No	1	3.00			
Federal Maritime Commission	A–1, 2	No	No					
Federal Mediation and Conciliation Service	A–2	No	No					
Federal Power Commission	A–1, 2	No	No					
Federal Reserve System		No	No					
Federal Trade Commission	A–1, 2	No	No					
Foreign Claims Settlement Commission		Yes	Yes					
General Services Administration	A–1, 2	No	No	35	295.00			
Interstate Commerce Commission		No	No					
National Aeronautics and Space Administration	A–1	No	No				1	36.00
National Labor Relations Board	A–2	No	No	271	1,858.44			
National Mediation Board		No	No	(3)	(4)			
National Science Foundation		No	No					
Overseas Private Investment Corporation	A–2	No	No					
Renegotiation Board	A–1	No	No					
Securities and Exchange Commission	A–1	No	No					
Small Business Administration	A–1, 2	No	No	10	120.00			
U.S. Arms Control and Disarmament	A–1	No	No					
U.S. Civil Service Commission		No	Yes	5		(1)		
U.S. Information Agency	A–1, 2	No	No	32	592.00			
U.S. Postal Service		Yes	Yes					
U.S. Tariff Commission	A–1, 2	No	No	44	147.00			
Other	A–1, 2	Yes	Yes					
Veterans' Administration		No	No					
Grand total		Yes	Yes	623	6,981.00			
				18,654	109,852.45	3[4]	270.00	1,880	14,046.00

See footnotes at end of following table.

MONITORING PRACTICES AND DEVICES USED BY FEDERAL GOVERNMENT AGENCIES—Continued

Agency	Recorders: Number: Wired circuit	Recorders: Number: Induction	Recorders: Other types	Recorders: Beeper equipped	Recorders: Acquisition cost	Recorders: Annual operating cost	Telephone service observing devices: Number	Telephone service observing devices: Cost	Nontelephonic bugging devices: Number	Nontelephonic bugging devices: Cost	Monitoring controlled by regulation	
General Accounting Office											Yes	Prohibitive.
Office of Management and Budget											Yes	
National Security Council												
Central Intelligence Agency	8			2	$2,240.00				[1]	$10,800.00	Yes	Do.
Office of Telecommunication Policy											No	
Office of Consumer Affairs											No	
Office for Drug Abuse Prevention											No	
Agriculture											Yes	Do.
Commerce	2			2	1,200.00	$7.00					Yes	Do.
Department of Defense	1,351	29	222	294	2,367,757.00			$145,774.80		216,252.00	Yes	Do.
Health, Education, and Welfare							[5] D–1				Yes	Do.
Housing and Urban Development											Yes	Do.
Interior	B–6 14	12		10	92,000.00						Yes	
Justice	[6]			Yes	[7]	7,200.00					Yes	
Labor	1			1	8,446.00						No	
State	B–5 88	2		75	217,904.04						Yes	Do.
Transportation	B–7 49	263			600,570.00		[1]		[1]		Yes	Do.
Treasury	B–1 3			3	1,700.00						Yes	Prohibitive with exceptions.
ACTION											No	
Atomic Energy Commission	180	34		60	17,076.00	914.00					Yes	Prohibitive.
Civil Aeronautics Board	1	24		1	5,653.00						Yes	Do.
Cost of Living Council											No	
Environmental Protection Agency											No	
Export-Import Bank of United States											Yes	Do.
Farm Credit Administration											Yes	Do.
Federal Communications Commission	1			1	116.90	66.00					Yes	
Federal Deposit Insurance Corporation		4			350.00						Yes	Do.
Federal Home Loan Bank Board											No	
Federal Maritime Commission											Yes	Do.
Federal Mediation and Conciliation Service	B–2										No	
Federal Power Commission											Yes	Do.
Federal Reserve System	B–4 22		C–1	Yes	62,662.00	1,379.00					Yes	
Federal Trade Commission											Yes	
Foreign Claims Settlement Commission											No	Do.
General Services Administration							D–1 [1]	14,876.40			Yes	
Interstate Commerce Commission											No	
National Aeronautics and Space Administration	11			11	[8] 2,000.00				E–1 [9]		Yes	Do.
National Labor Relations Board											Yes	Do.
National Mediation Board											No	
National Science Foundation											No	
Overseas Private Investment Corporation											Yes	Do.
Renegotiation Board											No	
Securities and Exchange Commission											Yes	Do.
Small Business Administration											Yes	Do.
U.S. Arms Control and Disarmament											Yes	Do.
U.S. Civil Service Commission											Yes	
U.S. Information Agency											Yes	Do.
U.S. Postal Service	B–3 23				804.00						Yes	Do.
U.S. Tariff Commission	B–1 2			23	953.00	42.00					Yes	Do.
Other	84	323									Yes	Do.
Veterans' Administration		31									Yes	Do.
Grand total	1,840	722	222	732	3,432,252.04	9,068.00	D–2	843.80			Yes	Do.
				249	50,865.10			161,495.00		227,052.00		

[1] Various.
[2] Limited number.
[3] A few.
[4] Less than $500.
[5] Automated call distributor.
[6] Some electronic secretaries.
[7] Leased.
[8] Approximately.
[9] Countermeasure kit.

NOTES

Col. A. Monitoring permitted: A–1. Secretary may, with knowledge of parties to conversation, take notes of pertinent information; A–2. Secretary may make a verbatim record of conversation with knowledge and permission of parties to conversation; A–3. Exception is made to prohibition of telephone monitoring in emergency situations such as disaster reports, nuclear accidents, bomb threats, power dispatching, search and rescue, air and maritime safety and similar instances.

Col. B. Recorders—wired circuit—induction: B–1. Code-a-Phone; B–2. Code-a-Phone excluded; B–3. Connected through recorder couplers; B–4. 20 are wired into telephone circuit; status of 2 devices is not identified; B–5. Includes 78 wired into telephone circuits and 10 identified as "other types"; B–6. Includes one Code-a-Phone, 10 recorders, and 3 multichannel devices; B–7. Includes 41 Code-a-Phones; B–8. Telephone recording devices in use in component.

Col. C. Recorders—beeper equipped: C–1. All equipped with beeper or other warning device except those used for bomb warnings in Chicago office.

Col. D. Telephone service—observing devices: D–1. Telephone contact with public at teleservice centers can be monitored from supervisor's console for quality control; D–2. Silent monitors are used at Department of Veterans' Benefits for quality control.

Col. E. Nontelephonic bugging devices: E–1. Agency uses certain countermeasure kits to safeguard against secret monitoring of NASA communications.

Col. F. F–1. Includes 12 TCH monitoring buttons and two KDX transmitter cutoff keys; G–1. Department of Defense, for purposes of this report includes the following agencies:

1. Department of the Army.
2. Department of the Navy.
3. Marine Corps.
4. Department of the Air Force.
5. Defense Investigative Service.
6. Defense Communications Agency.
7. National Security Agency.
8. Defense Intelligence Agency.
9. Chairman, Joint Chiefs of Staff.
10. Defense Telephone Service.

Note: (a) The Department of the Navy advised that a breakout cannot be made as requested in areas; (b) The Department of the Air Force and the Department of the Army reported wired circuit recorders for the National Capital area only.

87-787—74—14

Mr. MOORHEAD. Mr. Cornish?

Mr. CORNISH. Thank you, Mr. Chairman.

Mr. Gentile, in your statement to the subcommittee you say that your written procedures require that the other party be apprised in advance that the conversation is being monitored and then it continues; is that mere notification or does that also require consent?

Mr. GENTILE. Well, it doesn't obviously by its statement require consent, but I am sure that if I had a secretary on the line and I told someone who was calling I would like to have my secretary on the line and he said I would like to talk to you alone, I would not have her on. That would be the only way you could do it.

Mr. CORNISH. That would be a matter of judgment within the Department where a request for confidentiality would be granted?

Mr. GENTILE. Yes.

Mr. CORNISH. I wonder if I might yield to Mr. Stettner.

Mr. MOORHEAD. Certainly.

Mr. Stettner?

Mr. STETTNER. Mr. Gentile, the policy statement that was attached to the letter that you presented to the subcommittee today speaks of holding monitoring of telephone calls to a minimum. What type of guidance does this constitute? OTP prohibits it, without consent. You recommend holding it to a minimum and merely advise people rather than obtaining their consent.

Mr. GENTILE. Well, I think the intent here is that you don't have your secretary on the line all the time so that it reaches a point of where every time someone calls you say, "I have got my secretary on the line, I have got my secretary on the line." In other words, confine it to those times when you need to use her to have information taken down.

Mr. STETTNER. When information is transcribed by a secretary, is it a policy to furnish the individual whose conversations are recorded a copy, some kind of authenticated copy, so that that individual has as much information as the receiver of the telephone call?

Mr. GENTILE. I have no knowledge where copies were ever handed out to persons who have called in.

In my experience the secretary is not taking down verbatim the whole conversation. I could see in a very unusual situation or in a very delicate matter if you wanted it word for word, you could do it. But the normal thing is to have the secretary on to take whatever notes are needed for followup by the supervisor. I know of no case where they are putting out a verbatim piece of paper after every one of the calls.

Mr. STETTNER. Even if it is restricted to minimum-essential type data, would it not be of equal interest to the party calling what the specifics of an arrangement were as it is to the individual who is receiving the telephone call?

Mr. GENTILE. Well, I am sure if he told the other party that the girl was on and was going to take down that if he asked for a copy he would get it. In the event he didn't ask for a copy, none would be furnished.

Mr. STETTNER. I think you were here when Mr. Watts explained what a normal circumstance might be for the use of a transmitter cutoff or listening device. Is it reasonable to assume most of those in

the State Department don't meet the criteria of boiler room, machine room, or industrial operation?

Mr. GENTILE. I didn't hear his testimony on that point. But I would certainly agree with that. Most of the offices have noises, two or three girls typing, servicing senior offices and some of the offices are fairly busy with two or three conversations going on in them. It certainly isn't a boiler room type atmosphere; no, sir.

Mr. STETTNER. Earlier you stated there might be some such devices in the operations center, and in your submission to the subcommittee you reported eight-track multiple-station recorders located in the operations center. What is the principal application or use of this eight-track multiple-station recorder?

Mr. GENTILE. It is very seldom used. There is a beeper system on it and it consists of actually seven telephone circuits and one they call a time circuit where they relate time to a call. The main purpose of having this is for such things as when senior officials are traveling overseas, as an example, and they have some requirements back at State. They call in and have a long list of various things they would like to have done, people notified, and calls made. This can be recorded for accuracy.

If you had a situation involving a kidnapping where the details are very important to get, or someone asking for asylum, they have the ability to put on the recorder, and as I say, the recorder has a beeper. They will tell the person they would like to record the conversation and would they have any objection. This is a standard instruction. Not only the beeper, but they also ask the person for their permission to record it.

Mr. STETTNER. Is all the monitoring—the recording—in the Department done at the operations center?

Mr. GENTILE. This is the only monitoring that I know of.

Mr. STETTNER. Is that the full responsibility of the operations center?

Mr. GENTILE. No; it is a 24-hour nerve center of the Department, where the FBI, CIA, all the other Government agencies come in, they are the eyes and ears at night, they are the ones who call the responsible departmental officer. It is really the office that keeps the Department going 24 hours a day.

Mr. STETTNER. Is it a limited access area?

Mr. GENTILE. Yes; it is a limited access area.

Mr. STETTNER. And yet it routinely handles requests of people overseas?

Mr. GENTILE. Not routine. This would be in connection with the Secretary's travels overseas, problems that he would want handled back in the States.

Mr. STETTNER. That is the last of the questions I have.

Mr. MOORHEAD. Mr. Daniels?

Mr. DANIELS. No questions.

Mr. MOORHEAD. Mr. Phillips.

Mr. PHILLIPS. Thank you, Mr. Chairman.

How long have you been at the State Department, Mr. Gentile?

Mr. GENTILE. Ten years, Mr. Phillips.

Mr. PHILLIPS. Is all that service in the present position?

Mr. GENTILE. Yes, sir.

Mr. PHILLIPS. Do you have any personal knowledge of any case where electronic surveillance was conducted of State Department employees, either in their office or at home, their home phones?

Mr. GENTILE. I have absolutely none in my 10 years there. I am not aware of any electronic or telephonic surveillance of any State Department employee.

Mr. PHILLIPS. Are you aware of the Otepka case?

Mr. GENTILE. That is why I went there.

Mr. PHILLIPS. That was after the deluge?

Mr. GENTILE. Yes, sir.

Mr. PHILLIPS. One more question. Are the transmitter cutoff devices that we discussed earlier used in your Congressional Relations Office as well as other offices of State?

Mr. GENTILE. I can't say for sure, but I do know that Mr. Holton has one. I would want to check to make sure but I do believe Mr. Holton has one in his office.

Mr. PHILLIPS. The reason I ask, in all the conversations we had with that office, no one has ever said "my secretary is on the phone, do you mind?"

Mr. GENTILE. I can assure you after these discussions the matter will be clarified quickly.

Mr. MOORHEAD. Thank you very much, Mr. Gentile.

[Questions submitted in writing to the Department of State and the answers follows:]

QUESTIONS FOR THE STATE DEPARTMENT

Question 1. How many of the transmiter cutoffs, listening-in circuits, et cetera, are on instruments in industrial-type environments such as boiler rooms, foundries, et cetera, for which they are basically intended?

Answer: None.

Question 2. How many of such devices are in normal administrative and executive office situations, where ambient noises normally are not a problem?

Answer. This would be impossible to determine without a physical check being made of each office wherein a monitor button is located. These devices are generally in offices where there is noise from typewriters and normal office conversation.

Question 3. For how many and for which of the 606 reported transmitter cutoffs, listening-in circuits, and service observing equipment were justifications of need made since July 9, 1972?

Answer. A recheck of Department of State records revealed that the figure of 606 transmitter cutoffs, listening-in circuits and service observing equipment is not a current valid figure. For example, a physical check was made of the 21 KDZ service observing equipment reported by the General Services Administration (GSA) and it was determined that only one KDZ is in operation in the Department of State and that one is being used in the same manner as a KDX. State Department records do not contain individual letters of justification of need on this equipment.

Question 4. The Department of State reported that it does not use service observing equipment of any kind. The information furnished to the subcommittee indicates that the Department does have 21 such items which generally are associated with a call director and are characterized by a control button on the telephone instrument. The telephone company codes these as KDZ service observing equipment. Who approved the installation of those 21 equipment items: when; and what is their present use? Identify the organizational element and position of the individual who is normally assigned to the work position where these KDZ equipment items are (or were) installed.

Answer. As a result of the testimony of Mr. G. Marvin Gentile, Department of State, on June 11, 1974, a physical check was made of the 21 Department of State telephone lines reported by the GSA as having KDZ equipment on them.

It was determined that one suite of offices in the Department has five call directors equipped with "monitoring capability." Four call directors are equipped with KDX and one with a KDZ circuit. Four call directors are used by secretaries and the fifth one is used by a staff assistant to an Assistant Secretary of State. Any one of the five call directors can monitor calls on the telephone lines coming into that office. It was ascertained that this is the only telephone extension in the Department of State which is equipped with a KDZ circuit.

As a result of this survey concerning the use of the KDZ in the State Department building, the C. & P. Telephone Co. has been requested to conduct an up-to-date survey to determine exactly how many monitoring devices are actually in use at the present time. It is anticipated this survey will be completed in 30 days. Once this survey is completed the Department of State will closely scrutinize the justification for continuance of any monitoring devices reported to be in operation.

Question 5. What are the full responsibilities assigned to the Operations Center; to what division does it report?

Answer. The State Department Operations Center is an around-the-clock alerting and crisis management center. The Operations Center's major responsibility is the channeling of information related to foreign affairs from a variety of sources to the Secretary of State and his principal deputies. The Center insures that they are alerted to and briefed on fast-breaking developments and assists in the coordination of communications support during their travels.

A second major responsibility is to alert State Department officers, the White House, and agencies and departments concerned with foreign affairs to situations requiring immediate action. The Operations Center assists in coordinating and following up on the action taken.

The Operations Center assists in the establishment of task forces or special working groups assigned to deal with a specific foreign affairs problem. Task forces and working groups are located in the Operations Center's task force area. The Operations Center prepares a daily summary of significant reports for the Secretary of State and his principal deputies and is responsible for the distribution of telegrams and various other reports to the principal officers in the Department.

The Operations Center is one of four constituent offices of the Department of State Executive Secretariat which is headed by an executive secretary. Within the Secretariat, the Operations Center is supervised by a director who reports, in the chain of command, to the executive secretary through the deputy executive secretary.

Question 6. Does the State Department have in its files, or has it filed with the General Services Administration, those written justification-of-need statements, required under FPMR Regulations 101–35.307–2 for the "installation of listening-in circuits, transmitter cutoff switches, and other devices for recording and listening to telephone conversations"?

Answer. Several years ago, verbal authority was given to the Department of State by the then Commissioner of Telecommunications, General Services Administration, for the Department to control its own telephone equipment installation requirements. The Department at that time had its own switchboard and frame rooms. Requests for equipment justified by the individual bureaus was installed. Written justifications were not submitted to GSA.

Mr. MOORHEAD. The subcommittee stands adjourned.

[Whereupon, at 2:55 p.m., the subcommittee adjourned, to reconvene, subject to the call of the chair.]

TELEPHONE MONITORING PRACTICES BY FEDERAL AGENCIES

THURSDAY, JUNE 13, 1974

HOUSE OF REPRESENTATIVES,
FOREIGN OPERATIONS AND
GOVERNMENT INFORMATION SUBCOMMITTEE
OF THE COMMITTEE ON GOVERNMENT OPERATIONS,
Washington, D.C.

The subcommittee met, pursuant to notice, at 10:05 a.m., in room 2203, Rayburn House Office Building, Hon. William S. Moorhead (chairman of the subcommittee) presiding.

Present: Representatives William S. Moorhead, Bill Alexander, John N. Erlenborn, and Gilbert Gude.

Also present: William G. Phillips, staff director; Norman G. Cornish, deputy staff director; L. James Kronfeld, counsel; and Stephen M. Daniels, minority professional staff, Committee on Government Operations.

Mr. MOORHEAD. The Subcommittee on Foreign Operations and Government Information will please come to order.

Today's public hearing by the House Foreign Operations and Government Information Subcommittee is a continuation of our investigations into telephone monitoring practices by the Federal Government.

This inquiry stems from the deep concern of the Congress over the problems of invasion of privacy as they affect ordinary law-abiding American citizens.

The subcommittee is primarily studying the monitoring of telephones in the day-to-day business of the Government.

As I stated at our last hearing on Tuesday, we firmly believe that when a citizen of the United States contacts a Federal agency by telephone, that citizen should know whether his call is being monitored or recorded, and if so, why. This should never be done without his knowledge and consent in my view.

For my tax dollar and those of millions of other American citizens, there are too many potential "Big Brothers" listening in. As Congressman Alexander of Arkansas put it the other day, Americans simply do not want to be part of one big government "party line." They want to talk to real people about their very human and personal problems—not an institution. These real people are called "public servants." I can assure you they do not like telephone monitoring either despite its alleged good intentions.

Today we will hear the testimony of spokesmen for several Federal agencies. Hopefully we will learn that there is going to be a massive

reduction in telephone monitoring by Federal agencies. Americans have a right to privacy. They deserve it. And they are going to get it.

The subcommittee would like to hear first from Mr. Warren E. Burton, Deputy Commissioner, Automated Data and Telecommunications Service of the General Services Administration. He will be accompanied by Mr. Leonard Plotkin, Deputy Assistant Commissioner and Ms. Allie Latimer, Assistant General Counsel.

We are pleased to have you with us, and in accordance with our proceedings, at the appropriate time we will administer the oath retroactively and prospectively.

Mr. Burton, you may proceed, sir.

STATEMENT OF WARREN E. BURTON, DEPUTY COMMISSIONER, AUTOMATED DATA AND TELECOMMUNICATIONS SERVICE, GENERAL SERVICES ADMINISTRATION; ACCOMPANIED BY ALLIE LATIMER, ASSISTANT GENERAL COUNSEL; AND LEONARD PLOTKIN, DEPUTY ASSISTANT COMMISSIONER

Mr. BURTON. Mr. Chairman and members of the subcommittee, I am Warren E. Burton, Deputy Commissioner for the Automated Data and Telecommunications Service of the General Services Administration. I am accompanied by Ms. Allie Latimer, Assistant General Counsel for the Automated Data and Telecommunications Service, and Mr. Leonard Plotkin, Deputy Assistant Commissioner for Telecommunications Operations Division.

We are pleased to have this opportunity to appear before your subcommittee on behalf of the Honorable Arthur F. Sampson, Administrator of General Services. My appearance is at the request of Chairman Moorhead to the Administrator to discuss the current technology of monitoring equipment and the nature of the use of such equipment by the General Services Administration. You also requested that we expand on and update, if necessary, the material previously furnished to the General Accounting Office in response to an October 5, 1973, questionnaire on monitoring practices and devices.

At the outset, I would like to explain that pursuant to the authority of the Federal Property and Administrative Services Act of 1949, as amended, the General Services Administration (GSA) is responsible for the operation and management of the Federal Telecommunication System (FTS). The telephone portion of this system is composed of some one million telephones and approximatetly 250 switchboards located throughout the United States which serve both the intragovernmental community and contacts with the public. In addition to calls between agencies, a large number of calls are received at our FTS switchboard from the general public in order for them to transact their business with the Government.

GSA's Government-wide policy with respect to the installation of monitoring and listening-in devices is outlined in our Federal Property Management Regulations, FPMR–101–35.308.9f, which states that the "installation of listening-in circuits, transmitter cut-off switches, and other devices for recording and listening to telephone conversations is prohibited."

However, our FPMR Regulation 101–35.307–2 does permit the deviation from the above regulation when the head of an agency or his

authorized designee determines, in writing, that the deviation is essential to the effective execution of agency responsibilities, or is required by operational needs. Orders for such telephone equipment to be utilized and installed on GSA-operated facilities are placed with GSA and are required to be accompanied by a copy of such written determinations. When orders for such equipment are on agency-operated telephone facilities, they are placed directly with the local telephone company and the written agency determinations are to be retained in their files.

The General Services Administration has received requests for deviation from our FPMR to permit installation of listening-in devices for the Department of the Treasury (IRS), Department of Health, Education, and Welfare (SSA), and the Veterans' Administration (VA). These deviations were requested for service observation equipment located principally in IRS Taxpayer Service Program Centers (TSP), Teleservice Centers operated by the Social Security Administration, and a VA Regional Office Contact Center located in Phoenix, Ariz. GSA's approval of these deviations was contingent upon the following:

1. No recording devices were to be associated with the monitoring equipment.

2. All agency employees answering the calls were to be made aware of the fact that their conversations may be monitored.

3. The monitoring feature was to be used only for training purposes and to maintain a high degree of quality in the service programs of and agency.

We have been informed that the DHEW has issued instructions to suspend the use of the service observation features in their Teleservice Centers. We understand this action took place in March of 1974 and that your subcommittee was advised on May 15, 1974, that this latest action was a result of your recent request that DHEW review the exceptions previously granted SSA in this area.

GSA's internal policy implementing the above FPMR's is incorporated in our Policy Manual ADM P 1000.2B, chapter 2, and the Internal Telecommunications Handbook, OAD P 2100.1, chapter 2. The pertinent extracts from these publications are submitted for the record. In addition to the above internal regulations, GSA has issued in its Telephone Operations Handbook, TCS P 7140.1A, the necessary operating instructions to our FTS telephone operators for maintaining the secrecy and privacy of all telephone conversations. The pertinent operating instructions referred to above are all submitted for the record.

Mr. MOORHEAD. Without objection, the various attachments will be made a part of the record.

[The material referred to above follows:]

GSA POLICY MANUAL, GENERAL SERVICES ADMINISTRATION, WASHINGTON, D.C.

(ADM P 1000.2B, Feb. 27, 1973)

90. *Telecommunications.*

a. *Basic policy.* Provisions will be made, through the Federal Telecommunications System, for the economical acquisition and efficient utilization of the telecommunications facilities and services needed internally by GSA in carrying out its assigned responsibilities.

b. *Operating policy.*

(1) Telecommunications services used by GSA will conform with the Government-wide standards prescribed by the automated data and telecommunications service.

(2) Telephone conversations will not be monitored by a recording device, secretary, or other person not party to the conversation for the purpose of taking a verbatim transcript of the conversation, in whole or in part.

c. *Wink-hold.* The use of "wink-hold" illumination is prohibited, where any additional costs are involved, unless special requirements justify the additional cost.

d. *Hold buttons.* Hold buttons should be installed only where there is a valid need. They should not automatically be provided on all key system instruments that have more than one line.

e. *Automatic answering devices.* These may be installed only when there is a valid need to leave a message on unattended telephones, such as in emergency control centers, the offices of PBS area or buildings managers, ADTS record communication centers and interagency ADP coordinators, and the FSS interagency motor pools. Each proposed installation must be approved by the Head of the Central Office Service or Staff Office or the Regional Administrator.

f. *Recording and listening devices.* Installation of listening-in circuits, transmitting cutoff switches, and other devices for recording and listening to telephone conversations is prohibited. (See par. 13 for instructions pertaining to the stenographic monitoring of telephone calls.)

g. *Color telephones.* Color telephones may be installed only where required to identify emergency or security telephone lines or where instruments may be installed without an additional charge.

h. *Essential residence telephone service in time of emergency.* A special service provided by telephone companies, at no increase in rates, enables subscribers having essential emergency functions to place calls from their residences with minimum delay. Instructions on developing and certifying a listing of key GSA personnel requiring such undelayed service are provided in ADM 7140.1.

i. *Review of charges.* Whenever any special type of installation is planned, a review is to be made of aggregate charges for items making up the total cost of the installation and shall be compared with the actual need for each item. While some special items are relatively inexpensive, they require additional features and equipment to operate so that aggregate charges are relatively large.

9 through 11. *Reserved.*

GSA Internal Telecommunications Management

(OAD P 7100.1, Oct. 28, 1969)

Part 3. Use of Telephone Services

Section 1. General

12. *Personal use*

(*a*) Official telephones may be used for personal calls only in extreme emergencies.

(*b*) Supervisors, including those on night shifts, shall take appropriate action to insure that local personal calls are placed only in the event of an emergency. All employees should discourage friends, relatives, and associates from calling them during office hours.

(*c*) Under no circumstances should personal calls be placed over the FTS intercity network.

13. *Stenographic monitoring of telephone calls.*—As provided in the GSA policy Manual, 2–90b(2), except with the prior consent of the other persons or persons, and subject to the existence of a real need, telephone conversations will not be monitored by a recording device, secretary, or other person not party to the conversation, for the purpose of taking a verbatim transcript of the conversation, in whole or in part.

14. *Reduction in use during emergency conditions.*—To minimize possible disruptions to the orderly processes of Government and to insure that outgoing calls can be made during an emergency by those officials responsible for resolving problems arising therefrom, it is imperative that each employee forego or drastically limit his use of the telephone during such emergency. When an

essential call must be made during an emergency, the caller should strive for the utmost brevity in completing the conversation. Also during an emergency, official business unrelated to the emergency which would normally be conducted by telephone should be delayed, where possible, until demands on telephone facilities have subsided or should be conducted by alternative means of communication.

15 through 17. *Reserved.*

Telephone Operations

(TCS P 7140.1A, Feb. 24, 1971)

Chapter 1. Introduction

1. *Purpose.*—This handbook prescribes standards and operating procedures governing the operation of Federal Government telephone switchboards.

2. *Applicability.*—The provisions of this handbook apply to all Federal Telecommunications System (FTS) switchboards nationwide, both those operated by the General Service Administration and those operated by other agencies under special arrangement with GSA.

3. *Telephone Operating Notices.*—New operating procedures, or changes in existing procedures, will be promulgated initially by telephone operating notices (TPON's) issued by the Office of Telecommunications Operations. TPON's are numbered consecutively during each calendar year, for example, 1–70, 2–70, 3–70, et cetera. Copies will be filed at each FTS switchboard and reviewed periodically. Instructions contained in TPON's will be a part of the indoctrination of all new telephone operators in conjunction with this handbook. When a change to the telephone operations handbook is issued containing a new or changed procedure promulgated by a TPON, that TPON will be canceled and destroyed.

4. *Secrecy of communications.*—Exact secrecy of communications is protected by law and must be maintained. Federal law subjects any offender to fine and imprisonment. Sections 605 and 501 of the Federal Communications Act of 1934, as amended, shall be conspicuously posted in each switchboard room and reviewed by all operators periodically. Although these sections of the act apply to all Federal personnel, they are particularly applicable to communications personnel. Texts of sections 605 and 501, together with an interpretation of the language as it applies to telephone operators, are shown in figure 1–4 and figure 1–4.1.

5. *Physical security of communications areas.*—Keep the doors locked for your own safety and protection. Each person must be sure that doors are locked after entering or leaving a communications area. Keep shades or venetian blinds drawn, to prevent identification of communications activity and equipment, where required. Inquiries as to the location of the telephone facilities should be referred to the supervisor. Unauthorized personnel are not permitted in communications areas. No deviations from these procedures are authorized.

"Sec. 605. No person receiving or assisting in receiving, or transmitting or assisting in transmitting, any interstate or foreign communication by wire or radio shall divulge or publish the existence, contents, substance, purport, effect, or meaning thereof, except through authorized channels of transmission or reception, to any person other than the addressee, his agency, or attorney, or to a person employed or authorized to forward such communication to its destination, or to proper accounting or distributing officers of the various communicating centers over which the communication may be passed, or to the master of a ship under whom he is serving, or in response to a subpena issued by a court of competent jurisdiction, or on demand of other lawful authority; and no person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communications to any person; and no person not being entitled thereto shall receive or assist in receiving any interstate or foreign communication by wire or radio and use the same or any information therein contained for his own benefit or for the benefit of another not entitled thereto; and no person having received such intercepted communication or having become acquainted with the contents, substance, purport, effect, or meaning of the same or any part thereof, knowing that such information was so obtained, shall divulge or publish the existence, contents, substance, purport, effect, or meaning of the same or any part thereof, or use the same or any information therein contained for his own benefit or for the benefit of another not entitled thereto: *Provided*, That this section shall not apply to the receiving, divulging, publishing, or utilizing the

contents of any radio communication broadcast, or transmitted by amateurs or others for the use of the general public, or relating to ships in distress."

"Sec. 501. Any person who willfully and knowingly does or causes or suffers to be done any act, matter, or thing, in this act prohibited or declared to be unlawful, or who willfully and knowingly omits or fails to do any act, matter, or thing in this act required to be done, or willfully and knowingly causes or suffers such omission or failure, shall, upon conviction thereof, be punished for such offense, for which no penalty (other than a forfeiture) is provided in this act, by a fine of not more than $10,000 or by imprisonment for a term not exceeding 1 year, or both, except that any person, having been once convicted of an offense punishable under this section, who is subsequently convicted of violating any provision of this act punishable under this section, shall be punished by a fine of not more than $10,000 or by imprisonment for a term not exceeding 2 years, or both."

SECRECY OF TELEPHONE COMMUNICATIONS

Your competence, efficiency, and integrity have substantially enhanced the reputation of the FTS voice network. You must go one important step further and understand that privacy is most essential to the communications we furnish. Some examples of your obligations to assure secrecy of communications are:

You must not listen in to any call or any portion of a call except as required for the proper handling of the call.

Not only should you never repeat any part of a communication but even the fact that there has been a call from one telephone to another is not to be divulged. What might seem to you to be an innocent remark, about one person calling another, could cause problems.

You must never use any information regarding any call for your own benefit or for the benefit of any other person.

You must never permit any person, other than the parties to the call, to hear, record, or otherwise intercept any call, except as required for proper handling of the call.

Any requests for information regarding the location of any equipment, including trunks, circuits or cables, or regarding records of calls, except as required in the operation of the switchboard, must be referred to your supervisor.

You must not permit anyone to tamper with communications facilities of the Government or to have unauthorized access to Government communications premises.

You must not discuss any communications arrangements provided for our users, except as required in the operation of the switchboard or as specifically authorized by the user.

Even if you are presented with a court order from a law enforcement agent authorizing interception and/or information concerning telephone lines or equipment, do not divulge any information. All such inquiries and requests must be handled by the supervisor. The supervisor will immediately call the regional office for guidance.

Mr. BURTON. Thank you, Mr. Chairman.

As reported to the General Accounting Office on November 14, 1973, we listed 271 transmitter cut-off switches in use on internal telephones assigned to GSA, in addition to service observation equipment located at a number of GSA switchboards and at the Federal Information Center in Washington, D.C. This information was obtained from our telephone inventories which listed the devices as cut-off keys. A recent physical inventory by our regional telecommunications personnel indicates that of these 271 devices, only 11 are actually transmitter cut-offs, 38 are amplified receiving telephones for people with impaired hearing, and the balance which includes line exclusion controls and confidencers.

A line exclusion device is designed to provide privacy when calling by cutting off predetermined telephone lines. A confidencer is a special transmitter mouthpiece added to the telephones located in noisy areas. None of these categories are monitoring or listening-in devices. The previously reported information indicated there were 10 press-to-talk

headsets, 9 of which were located in noisy elevator penthouses, and one in a steamplant. The 11th was installed at the LBJ Library and was disconnected on May 8, 1974.

GSA has 17 FTS switchboards which are equipped with service observation equipment. This type of equipment is used by the telephone industry and has been in use on the FTS for many years. There are various physical configurations of this equipment. However, all perform the same fundamental function. The service observer, from a control position, can be connected with the FTS telephone operator on any selected switchboard position. This permits the observer to listen to the telephone operators' handling of all calls on the selected position. These calls fall into two general categories, information and assistance. The observer, just as the operator, can hear only the exchange between the FTS operator and the caller.

After the operator has completed the caller's request, she immediately leaves the connection and neither the observer nor the operator can hear the conversation between the caller and the called party.

This equipment is used as a supervisory tool to determine the effective application of prescribed operating procedures and to assist in the training of switchboard operators. Responsibility for service observing is reserved to specifically designated supervisors and all operators are informed of its existence and use as a supervisory and training facility. Use of this equipment has proven to be a very effective and flexible management tool in improving the level of operator performance and FTS service.

The automatic call distributor equipment is furnished by the telephone company equipped with a service observation feature. This equipment was utilized in the Washington Federal Information Center, and an appropriate deviation for its use was obtained from the Administrator of GSA. Recently, this feature was ordered out and disconnected by the C. & P. Telephone Co.

Mr. Chairman, this completes my statement. We will be happy to respond to any questions which you or other members of the subcommittee may have.

Mr. MOORHEAD. Thank you very much, Mr. Burton. I think now might be an appropriate time to administer the oath to your associates.

Do you solemnly swear the testimony you have given and will give to this subcommittee is the truth, the whole truth and nothing but the truth so help you God?

Mr. BURTON. I do.

Ms. LATIMER. I do.

Mr. PLOTKIN. I do.

Mr. MOORHEAD. Thank you very much, Mr. Burton.

I will try and keep questions brief of myself and my colleagues and staff because we have three more witnesses.

As Deputy Commissioner for Automated Data, Mr. Burton, can you give us the status, so far as GSA is concerned, of the so-called Fed-Net?

Mr. BURTON. Yes, sir, I think I can, although I was not really prepared to discuss Fed-Net with you today.

Mr. MOORHEAD. I happened to have had a conference with Mr. Sampson recently so I think I know what your answer should be.

Mr. BURTON. This is a project we called the new equipment project (NEP) recently referred to as "Fed-Net."

The original purpose of the NEP was to procure ADP and telecommunications solely to satisfy all of GSA's requirements. We had determined that our equipment was outmoded and inefficient (it was second-generation equipment purchased in the mid-1960's). Our in-house determination for the need for new equipment was confirmed by a study done by an outside consultant.

However, there evolved a change in the original purpose. In April of 1973, we became aware that the Department of Agriculture needed new equipment. Both GSA and the Department of Agriculture saw this as a unique opportunity to join procurements of major computer systems. It was a chance to achieve significant cost reduction in the acquisition of equipment and to enjoy the economic and operational benefits from a common shared data communications network in accordance with GSA's legislative mandate.

In September of 1973, it was determined that additional economies could be obtained if we included within this acquisition three additional computer systems on an option basis to take care of a portion of the potential future computational requirements of Federal agencies beyond fiscal year 1978.

The final requests for proposal sent to industry in February 1974, contained four computer systems for the Department of Agriculture plus one optional system for them. It contained one computer system for GSA plus three optional systems to meet a portion of potential future needs. Options were used instead of firm commitments in case the future needs did not materialize. The proposal also contained a data communications network (DCN) to serve all the ADP sites. From the beginning, the purpose of this project was to fulfill our mandate to provide modern equipment needed by agencies to fulfill their missions in serving people.

The current status is that the communications network portion of the proposal has been deleted from the RFP that is presently on the street. The number of ADP sites has been changed. The Department of Agriculture ADP sites are still the same, namely, four firm sites, and one optional site. The GSA requirement has been reduced to only one optional site.

Mr. MOORHEAD. Understand, Mr. Burton, I was on the subcommittee of our full committee that participated in legislation giving GSA the authority over automated data processing in the Government. I think this was a good bill. I supported it. I think that the intentions—I think that Fed-Net was started with good intentions without the realization that it could be an automated national data bank because of interconnections. I hope that, as Mr. Sampson told me, you will halt any part of the Fed-Net project that could conceivably be transferred into an automated national data bank until further study could be made as to its privacy implications.

Mr. BURTON. Mr. Chairman, as you indicated, the Administrator, Mr. Sampson, is very much concerned about the issue of privacy. He is just as much concerned as this committee. He has been in contact with several of the interested committees. He has indicated, for example, that we will do nothing on the DCN, the telecommunications portion, that is the transmission portion of that procurement at this time. We have deleted it from the present RFP. He is hopeful that some legislation can be passed in this session of Congress. If it is not,

he has assured all those committees that are interested that we will consult with them before proceeding in any way with the communications network.

Mr. MOORHEAD. Why hasn't the communications portion of the Agriculture Department's procurement as part of Fed-Net been recalled and deleted?

Mr. BURTON. As GSA handled the joint procurement, all of the DCN, the communications network, has been deleted, Mr. Chairman.

Mr. MOORHEAD. All of the communications portion?

Mr. BURTON. Yes, sir. Now, I am not aware of any separate action that Agriculture may be taking. But as far as GSA is concerned, to my best knowledge as I sit here talking with you, the entire communication network portion has been deleted.

Mr. MOORHEAD. It is my understanding that Agriculture has a request for procurement outstanding at the present time which has not been recalled.

Mr. BURTON. They may have, Mr. Chairman. I am not aware of that.

Mr. MOORHEAD. You would not have control over that?

Mr. BURTON. Agriculture would have to come to us for a delegation of procurement authority before they proceeded with it. I am not aware of any separate procurement that they have on the street at this time.

Mr. Chairman, perhaps I can clarify a little bit. They, as I understand it, do have a procurement out for hardware, not a communications network, but for some terminal devices that attach to a network. What network it is going to be attached to, I do not know. There is in existence a network, the public telephone system is a network.

Mr. ALEXANDER. Will the chairman yield just for one question? Sir, do you happen to know how long the request or the order for hardware by USDA has been implemented or has been out for implementation?

Mr. BURTON. Are you talking about the terminal equipment?

Mr. ALEXANDER. Right.

Mr. BURTON. As a matter of fact, since I was handed a note reminding me of the hardware and the interest here, I also am under the impression that Agriculture was proceeding with a procurement, but that it has been withdrawn. I am not sure of that.

Mr. ALEXANDER. Do you know whether or not the withdrawal of that request for procurement was concurrent with the recession of the Executive order which permitted the Internal Revenue Service to turn over income tax data to the Department of Agriculture for, as they described it, statistical purposes?

Mr. BURTON. I have no knowledge of that. I just do not know.

Mr. ALEXANDER. Would that information be available to you through your normal inquiry?

Mr. BURTON. I would assume that that information is available to us.

Mr. ALEXANDER. Could you provide this committee with that research, please?

Mr. BURTON. We will do so.

Mr. ALEXANDER. Thank you, Mr. Chairman. I would like to ask unanimous consent that the record be held open for submission of that data at that point.

Mr. MOORHEAD. Without objection, so ordered.
[The material referred to follows:]

QUESTION CONCERNING THE PROCUREMENT OF 4,000 DEPARTMENT OF AGRICULTURE DATA TERMINALS

Do you know whether or not the withdrawal of that request for procurement was concerned with the recession of the Executive order which permitted the Internal Revenue Service to turn over income tax data to the Department of Agriculture for, as they described it, statistical purposes?

Executive Order 11709, which we believe is the order that is being referred to, was issued on March 27, 1973. Since the Agriculture procurement OIS-74-R-512 was issued on May 7, 1974. GSA by letter dated June 7, 1974, required the Department of Agriculture to discontinue this procurement until a review could be made. These actions were not concurrent, but were completely independent of each other. GSA is in receipt of a letter dated June 14, 1974, from the Department of Agriculture requesting our concurrence for the procurement of 952 terminal devices. To date, GSA has verbally requested the Department of Agriculture to take no further action on this procurement, and a written statement of this position is being forwarded to USDA. For the record, it is our understanding that the Department of Agriculture procurement has not been withdrawn but has been extended by the Department of Agriculture to July 17, 1974.

Mr. MOORHEAD. Under the 5-minute rule, extended by 1 minute Mr. Alexander took, I would like to ask you about your statement on page 3 that only three agencies requested variations from your listening-in device regulation. Testimony previously submitted to this committee indicated quite a number of other agencies with various devices, whether they were transmitter cutoffs or real listening-in devices. The largest number, 596 out of the total of 997 in Federal Government agencies in the Metropolitan Washington area, were by the Department of State; yet you do not list them as one of those departments which had requested a variation. Is there a reason for that?

Mr. BURTON. Mr. Plotkin, I think, can probably give you a better indication of that than I.

Mr. PLOTKIN. As far as we know, State Department never asked us for a deviation under the regulation.

Mr. MOORHEAD. Mr. Plotkin, my time has expired, but may I hand you this list. Could you come forward, sir, and maybe while Mr. Burton is answering the questions, you can read that and see why there is such a deviation from your testimony and the reports given to us from the various departments and agencies as to various listening-in devices.

Mr. Gude?

Mr. GUDE. Thank you, Mr. Chairman.

Mr. Burton, I was wondering, in reference to the statement on page 4, that all agency employees answering the calls were to be made aware of the fact their conversations may be monitored. Has it come to your attention that employees in any of the agencies have been unaware of monitoring? Is the advisement of that practice carried out in a satisfactory manner for new employees coming on the job? What guarantee is there that they are advised that some of their telephone work may be monitored?

Mr. BURTON. When a new employee, an operator, comes into that job, of course the regulations call for it, but your question is: How are we sure that they are advised? The supervisors are aware of the importance of this regulation, and as far as we can ascertain they faithfully carry that out.

Mr. GUDE. You have never had any instance of employees complaining that they were unaware of this practice?

Mr. BURTON. No, sir.

Mr. GUDE. There has never been any evidence of a failure to carry this out?

Mr. BURTON. That is correct, sir.

Mr. GUDE. Thank you, Mr. Chairman.

Mr. MOORHEAD. Mr. Alexander?

Mr. ALEXANDER. Mr. Chairman, thank you very much. I will not use all of my time this morning. We have several witnesses to hear and we are all interested in doing this as expeditiously as possible.

I would like to thank the gentleman for his testimony and merely state that sometimes there is difficulty in determining the difference between legitimate Government function and abuse of Executive authority. Your participation this morning has helped us in seeking this definition, and we appreciate your contribution.

Mr. BURTON. Thank you.

Mr. MOORHEAD. I have a few more questions, Mr. Burton, and I will try to emulate the good example of my colleagues to be brief.

Explain the operation of the sampling by GSA of FTS telephone calls.

Mr. BURTON. Sampling of the FTS telephone calls is for billing purposes only; it is part of a billing procedure. It in no way involves the monitoring of telephone conversations. This sampling procedure for billing is accomplished in three ways: Automatic message accounting equipment, which is purely a mechanical device which records the fact that a phone call has been made from and to where it was placed to. It is purely a mechanical process; no people are involved in it.

There is DART equipment, which stands for dial acquisition recording trunk. This is equipment which is semiautomatic. It is automatic to the extent that when a call comes in, a signal is flashed and an operator is brought in, the circuit is split, the called party is advised by the operator to stand by for a FTS phone call. The calling party is then asked for his FTS agency identification and the number he is calling from; then the circuit is completed and the operator goes off the line.

The third way is done manually, where you place a telephone call through the operator who records the called party and the calling party. These FTS sampling techniques are similar to those used by the telephone company for billing purposes.

Mr. MOORHEAD. I do not want to sound too parochial, but as a Member of Congress, using the FTS system under regulations, can you tell me whether or not congressional calls on the FTS system are at any time monitored manually? I am not concerned about the machine that checks where the call goes to or comes from.

Mr. BURTON. It is possible that congressional calls are sampled manually for billing purposes. There is no way of distinguishing a congressional originated call from any other.

Mr. MOORHEAD. I yield to Mr. Cornish at this point to follow up on that question.

Mr. CORNISH. Thank you, Mr. Chairman.

Mr. Plotkin, do you know for a fact whether this has ever been done, the monitoring of an FTS call on congressional lines?

Mr. PLOTKIN. Not monitoring; we sample.

Mr. CORNISH. All right, sample?

Mr. PLOTKIN. The answer is yes. Congress uses the FTS and if they place calls on the FTS they can be sampled. This is our only method for determining usage for billing purposes.

Mr. CORNISH. Do you have any personal knowledge of this being done on a sample basis?

Mr. PLOTKIN. No.

Mr. CORNISH. I am sorry. I did not hear your response.

Mr. PLOTKIN. Not personally, no.

What I am saying, if a staff member or if a congressional office was placing a call, and they wanted to get to one of the FTS local intrastate WATS lines, they could be sampled. Let me explain how this would work. When they place a call and arrive at an FTS switchboard and their FTS call was to go over a manual circuit, which was selected for sampling this quarter, the FTS operator would ask for your agency name and identification. They have not placed or completed the call yet. She will then place the call. If the party answers, she will keep the ticket. If the party does not answer, she will tear up the ticket. That is what we mean by a manual sample—the operator is not monitoring the call.

Mr. MOORHEAD. Mr. Gude?

Mr. GUDE. No questions.

Mr. MOORHEAD. Mr. Daniels?

Mr. DANIELS. No questions.

Mr. MOORHEAD. Mr. Phillips?

Mr. PHILLIPS. Thank you, Mr. Chairman.

Mr. Burton, I would like to go back to the testimony which you gave on page 3 where you discuss the request for deviation received by GSA from other agencies.

Mr. Chairman, I think it would be helpful for our record if we could obtain copies of the requests that were granted by GSA to other agencies. There are three that are mentioned here on page 3. Could we have copies of those determinations for the record?

Mr. BURTON. Yes, sir.

[The information follows:]

GENERAL SERVICES ADMINISTRATION
Washington, D.C., December 3, 1973.

MR. FRANK DEGEORGE,
Assistant Commissioner for Administration, Social Security Administration, Department of Health, Education, and Welfare, Baltimore, Md.

DEAR MR. DEGEORGE: In accordance with the Federal property management regulations 101-35, approval is granted to establish a Teleservice center utilizing automatic call distributor (ACD) equipment at each of the locations mentioned in Mr. Zawatzky's letter of October 15, 1973.

As you know, one of the standard features of the ACD supervisory console is an ability to monitor incoming calls. Our regional offices have instructions not to install GSA circuits into monitoring equipment without approval from this office. In view of your determination that monitoring of incoming calls at Teleservice centers is essential, we have requested our regional offices to provide General Services Administration facilities to your ACD locations provided that:

(1) Your request for service to the regional office is accompanied with a copy of the August 28, 1972, determination by the Assistant Secretary for Administration of the Department of Health, Education, and Welfare that the ACD's are essential to the effective execution of agency responsibilities and is required by operational needs;

(2) No recording devices are to be associated with the monitoring equipment;

(3) The monitoring feature will be used only for training purposes and to maintain a high degree of quality in the Social Security Administration (SSA) program;

(4) SSA employees are informed that their conversations may be monitored; and

(5) Future similar requests for monitoring devices which comply with requisites of this request should cite the approval given in this instance. Other nonconforming requests should be reviewed for new authorization.

If we can be of any further assistance in this matter, you or a member of your staff may contact Mr. Robert J. Baldwin on 202-254-6306.

Sincerely,

M. S. MEEKER, *Commissioner.*

DEPARTMENT OF HEALTH, EDUCATION, AND WELFARE,
SOCIAL SECURITY ADMINISTRATION,
Baltimore, Md., October 15, 1973.

MR. SIDNEY WEINSTEIN,
Assistant Commissioner for Agency Assistance, Planning and Policy, Automated Data and Telecommunications Service, General Services Administration, Washington, D.C.

DEAR MR. WEINSTEIN: The Social Security Administration (SSA) requests approval to initiate centralized telephone answering services by establishing a Teleservice center (TSC) utilizing automatic call distributor (ACD) equipment at each of the following locations.

Location	*Service area*
Minneapolis, Minn	Minneapolis/St. Paul metropolitan area.
Cincinnati, Ohio	Metropolitan area.
Denver, Colo	Metropolitan area.
New York, N.Y. (Queens)	Brooklyn and Queens Boroughs.
Jersey City, N.J	Manhattan, Richmond, Bronx, Boroughs.
Perth Amboy, N.J	Upper New Jersey.
Seattle, Wash	Puget Sound area.
Portland, Oreg	Metropolitan area.
Jacksonville, Fla	Metropolitan area.

These TSC installations are viewed as operational requirements that will improve public service and SSA operations. Data sheets for each installation are enclosed.

If there are any questions or if additional information is required, please have your staff call Mr. Russell Mize on IDS Code 130, extension 46276.

Sincerely yours,

LOUIS ZAWATZKY,
Acting Assistant Commissioner for Administration.

Enclosures.

DEPARTMENT OF HEALTH, EDUCATION, AND WELFARE,
August 28, 1972.

To: Mr. L. Zawatsky, Acting Assistant Commissioner for Administration, SSA.
From: Assistant Secretary for Administration and Management.
Subject: Monitoring employee telephone calls for service quality evaluation; Mr. Futterman's memorandum of June 29, 1972.

We have reviewed Mr. Futterman's memorandum which stressed the importance of evaluating the quality of service furnished to the public by Social Security Administration personnel assigned to Metropolitan Answering Service (MAS) units. The MAS units utilizing telephone company automatic call distributor equipment provide a centralized telephone answering service for a given geographic area.

The Department's Telecommunications Management Manual, 103-35.6304(a), forbids the recording, monitoring, or listening in on telephone conversations without prior knowledge of all parties to the conversation except when a determination is made that an exception is essential to the effective execution of agency responsibilities and is required by operational needs. I have made this

determination in this instance because the effectiveness of the SSA program to improve public service and district office efficiency by the institution of Metropolitan Answering Service units depends on the quality of service furnished by employees who are assigned to handle the telephone inquiries and relate the SSA program to callers in a meaningful, courteous, and productive manner. In monitoring telephone calls at the MAS units, management officials will be able to measure the success of the program by determining the strengths and weaknesses of each employee assigned to the units. This exception also constitutes a deviation in accordance with section 101–35.307–2 of the Federal property management regulations.

Monitoring of telephone calls at MAS units, therefore, will be permitted under the following conditions:

(*a*) Monitoring shall only be done at the supervisor console of the ACD;

(*b*) Monitoring shall be limited to observing employee courtesy and accuracy of information furnished to the caller;

(*c*) Monitoring shall be limited to those telephone lines associated with directory listed numbers, and no recording shall be made of any part of the conversation;

(*d*) Monitoring shall be done only for as long, and as often, as necessary to make the quality evaluations as set forth in your memorandum;

(*e*) SSA shall protect the rights of those individuals whose calls are subject to monitoring by—

1. Affixing to ACD attendant position telephones, a label that states "this instrument is subject to monitoring of quality control."

2. Orient all present and new employees in MAS units why, when, and hours monitoring will be conducted to insure complete understanding of the system.

Please furnish to this office a copy of the SSA implementing regulations. Should your staff have any questions on this matter, feel free to contact Frank J. Campbell on 963–4964.

RODNEY H. BRADY.

GENERAL SERVICES ADMINISTRATION,
Washington, D.C., August 2, 1973.

MR. DONALD C. ALEXANDER,
Commissioner, Internal Revenue Service,
Department of the Treasury, Washington, D.C.

DEAR MR. ALEXANDER: This is in reply to your letter of July 13, 1973, to Mr. Sidney Weinstein, Assistant Commissioner for Agency Assistance, Planning, and Policy, concerning the operational necessity of monitoring taxpayer service telephone calls. In accordance with the provisions of Federal property management regulations (FPMR) 101–35, and based on your determination that monitoring incoming calls is essential to your agency's taxpayers service program, we concur in the installation of automatic call distributors (ACD's) with service-observing capability.

This approval, however, is contingent upon the following:

1. No recording devices are to be associated with the monitoring equipment.

2. All Internal Revenue Service employees answering taxpayers calls are made aware of the fact that their conversations may be monitored.

3. The monitoring feature will be used only for training purposes and to maintain a high degree of quality in the taxpayers assistance program.

4. Future submission of requirements for ACD's containing the service observing feature in accordance with the provisions of FPMR 101–35, when applicable, should cite this letter of approval to insure expeditious fulfillment of your requirements.

Our regional commissioners are being notified of this approval. If you have any questions in this matter, or if I can be of any further assistance, please let me know.

Sincerely,

M. S. MEEKER,
Commissioner.

DEPARTMENT OF THE TREASURY,
INTERNAL REVENUE SERVICE,
Washington, D.C., July 13, 1973.

MR. SIDNEY WEINSTEIN,
Assistant Commissioner for Agency Planning and Policy, General Services Administration, Washington, D.C.

DEAR MR. WEINSTEIN: As provided for in section 101–35.308 of the Federal property management regulations, I have determined that the service monitoring of taxpayer service telephone calls is operationally essential to the effective execution of the Internal Revenue Service taxpayer service program.

This operational requirement is based on the service's interest in determining that taxpayer service telephone calls are being courteously and accurately handled by our employees.

The functional authority for this decision is vested in Treasury Department Order No. 150–2, dated May 15, 1952, and Treasury Department Order No. 150–37, dated March 17, 1955.

With kind regards.

Sincerely,

DONALD C. ALEXANDER,
Commissioner.

GENERAL SERVICES ADMINISTRATION,
July 11, 1973.

MR. RICHARD F. SIMKO,
Chief, Information Systems Branch, Internal Revenue Service, Department of the Treasury, Washington, D.C.

DEAR MR. SIMKO: This is in reference to your letter of June 29, 1973, concerning the service observation feature of automatic call distributors. We do not question your General Counsel's opinion that this feature does not violate applicable Federal statutes. However, your correspondence does not indicate that the Secretary of Treasury, or his authorized designee, has determined in writing that the service observation feature is essential to the effective execution of agency responsibilities or is required by operational needs. Such a determination is required by Federal property management regulations 101–35.307–2.

We would appreciate receiving such a determination at your earliest convenience. If the Secretary, himself, does not sign such determinations, we would also like to see the delegation of authority authorizing the actual signatory official to make them.

If you have any questions on this matter, please call Mr. Robert Baldwin on IDS 193–46306.

Sincerely,

SIDNEY WEINSTEIN,
Assistant Commissioner for Agency Assistance, Planning, and Policy.

DEPARTMENT OF THE TREASURY,
INTERNAL REVENUE SERVICE,
Washington, D.C., June 29, 1973.

MR. SIDNEY WEINSTEIN,
Assistant Commissioner for Agency Planning and Policy, General Services Administration, Washington, D.C.

DEAR MR. WEINSTEIN: In response to your telephone conversation of June 27, 1973, with Mr. Inglesby, please note the enclosed memorandum in which our chief counsel has thoroughly studied and reviewed the question of service monitoring of telephone calls related to our taxpayer service function. The attached memorandum of law reviews the practice of service monitoring of taxpayer telephone calls and emphatically concludes that our monitoring policy is supported not only by recent case law, but also by an explicit opinion of the Assistant Attorney General.

We interpret this memorandum to say that the use of ACD supervisory monitoring equipment (a package item associated with the equipment) is both legally and practically acceptable. Furthermore, we feel that supervisory monitoring is necessary to maintain a high degree of quality in our taxpayer assistance program.

If I can provide any additional details about our telephone taxpayer service program which might be helpful in the matter, please contact me as soon as possible.

Sincerely,

RICHARD E. SIMKO,
Chief, Information Systems Branch.

Enclosure.

GENERAL SERVICES ADMINISTRATION,
Washington, D.C., April 13, 1974.

Re Veterans' Administration Phoenix request for telephone monitoring equipment (Ref. FPMR 101–35.308–9(f) and FPMR 101–35.307–2).

This confirms Mr. Edwards' discussion with you on February 1, 1974 concerning your correspondence of December 19, 1973, relating to a request for silent observer equipment for the Veterans' Administration Regional Office in Phoenix.

This matter has been discussed with the Veterans' Administration Central Office. They agree that this request falls within the purview of the above-cited regulation. They have discussed the matter with their Phoenix office and have advised us that they will not oppose their regional office installing the desired observing equipment and will provide the necessary authorization to their regional office.

Since the regulation provides that deviations accompanied by the proper written determination can be placed through GSA facilities, this matter can be handled by your region. Please insure that the proper determination is received prior to installation of silent observer equipment.

If there are any questions concerning this matter, you or a member of your staff may contact Mr. J. T. Edwards on FTS 202–254–6306.

SIDNEY WEINSTEIN,
Assistant Commissioner for Agency Assistance, Planning, and Policy.

VETERANS' ADMINISTRATION,
REGIONAL OFFICE,
Phoenix, Ariz., November 30, 1973.

DIRECTOR OF TELECOMMUNICATIONS,
General Services Administration ADTS,
San Francisco, Calif.
(Attention: R. J. Wright.)

This is in regard to our request for silent observer equipment to be placed on the telephones in our telephone unit.

VA Manual MP–6, part VIII, section 204.10c, authorizes the use of monitoring equipment when it is solely used for the purposes of evaluating the quality of telephone interviews conducted by veterans' benefits counselors. The objective is to maintain the highest possible quality of service to those who telephone the Veterans' Administration for information, advice and assistance.

Before the evaluation is conducted the veterans' benefit counselors will be notified. There will be no need to notify the party calling, since monitoring will be performed only for the purpose of improving the quality of service to be given.

Sincerely yours,

GORDON A. LYONS,
Director.

GENERAL SERVICES ADMINISTRATION,
San Francisco, Calif., December 19, 1974.

Subject: Veterans' Administration Phoenix request for telephone monitoring equipment (Ref. FPMR 101–35.308–9(f)).

Enclosed Veterans' Administration request and R–9 reply forwarded for your information and future reference.

The Veterans' Administration regional office in Phoenix is served by the GSA switchboard there, Facility No. (985). If approved, equipment is available and can be ordered from the Mountain States Telephone Co.

C. W. GETZ.

Mr. PHILLIPS. Also, are these determinations given in blanket form or limited to 1 year or 2 years or what is the policy on that?

Mr. BURTON. There is no limitation as far as the number of years.

Mr. PHILLIPS. We are curious as to why, since our investigation shows there are over 30 agencies that use transmitter cutoffs or listening-in circuits or variations of those two, and you have only granted three agencies deviations, which does not include DOD, State, Labor, almost every department in the Government using this equipment, and yet you say there are only three to whom you granted deviations. Does this mean that each of these other agencies is in violation of your regulation?

Mr. BURTON. I do not know the specifics, but there are reasons why they would not have to come to us for a deviation. In those cases where they are using a telephone service not provided by the FTS, then the regulations state that they should have those deviations in writing in their file.

Mr. PHILLIPS. How many agencies have their own system that would not come under your regulation?

Mr. BURTON. Probably at one place or another, a telephone here or a telephone there in small offices, maybe most agencies. I cannot give you an exact answer.

Mr. MOORHEAD. Mr. Phillips, I handed Mr. Plotkin that list.

Mr. PHILLIPS. Yes, he is leading up to whether or not he had a response on that point.

Mr. PLOTKIN. For example, the list furnished by the chairman indicates a number of agencies. The list is of the Washington metropolitan area, and these devices may not necessarily be on GSA facilities.

Mr. BURTON. Excuse me.

Ms. Latimer called my attention to something which is important, I think. There are a number of agencies exempt by law from this regulation.

Mr. PHILLIPS. What are they? Or could you supply a list for the record at this point?

Mr. BURTON. Yes, sir.

Ms. LATIMER. Yes, sir.

Mr. MOORHEAD. May I interrupt?

Is State Department one of those exempt?

Ms. LATIMER. As to the State Department, under the Federal Property Act, the Secretary of State, under the Foreign Service Buildings Act of May 7, 1926, as amended, would be one of the exempt activities, so we would have to know specifically under what authority they are doing it.

Under section 602(d) of the Federal Property Act there are a number of agencies and programs requiring special treatment that are exempt. There are about 20 with reference to specific programs.

Mr. MOORHEAD. Maybe after the hearing when you have your transcript back, maybe you and Mr. Plotkin can get together and supply

us with some information. There seem to be inconsistencies. Maybe they can be explained.

[The information follows:]

AGENCIES AND PROGRAMS EXEMPT FROM PART 101-35—TELECOMMUNICATIONS OF THE FEDERAL PROPERTY MANAGEMENT REGULATIONS (FPMR)

Telecommunications services and equipment are provided by GSA to other agencies pursuant to section 201 of the Federal Property and Administrative Services Act of 1949, 63 Stat. 383, as amended (40 U.S.C. 481), as well as section 7 of the act of June 14, 1946 (40 U.S.C. 295) (attachment 1). This authority however, is expressly limited, thus exempting certain agencies and programs from the GSA responsibility. These limitations are:

1. Section 201 of the Property Act limits the GSA authority to executive agencies, and if requested to Federal agencies, mixed-ownership corporations, and the District of Columbia. In addition, section 602(e) of the Property Act extends the authority to furnish such services, if requested, "to the Senate, the House of Representatives, or the Architect of the Capitol."

2. Section 201 further requires GSA to determine that providing such services and equipment are "advantageous to the Government in terms of economy, efficiency, or service, and with due regard to the program activities of the agencies concerned * * * in the proper discharge of their responsibilities."

3. Further, section 201 of the Property Act states that the Secretary of Defense may from time to time, unless the President otherwise directs, exempt the Department of Defense (DOD) from action taken by GSA whenever he determines such exemption to be in the best interest of national security. (Attachment 2—copy of the delegation of authority from GSA to DOD, and the statement of areas of understanding between DOD and GSA regarding communications.)

4. Section 7 of the act of June 14, 1946, "does not apply to communications systems for handling messages of a confidential or secret nature, or to the operation of cryptographic equipment or transmission of secret, security, or coded messages, or to buildings operated or occupied by the Post Office Department, except upon request of the department or agency concerned."

5. Section 602(d) of the Property Act lists some 20 activities or programs requiring special treatment that are exempt from the Property Act (attachment 3).

6. In addition, pursuant to the above cited authority, GSA has listed in the Federal property management regulations (FPMR) certain other agencies and programs where the provisions of the FPMR 101-35 do not apply (attachment 4).

NOTE.—In order to determine whether certain devices were installed by agencies under exempt programs and activities, GSA would require specific information from each listed agency.

ATTACHMENT 1

TITLE II—PROPERTY MANAGEMENT

PROCUREMENT, WAREHOUSING, AND RELATED ACTIVITIES

[40 U.S.C. 481] SEC. 201. (a) The Administrator shall, in respect of executive agencies, and to the extent that he determines that so doing is advantageous to the Government in terms of economy, efficiency, or service, and with due regard to the program activities of the agencies concerned—

(1) prescribe policies and methods of procurement and supply of personal property and nonpersonal services, including related functions such as contracting, inspection, storage, issue, property identification and classification, transportation and traffic management, management of public utility services, and repairing and converting; and

(2) operate, and, after consultation with the executive agencies affected, consolidate, take over, or arrange for the operation by any executive agency of warehouses, supply centers, repair shops, fuel yards, and other similar facilities; and

(3) procure and supply personal property and nonpersonal services for the use of executive agencies in the proper discharge of their responsibilities, and perform functions related to procurement and supply such as those mentioned above in subparagraph (1): *Provided*, That contracts for public utility services may be made for periods not exceeding ten years; and

(4) with respect to transportation and other public utility services for the use of executive agencies, represent such agencies in negotiations with carriers and other public utilities and in proceedings involving carriers or other public utilities before Federal and State regulatory bodies;

Provided, That the Secretary of Defense may from time to time, and unless the President shall otherwise direct, exempt the Department of Defense from action taken or which may be taken by the Administrator unless clauses (1), (2), (3), and (4) above whenever he determines such exemption to be in the best interests of national security.

(b) The Administrator shall as far as practicable provide any of the services specified in subsection (a) of this section to any other Federal agency, mixed ownership corporation (as defined in the Government Corporation Control Act), or the District of Columbia, upon its request.

(c) In acquiring personal property, any executive agency, under regulations to be prescribed by the Administrator, may exchange or sell similar items and may apply the exchange allowance or proceeds of sale in such cases in whole or in part payment for the property acquired: *Provided*, That any transaction carried out under the authority of this subsection shall be evidenced in writing.

(d) In conformity with policies prescribed by the Administrator under subsection (a), any executive agency may utilize the services, work, materials, and equipment of any other executive agency, with the consent of such other executive agency, for the inspection of personal property incident to the procurement thereof, and notwithstanding section 3678 of the Revised Statutes (31 U.S.C. 628) or any other provision of law such other executive agency may furnish such services, work, materials, and equipment for that purpose without reimbursement or transfer of funds.

(e) Whenever the head of any executive agency determines that the remaining storage or shelf life of any medical materials or medical supplies held by such agency for national emergency purposes is of too short duration to justify their continued retention for such purposes and that their transfer or disposal would be in the interest of the United States, such materials or supplies shall be considered for the purposes of section 202 of this Act to be excess property. In accordance with the regulations of the Administrator, such excess materials or supplies may thereupon be transferred to or exchanged with any other Federal agency for other medical materials or supplies. Any proceeds derived from such transfers may be credited to the current applicable appropriation or fund of the transferor agency and shall be available only for the purchase of medical materials or supplies to be held for national emergency purposes. If such materials or supplies are not transferred to or exchanged with any other Federal agency, they shall be disposed of as surplus property. To the greatest extent practicable, the head of the executive agency holding such medical materials or supplies shall make the determination provided for in the first sentence of this subsection at such times as to insure that such medical materials or medical supplies can be transferred or otherwise disposed of in sufficient time to permit their use before their shelf life expires and they are rendered unfit for human use.

PROPERTY UTILIZATION

[40 U.S.C. 483] SEC. 202. (a) In order to minimize expenditures for property, the Administrator shall prescribe policies and methods to promote the maximum utilization of excess property by executive agencies, and he shall provide for the transfer of excess property among Federal agencies and to the organizations specified in section 109(f). The Administrator, with the approval of the Director of the Bureau of the Budget, shall prescribe the extent of reimbursement for such transfers of excess property: *Provided*, That reimbursement shall be required of the fair value, as determined by the Administrator, of any excess property transferred whenever net proceeds are requested pursuant to section 204(c) or whenever either the tansferor or the transferee agency (or the organizational unit affected) is subject to the Government Corporation Control Act (59 Stat. 597, 31 U.S.C. 841) or is an organization specified in section 109(f); and the excess property

* * * * * * *

PUBLIC UTILITY COMMUNICATIONS SERVICES SERVING GOVERNMENTAL ACTIVITIES

60 Stat. 258, as amended (40 U.S.C. 295)

* * * * * * *

SEC. 7. The Administrator of General Services is authorized to provide and operate public utility communications services serving one or more governmental activities, in and outside the District of Columbia, where it is found that such services are economical and in the interest of the Government. This section does not apply to communications systems for handling messages of a confidential or secret nature, or to the operation of cryptographic equipment or transmission of secret, security, or coded messages, or to buildings operated or occupied by the Post Office Department, except upon request of the department or agency concerned.

* * * * * * *

Approved June 14, 1946.

GENERAL SERVICES ADMINISTRATION

SECRETARY OF DEFENSE

REVISED DELEGATION OF AUTHORITY, WITH RESPECT TO CONTRACTS FOR PROCUREMENT OF PUBLIC UTILITY SERVICES FOR PERSONS NOT EXCEEDING TEN YEARS

1. Pursuant to authority vested in me by the provisions of the Federal Property and Administrative Services Act of 1949, as amended (63 Stat. 383; 64 Stat. 591), authority is hereby delegated to the Secretary of Defense to enter into contracts for public utility services (power, gas, water, and communications) for periods extending beyond a current fiscal year but not exceeding ten years, under one or more of the following circumstances:

(a) Where there are obtained lower rates, larger discounts or more favorable conditions of service than those available under contracts the firm term of which would not extend beyond a current fiscal year;

(b) Where connection or special facility charges payable under contracts the firm term of which would not extend beyond a current fiscal year are eliminated or reduced;

(c) The utility refuses to render the desired service except under a contract the firm term of which extends beyond a current fiscal year.

2. Copies of, and other pertinent data and information with respect to such contracts executed by the Department of Defense for such utility service under the authority of this delegation will be furnished to the General Services Administration unless distribution thereof is inadvisable for reasons of security.

3. This authority shall be exercised strictly in accordance with the applicable provisions of the "Statement of areas of understanding between the Department of Defense and General Services Administration" entitled "Procurement of Utility Services (Power, Gas, Water) (15 F.R. 8227), and "Procurement of Communication Services" (15 F.R. 8226).

4. The authority herein delegated may be redelegated to any officer, official or employee within the Department of Defense.

5. This delegation of authority shall be effective as of the date hereof, and supersedes prior delegation of August 14, 1951 (16 F.R. 8309).

Dated: October 11, 1954.

EDMUND F. MANSURE,
Administrator.

[F.R. Doc. 54-8156; Filed, Oct. 13, 1954; 4:28 p.m.]

GENERAL SERVICES ADMINISTRATION

PROCUREMENT OF COMMUNICATIONS SERVICES

STATEMENT OF AREAS OF UNDERSTANDING BETWEEN DEPARTMENT OF DEFENSE AND GENERAL SERVICES ADMINISTRATION

1. The areas of understanding herein set forth were worked out pursuant to order of the President of July 1, 1949, directed to the Secretary of Defense, the Director, Bureau of the Budget, and the Administrator of General Services.

2. The areas of understanding with respect to communications services are:

(a) (1) As used in this statement, with respect to communications services: "Area contracts" are contracts providing for the furnishing of a communication service to all, or substantially all, activities of the Government located within a specified area, executed by GSA or by another agency designated by GSA.

(2) As appropriate for contractual and operational matters, "Department of Defense" means one or more of the military departments.

(b) The basic principle in the procurement of communication services is that all such services shall be procured or provided at the minimum total cost of the Government consistent with requirements for capacity, efficiency of operation, reliability of service, security, and programed activities. These requirements must be determined by the using agency.

(c) Close coordination and cooperation between the GSA and the Department of Defense shall be maintained to obtain the maximum economy consistent with the requirements for service.

(d) Communications services for activities of the Department of Defense occupying property controlled or operated by another Federal agency will be procured or provided by the General Services Administration or by the operating agency unless in the opinion of the Department of Defense the procurement or provision thereof by the Department of Defense is necessary in the interest of military operations, exercise of command and/or National security.

(e) Communications services for the Department of Defense, in localities within an area where these services are or may become available under a General Services Administration contract, will be procured under a General Services Administration area contract when such a procedure is of benefit to the Government as a whole and does not adversely affect Military operations, exercise of command and/or National security. In all other instances, communication services required by the Department of Defense will continue to be procured under a standardized National Defense contract. Copies of or data on contracts executed by the Department of Defense for communications facilities and services will be furnished to the GSA upon request unless distribution is inadvisable for reasons of security.

(f) Except as provided in paragraphs 2 (d) and (e) above, all communication facilities and services for activities of the Department of Defense will be provided or procured by the Department of Defense.

(g) The Department of Defense will provide for complete coordination of all communication services procured or provided by it for all activities of the Department of the Army, Navy (including the Marine Corps) and Air Force, and for maximum economy consistent with requirements.

(h) Joint use of telephone facilities such as private branch exchanges is to be encouraged wherever such use will result in efficient and economical service: Provided, That in the opinion of the Department of Defense, no interference with military operations or violations of military security will result.

(i) It is recognized that rapid written communications for the Government as a whole can best be obtained by independent military and civilian agency systems, with these systems cooperating with each other. These systems, however, may interchange traffic where such interchange is efficient, and economical and practicable, provided that in the opinion of the Department of Defense there

is no interference with movement of military traffic, and the handling of civilian traffic does not necessitate the utilization of additional facilities and personnel by the Department of Defense.

(j) Except as otherwise provided herein, the GSA will represent executive agencies including the Department of Defense in proceedings involving communications before municipal, State and Federal regulatory bodies in all rate cases and matters associated therewith.

Exceptions. (1) In those instances where the Department of Defense has the sole Government interest in a proceeding involving communications before a regulatory body, the Department of Defense will conduct the representation on behalf of all executive agencies of the United States Government. The Department of Defense and the General Services Administration in pending or proposed proceedings will advise each other of action taken or to be taken that may have effect upon or be of interest or assistance to each other. Such representations conducted by the Department of Defense shall be subject to over-all coordination by General Services Administration. This shall not preclude representation for the Department of Defense by the General Services Administration when such representation is requested by the Department of Defense and is mutually agreeable.

(2) In those instances where the Department of Defense does not have sole Government interest in a proceeding involving communications before a regulatory body, the Department of Defense will conduct the representation on behalf of all executive agencies whenever representatives of the Department of Defense and the General Services Administration agree that conduct of the representation by the Department of Defense is in the best interest of the Government. Such representation conducted by the Department of Defense shall be subject to over-all coordination by the General Services Administration.

(3) Except as pertains to the applications of pertinent provisions of section 5, Public Law 211, 81st Congress.

(k) Liaison between the Department of Defense and the General Services Administration for all matters involving representation of executive agencies in proceedings involving communications before regulatory bodies shall be maintained between the Office of General Counsel, General Services Administration and the Office of General Counsel, Department of Defense.

(l) Liaison with regard to policy matters concerning this agreement and matters pertinent thereto except as provided in paragraph k, will be maintained between the Chief, Public Utilities Branch, Public Buildings Service, General Services Administration and Chief, Electronics Division, Munitions Board of the Department of Defense and for operational and contractual matters between designated representatives of the General Services Administration and of the Department of Defense.

(m) This area of understanding is applicable to communications services within the Continental United States, Hawaii, Puerto Rico and the Virgin Islands. The Department of Defense shall be exempt from action taken by the Administrator with respect to communications services under section 201(a) of Public Law 152 in other geographical areas.

Dated: November 27, 1950.

JESS LARSON,
Administrator of General Services.

Dated: November 22, 1950.

J. D. SMALL,
Chairman, Munitions Board,
Department of Defense.

[FR Doc. 50-10865 Filed Nov. 30, 1950; 8:46 a.m.]

ATTACHMENT 3

[40 U.S.C. 474] SEC. 602. (d) Nothing in this Act shall impair or affect any authority of—

(1) the President under the Philippine Property Act of 1946 (60 Stat. 418; 22 U.S.C. 1381);

(2) any executive agency with respect to any phase (including, but not limited to, procurement, storage, transportation, processing, and disposal) of any program conducted for purposes of resale, price support, grants to farmers, stabilization, transfer to foreign governments, or foreign aid,

relief, or rehabilitation: *Provided*, That the agency carrying out such program shall, to the maximum extent practicable, consistent with the fulfillment of the purposes of the program and the effective and efficient conduct of its business, coordinate its operations with the requirements of this Act and tthe policies and regulations prescribed pursuant thereto;

(3) any executive agency named in the Armed Services Procurement Act of 1947, and the head thereof, with respect to the administration of said Act;

(4) the Department of Defense with respect to property required for or located in occupied territories;

(5) the Secretary of Defense with respect to the administration of the National Industrial Reserve Act of 1948;

(6) the President with respect to the administration of the Strategic and Critical Materials Stock Piling Act (60 Stat. 596);

(7) the Secretary of State under the Foreign Service Buildings Act of May 7, 1926, as amended;

(8) the Secretary of the Army, the Secretary of the Navy, and the Secretary of the Air Force with respect to the administration of section 1(b) of the Act entitled "An Act to expedite the strengthening of the national defense", approved July 2, 1940 (54 Stat. 712);

(9) the Secretary of Agriculture or the Department of Agriculture under (A) the National School Lunch Act (60 Stat. 230); (B) the Farmers Home Administration Act of 1946 (60 Stat. 1062); (C) the Act of August 31, 1947, Public Law 298, Eightieth Congress, with respect to the disposal of labor supply centers, and labor homes, labor camps, or facilities; (D) section 32 of the Act of August 24, 1935 (49 Stat. 774), as amended, with respect to the exportation and domestic consumption of agricultural products; or (E) section 201 of the Agricultural Adjustment Act of 1938 (52 Stat. 36) or section 203(j) of the Agricultural Marketing Act of 1946 (60 Stat. 1082);

(10) The Secretary of Agriculture, Farm Credit Administration, or any farm credit board under section 6(b) of the Farm Credit Act of 1937 (50 Stat. 706), with respect to the acquisition or disposal of property;

(11) the Department of Housing and Urban Development or any officer thereof with respect to the disposal of residential property, or of other property (real or personal) held as part of or acquired for or in connection with residential property, or in connection with the insurance of mortgages, loans, or savings and loan accounts under the National Housing Act;

(12) the Tennessee Valley Authority with respect to nonpersonal services, with respect to the matters referred to in section 201(a)(4), and with respect to any property acquired or to be acquired for or in connection with any program of processing, manufacture, production, or force account construction: *Provided*, That the Tennessee Valley Authority shall to the maximum extent that it may deem practicable, consistent with the fulfillment of the purpose of its program and the effective and efficient conduct of its business, coordinate its operations with the requirements of this Act and the policies and regulations prescribed pursuant thereto;

(13) the Atomic Energy Commission;

(14) the Administrator of the Federal Aviation Agency or the Chief of the Weather Bureau with respect to the disposal of airport property and airway property for use as such property. For the purpose of this paragraph the terms "airport property" and "airway property" shall have the respective meanings ascribed to them in the International Aviation Facilities Act (62 Stat. 450);

(15) The Postmaster General or the Postal Establishment with respect to the means and methods of distribution and transportation of the mails, and contracts, negotiations, and proceedings before Federal and State regulatory and rate-making bodies, relating to the transportation of the mails, and the leasing and acquisition of real property, as authorized by law;

(16) the Secretary of Commerce with respect to the construction, reconstruction, and reconditioning (including outfitting and equipping incident to the foregoing), the acquisition, procurement, operation, maintenance, preservation, sale, lease, or charter of any merchant vessel or of any shipyard, ship site, terminal, pier, dock, warehouse, or other installation necessary or appropriate for the carrying out of any program of such Commission authorized by law, or nonadministrative activities incidental thereto: *Provided*, That the Secretary of Commerce shall to the maximum extent that it may deem practicable, consistent

with the fulfillment of the purposes of such programs and the effective and efficient conduct of such activities, coordinate its operations with the requirements of this Act, and the policies and regulations prescribed pursuant thereto;

(17) the Central Intelligence Agency;

(18) the Joint Committee on Printing, under the Act entitled "An Act providing for the public printing and binding and the distribution of public documents" approved January 12, 1895 (28 Stat. 601), as amended or any other Act;

(19) for such period of time as the President may specify, any other authority of any executive agency which the President determines within one year after the effective date of this Act should, in the public interest, stand unimpaired by this Act; or

(20) the Secretary of the Interior with respect to procurement for program operations under the Bonneville Project Act of 1937 (50 Stat. 731), as amended.

(e) No provision of this Act, as amended, shall apply to the Senate or the House of Representatives (including the Architect of the Capitol and any building, activity, or function under his direction), but any of the services and facilities authorized by this Act to be rendered or furnished shall, as far as practicable, be made available to the Senate, the House of Representatives, or the Architect of the Capitol, upon their request, and, if payment would be required for the rendition or furnishing of a similar service or facility to an executive agency, payment therefor shall be made by the recipient thereof, upon presentation of proper vouchers, in advance or by reimbursement (as may be agreed upon by the Administrator and the officer or body making such request). Such payment may be credited to the applicable appropriation of the executive agency receiving such payment.

(f) Section 3709, Revised Statutes, as amended (41 U.S.C. 5), is amended by striking out "$100" wherever it appears therein and inserting in lieu thereof "$500".

AUTHORIZATIONS FOR APPROPRIATIONS AND TRANSFER AUTHORITY

[40 U.S.C. 475] SEC. 603. (a) There are hereby authorized to be appropriated such sums as may be necessary to carry out the provisions of this Act, including payment in advance, when authorized by the Administrator, for library memberships in societies whose publications are available to members only, or to members at a price lower than that charged to the general public.

(b) When authorized by the Director of the Bureau of the Budget, any Federal agency may use, for the disposition of property under this Act, and for its care and handling pending such disposition, any funds heretofore or hereafter appropriated, allocated, or available to it for purposes similar to those provided for in sections 201, 202, 203, and 205 of this Act.

ATTACHMENT 4

§ 101-35.000 Scope.

This part prescribes policies and methods governing the utilization by executive agencies of telecommunications services within the United States and its insular possessions.

Subpart 101-35.1—General Provisions

§ 101-35.101 Authorities implemented.

This part 101-35 implements the following authorities: Section 201 of the Federal Property and Administrative Services Act of 1949 (40 U.S.C. 481); section 7, act of June 14, 1946 (40 U.S.C. 295); Presidential letter of July 1, 1949 (14 F.R. 3699; 3 CFR); Bureau of the Budget Bulletin 61-13, June 19, 1961; Executive Order No. 11093 of February 26, 1963 (28 F.R. 1351; 3 CFR); and Presidential Memorandum of August 21, 1963 (28 F.R. 9413; 3 CFR).

§ 101-35.102 Applicability.

The provisions of this part 101-35 apply to all executive agencies to the extent specified in the Federal Property and Administrative Services Act of 1949, 63 Stat. 377, as amended, or other law, except as provided in this section.

(a) The statement of areas of understanding between the Department of Defense and General Services Administration (15 F.R. 8226) shall govern the applicability of this part 101-35 to the Department of Defense. The statement of understanding between the General Services Administration and the Atomic Energy Commission, dated April 28, 1969, shall govern the applicability of this part 101-35 to the Atomic Energy Commission.

(b) The provisions of this part 101-35 do not apply to the requirements of the following operational telecommunications services and facilities:

(1) Federal Aviation Agency—Facilities used for regulation and protection of air traffic.

(2) National Aeronautics and Space Administration—Missile and satellite tracking facilities.

(3) Veterans Administration—Facilities installed in a hospital complex for biomedical communications.

(4) Bureau of Prisons—Facilities installed in penal or correctional institutions to meet physical security requirements.

(5) Tennessee Valley Authority—Non-common-use facilities peculiar to operation of TVA projects.

(c) GSA will, upon request, furnish the services provided for in this part 101-35—

(1) To executive agencies to which this part 101-35 may be inapplicable or of limited applicability by virtue of this section.

(2) To any other Federal agency, mixed-ownership Government corporation, the District of Columbia, the Senate, the House of Representatives, and the Architect of the Capitol, and any activity under his direction.

§ 101-35.103 Policy.

It is the policy of the Administrator of General Services to:

(a) Provide communications services for executive agencies at the minimum total cost to the Government consistent with requirements for capacity, efficiency of operation, reliability of service, security, and programed activities.

(b) Enter into agreements with other departments and agencies which would permit their operation of special-purpose communications facilities.

§ 101-35.104 Objectives.

The objectives of GSA's communications program are to:

(a) Provide a unified and coordinated Federal telecommunications system within the United States and its insular possessions designed to strengthen the national security posture and to provide economical and efficient telecommunications services for normal and emergency requirements of civil agencies and to fulfill the responsibilities of the Administrator of General Services in the development and implementation of the national communications system.

(b) Establish policies, methods, and procedures and provide guidance for executive agencies to insure efficient and economical procurement and utilization of telecommunications facilities.

Subpart 101-35.3—Utilization and Ordering of Telecommunications Services

§ 101-35.301 General.

The utilization and ordering of telecommunications facilities and services shall be undertaken in accordance with this subpart 101-35.3. Orders for changes or new installations are subject to the provisions of subpart 101-35.2.

§ 101-35.302 General requirements.

(a) *Advance notice.* Plans, service requests, and orders should be submitted as far as possible in advance of date service is desired to allow leadtime for planning and scheduling or work.

(b) *Floor plans.* GSA will notify the requesting agency when floor plans are required in connection with GSA-operated joint-use switchboards. In other cases, the common carrier representative or the agency telecommunications authorities will make appropriate arrangements. Floor plans also may be required in store-forward telegraph grade facility moves and installations.

(c) *Restrictions.* Installations or changes, other than those called for on the order, shall not be made without amending the existing order or preparing a new order. Only authorized employees shall be allowed to install or change telecommunications equipment.

§ 101-35.303 Telephone service.

(a) *Form for ordering service.* Standard Form 145, Order for Telephone Service, and Standard Form 145A, Continuation Sheet—Order for Telephone Service, are prescribed for use by Federal agencies in ordering telephone service from Government joint-use and GSA-operated or GSA-managed switchboards. Federal Government agencies with service from GSA-operated or GSA-managed switchboards forward all requests for telephone service to the serving switchboard. No

other form of ordering procedure shall be used unless it is expressly permitted or authorized by GSA. Agencies may use this form also as the basis for managing their own internal telephone systems.

(b) *Preparation of orders.* Instructions for the preparation of Standard Form 145, Order for Telephone Service, are provided on the flyleaf of each pad of forms. Any necessary supplemental or clarifying instructions will be issued by GSA regional offices.

§ 101–35.304 Changes in telephone listings.

Standard Form 146, Changes in Telephone Listings, shall be used to request changes in telephone listings. It shall be submitted in accordance with instructions on the form.

§ 101–35.305 Telegraph service.

Orders or requests for changes in and new installations or removal of telegraph facilities shall be submitted by letter, memorandum, standard form 145, or appropriate agency purchase order form.

§ 101–35.306 Forms for telegraph messages.

Standard Form 14, Telegraphic Message, is prescribed for use within the United States by executive agencies in preparing official Government telegrams, teletype messages, and other messages for transmission by wire and cable or radio communications facilities. Instructions for the preparation and use of standard form 14 are included as a part of the cited form. Appropriate special forms may be used in lieu of standard form 14 when messages are to be transmitted by facsimile and for certain data messages requiring prearranged format.

§ 101–35.307 Control of telephone station equipment.

§ 101–35.307–1 Agency surveys

Each agency shall establish a program of systematic survey of its installed telephone station equipment. Agencies shall establish internal regulations that require (a) compliance with §§ 101–35.307 and 101–35.308; (b) control of the installation and use of telephone station equipment at all levels of activity to insure that only station equipment necessary to carry out assigned missions is provided; (c) periodic surveys of installed equipment; and (d) correction of any deficiencies found. Agencies were to have conducted the initial survey not later than June 30, 1972. Subsequent reviews shall be made at least annually. Additional surveys shall be made soon after the establishment, reorganization, or major move of any agency or subordinate activity. Copies of agency regulations shall be furnished by the General Services Administration (CP), Washington, D.C. 20405. In addition, each agency shall certify annually to GSA that the required surveys have been conducted.

§ 101–35.307–2 Deviation from standards.

The standards provided in § 101–35.308 are applicable to the ordering of such equipment except where the head of an agency or his authorized designee determines, in writing, that deviation is essential to the effective execution of agency responsibilities or is required by operational needs (to be specified). Orders for equipment deviating from the standards and placed through GSA facilities shall be accompanied by a copy of the written determination. When orders for such equipment are placed directly with commercial common carriers, the determination shall be retained in the agency's file.

§ 101–35.308 Standards and guidelines for determining telephone station requirements.

§ 101–35.308–1 Telephone instruments.

(a) Telephones shall be provided only for employees whose duties require official calls.

(b) One telephone instrument will serve the needs of two or more persons at adjacent desks unless call volume is sufficiently high that sharing would affect operations adversely. In large, open office space where routine functions are performed and only occasional office calls are made or received, each instrument will be shared by as many employees as feasible.

(c) One instrument in an office occupied by only one employee shall be the standard practice unless special operational needs justify an additional instrument.

§ 101–35.308–2 Key stations.

Key stations should be provided only where traffic volume and work methods require an instrument to have access to more than one line and at secretarial locations to permit answering calls for several persons on more than one line. Where a six-button key station will not provide capacity for the required number of lines, key stations of larger capacity (10-button, 6051-type, or Call Director) may be used. The need for this equipment often can be eliminated by limiting the lines appearing on each station or by providing external buttons for inoffice signaling. The type of station to be installed should be selected by determining which equipment will satisfy the need at the least cost.

§ 101–35.308–3 Call Directors.

Call Directors may be provided only when the number of lines required exceeds the capacity of the 12-button strip. Call Directors may be used as a portion of a "package tariff" rate where there is no specific charge for the type of station to be provided.

§ 101–35.303–4 Automatic dialing equipment.

Automatic dialing equipment may be provided when the average number of calls placed each day exceeds 50, and when the same numbers are called on a repetitive basis.

§ 101–35.308–5 Touch-tone instruments.

Touch-tone instruments are prohibited, unless they are (a) provided without additional cost under a general tariff applicable to all instruments associated with the same PBX arrangement, (b) required for a physically handicapped employee to perform his official duties, provided the instrument can be substituted for regular service without modification to the switchboard, or (c) used only as data input devices in a data communications system.

§ 101–35.308–6 Speakerphones.

Speakerphones may be provided where there is frequent need for group participation in telephone conversations or where hands-free answering is essential. Acoustical adaptation may be required to obtain satisfactory results.

§ 101–35.308–7 Primary and secondary lines.

One primary line is adequate for 20 average-length calls made or received each day by an office. Where more than one line is necessary, the use of rotary numbers will provide for a considerable increase in the incoming call-handling capability over the same number of individual, nonrotary lines.

§ 101–35.308–8 Special lines.

(a) Individual business lines may be provided for the reception of an extremely high volume of bulk-type traffic into a central point during seasonal peaks.

(b) Intercommunicating lines, with calls completed by dialing (as with the 20–40 Dial Pak or the 6A dial intercom or other point-to-point intercommunicating systems) should not be provided where the less expensive PBX dial intercommunicating feature is available.

(c) Dial intercommunicating lines should not be used in lieu of manual signal buttons and buzzers and/or intercom lines unless economic or special advantages justify their use.

(d) Intercommunicating lines should be provided only where necessary for the distribution of incoming calls to a group of stations sharing the same lines or between points with an extremely high volume of traffic. Voice intercommunication may be used only where signal buttons and buzzers are incapable of passing adequate information for call distribution.

(e) Automatic ringing private lines (hot lines) may be installed only where, on an emergency use basis, immediate uninterrupted service is essential.

§ 101–35.308–9 Special service and equipment.

(a) Auto-call devices, such as Bell-Boy, may be provided only for use in connection with emergency activities and in unusual operating situations.

(b) Line illumination may be provided where the location or quantity of lines or instruments preclude discernment of distinctive audible signals on incoming calls or visual observation of line availability on outgoing calls. Illumination normally is not required on installations of only two lines appearing on a few

telephones located in the same room. Where only visual identication of incoming calls is required, the flashing "line lamp" illumination should suffice. For those cases where it is necessary to visually identify a busy line, the steady "busy lamp" illumination may be required. If both types of visual indication are required, then both the line and "busy lamp" illumination may be required.

(c) The use of "wink-hold" illumination is prohibited, where any additional costs are involved, unless special requirements justify the additional cost.

(d) Hold buttons should be installed only where there is a valid need. They should not automatically be provided on all key system instruments that terminate more than one line.

(e) Automatic answering devices should be installed only when there is a valid need to leave a message when the telephone is unattended.

(f) Installation of listening-in circuits, transmitter cutoff switches, and other devices for recording and listening to telephone conversations is prohibited.

(g) Color telephones are permitted where required to identify emergency or security telephone lines or where instruments may be installed without an additional charge for such instruments.

(h) Whenever any special type of installation is planned, review should be made of aggregate charges for items making up the total cost of the installation and compared with the actual need for each item. The Commissioner, Automated Data and Telecommunications Service, will assist agencies in implementing programs.

§ 101–35.309 FTS intercity voice network identification symbols.

§ 101–35.309–1 General.

Each Federal agency authorized to use the network will be assigned FTS identification symbols by the Automated Data and Telecommunications Service in the GSA Central Office or appropriate regional office. Use of FTS identification symbols enables GSA to obtain traffic information, allows FTS operators to efficiently control network usage, and insures completion of official long-distance telephone calls with minimum delay. At the beginning of each fiscal year GSA will revise these symbols to assist agencies in insuring that only authorized personnel are in possession of them. GSA also will cancel and revise specific agency symbols at other times upon request to avoid possible misuse. No calls to or from commercial telephones will be accepted unless the caller furnishes his name, proper FTS identification symbols, and 10-digit telephone number to the FTS operator, GSA may revise the symbols during the year.

* * * * * * *

Mr. MOORHEAD. Mr. Phillips.

Mr. PHILLIPS. Just one last question.

Does GSA make a determination on its own as to whether the reasons given in the request for deviation are proper, or do you just take the agency's word that they need this deviation for their own operational purposes?

Mr. BURTON. We accept the agency's determination that it is required for their mission.

Mr. PHILLIPS. Do you ever check to see if it is abused?

Mr. BURTON. To my knowledge, we do not, sir. We do not act as policemen.

Mr. PHILLIPS. Thank you, sir.

Mr. MOORHEAD. Mr. Stettner?

Mr. STETTNER. Thank you, sir.

From information previously furnished to us by your agency, Mr. Burton, we find that recent internal checks you made indicate that certain types of listening-in equipment shown on telephone company records are shown differently on your records. GSA is in fact being billed for equipment shown on telephone company records that does not exist in your agency. There are enough discrepancies noted to assume somebody will make a further check to reconcile these differences. That is for your own agency.

Is anybody going to address themselves to the same problem, Governmentwide, or at least metropolitan areawide? Would it be a responsibility of GSA?

Mr. BURTON. No, sir, that is not our responsibility.

Mr. STETTNER. Are you going to assume that all other agencies will be doing it of their own initiative?

Mr. BURTON. I would assume certainly those agencies that come before this committee are going to check them. Whether they are all going to check them or not, Mr. Stettner, I do not know.

Mr. STETTNER. We have found that some agencies appear to be paying for service that they are not getting from the telephone company and that they have been doing so over relatively long periods of time.

Mr. BURTON. Mr. Stettner, as a practical matter, I think all agencies continue to check their telephone bills because it is a severe problem. Telephones are constantly being changed, things are added, things are deleted. It is an extremely fluid situation, and it is a very detailed laborious task that as far as I know most agencies are doing constantly. It is true that we do have difficulty, every large user of telephone service has difficulty reconciling his telephone bill.

Mr. STETTNER. Mr. Chairman, I have just one other question.

I am struck by the contradiction that we have Federal agencies who are paying for devices to listen in and these same Federal agencies are paying for other devices to exclude people from listening in. I wonder whether there is any better justification for incurring costs to exclude people from listening in than there is to listen in?

Mr. BURTON. I would say that to exclude people from listening in is certainly important, and that we are all aware of the importance and it is in the forefront of our attention. With reference to the transmitter cutoff devices that are used to take notes from, apparently the people who use those feel that it is important to have a record of the conversation. Did I answer your question, Mr. Stettner?

Mr. STETTNER. Partially.

Mr. MOORHEAD. Mr. Kronfeld?

Mr. KRONFELD. Does GSA consider the use of a transmitter cutoff device for the purpose of allowing the secretary within a single office, or unit of offices, to take notes or to monitor a conversation for the purpose of taking down data, a monitoring device under the terms that you have discussed this morning that would require a deviation?

Mr. BURTON. Yes, sir.

Mr. KRONFELD. You would?

Mr. BURTON. Yes, sir.

Mr. KRONFELD. Even though the agency did not use such devices for the purpose of sampling or monitoring service as such?

Mr. BURTON. Yes; a deviation is required.

Mr. KRONFELD. Okay, because that is what I understand to be the purpose of these devices within the Department of State, so, therefore, even though they are not used for broad monitoring or service observing, they would still come within your regulations if State was not excluded under another section of the code?

Mr. BURTON. Yes, sir.

Mr. KRONFELD. Thank you.

Mr. MOORHEAD. Mr. Cornish?

Mr. CORNISH. Thank you, Mr. Chairman.

Mr. Burton, GSA has given authority to certain agencies to use these listening-in devices under certain conditions, and one of those conditions, according to your testimony, is that the agency employees of that particular agency are to be made aware of the fact that their conversations may be monitored. Now, what provision is there, if any, to make certain that the citizen is advised that the conversation may be monitored, or is it only the Federal employee?

Mr. BURTON. The regulations cover only the Federal employee.

Mr. CORNISH. So the citizen has no notice or understanding of that at all?

Mr. BURTON. That is correct.

Mr. CORNISH. I noticed that recently you had a service-observing device in connection with your Federal Information Center in Washington, and that it was recently discontinued. Why was that action taken?

Mr. BURTON. It was determined that the device was no longer needed in that center.

Mr. CORNISH. Was it needed in the first instance, and why?

Mr. BURTON. Well, that device is a normal regular service observing part of the basic equipment. The basic equipment comes with that as an integral part of the system. It is commonly used by the telephone companies and the people at the center felt they needed that to monitor handling of those calls by the operator for training and service evaluation. The Federal Information Center was a brand-new service when the equipment was installed.

Mr. CORNISH. Do you not think it might be wise that when ordering this equipment where the special observing feature comes in automatically that you ask the providers of that equipment to exclude that particular feature?

Mr. BURTON. Yes, sir, when it is not needed, I would think that would be advisable.

Mr. CORNISH. Thank you, Mr. Chairman.

Mr. MOORHEAD. Mr. Erlenborn?

Mr. ERLENBORN. No questions.

Mr. MOORHEAD. Mr. Alexander?

Mr. ALEXANDER. No questions.

Mr. MOORHEAD. Thank you very much, Mr. Burton. We appreciate your very helpful testimony and we look forward to hearing from Mr. Plotkin and Ms. Latimer on the discrepancies in the list between your testimony and that list.

We appreciate your being with us. Thank you very much.

[Questions submitted to GSA and the replies follow:]

QUESTIONS AND ANSWERS FOR THE GENERAL SERVICES ADMINISTRATION PERTAINING TO THE JUNE 13, 1974, SUBCOMMITTEE HEARING ON TELEPHONE MONITORING AND OTHER SURVEILLANCE PRACTICES

Question 1. As the agency having responsibility for telecommunications services, Government-wide, do you perceive that responsibility to include critical evaluation of agencies' requests for installation of listening-in circuits, transmitter cutoff switches, and other devices for recording and listening to telephone conversations which normally are prohibited by FPMR 101–35.308–9(f)?

Answer. FPMR 101–35 concerning telecommunications and public utilities normally prohibits the installation of the devices in question, but the head of an agency or his authorized designee can determine that a deviation is essential to the effective execution of agency responsibilities or is required by operational needs. The General Services Administration does not have the authority to question an agency's determination that particular communication devices are required for its program activities. (See section 201 of the Federal Property and Administrative Services Act of 1949, 63 Stat. 383, as amended, 40 U.S.C. 481).

Question 2. FPMR 101–35.307–2 provides for deviations from the general prohibition against installation of such devices. When agencies contract for their telephone service directly from the operating telephone company, rather than through General Services, how frequently does the General Services Administration review the special justifications which agencies are required to keep in their files?

Answer. GSA does not review the special justifications that agencies are required to keep in their files under the FPMR. These determinations are retained in the agency's file and would be available for review.

Question 3. Is it reasonable to expect a review of the statements of special justifications for such devices at some periodic interval and a periodic revalidation of the operational need?

Answer. We believe it is reasonable that the special justifications and operating needs for listening-in and monitoring devices be reviewed by the agency on an annual basis. Our implementing regulation FPMR 101–35.307 and 307–1 presently requires agencies to establish such periodic surveys. (See p. 236.)

Question 4. Should such revalidations be made annually, and should they be made by the agencies themselves or by GSA?

Answer. As indicated in question 3, we do believe the justification for the devices should be reviewed at least annually by the agencies. Such review should be made by the agencies themselves, as is now required under FPMR 101–35.307, but should be conducted by an audit or non-operating element rather than the operating element which has justified the listening-in or monitoring device.

Question 5. Could the requirement for such review and evaluation be imposed by revisions to the F.P.M.R. 101–35.307–2 with a further requirement for summary reporting by GSA or OTP to responsible congressional committees?

Answer. As indicated in our answers to questions 3 and 4, FPMR 101–35.307 and 307–1 requires agencies to survey the continuing need for any special communication equipment including listening-in circuits, transmitter cutoff switches, and other devices for recording and listening to telephone conversations, and to certify annually to GSA that the required surveys have been conducted. Copies of such agency surveys could be available to the respective congressional committees or OTP upon request, but we do not see a need for required summary reporting.

Question 6. Is the General Services Administration now considering or will it consider amending the F.P.M.R. to accomplish this?

Answer. We would only consider amendments to the FPMR in view of our answers to questions 3 through 5.

Question 7. Delegations of authority to approve the installation of such devices may be made by agency heads, according to the F.P.M.R. The General Services Administration internal directive restricts the level of delegation to the Director of the appropriate regional Management Services Division. What level of authority in the Washington Central Office is currently approving requests for such devices?

Answer. Normally, the level of authority for approving requests for telephone equipment for the GSA Central Office in Washington is the Director of Management Services for the GSA Region 3—Washington, D.C., Virginia, Maryland, West Virginia, and Pennsylvania. However, since listening-in, cutoff, and monitoring devices have been considered sensitive items within GSA, in each instance where GSA itself has required such devices, approval for such deviations has been made by the Administrator of General Services. This referral for approval to the Administrator is in accordance with existing limitations on delegated authority.

Question 8. Information furnished June 7, 1974, by GSA compares the telephone company equipment listing with the General Services Administration physical inventory identification of the 271 devices originally identified to the subcommittee as transmitter cutoff switches. We note a number of disparities as well as a number of instances where your agency's search showed that the device was nonexistent. Presumably, the telephone company is charging for these items shown on its records. What steps have been taken to insure that the telephone company's charges are corrected so that payment is made only for those devices

still installed, and then only at the proper rate for the device found by an agency's physical inventory?

Answer. GSA has initiated an automated telephone inventory and accounting system. This system permits a monthly review of the telephone equipment installed at our GSA switchboards and any disparities are corrected with the appropriate telephone company. We are currently in the process of implementing the system in the Washington metropolitan area, and this will complete its implementation throughout the country. We believe that with the use of this automated telephone inventory and accounting system agencies are in a position to quickly identify discrepancies. GSA will adjust any billing discrepancies with the appropriate telephone company and agency.

Question 9. From other inquiries by the staff, we have learned of other agencies having similar discrepancies between service they think they have—from their records—and the actual service available from their instruments. What operating procedures exist to minimize these differences, and is this matter periodically reviewed by the GSA?

Answer. As indicated in question 8, copies of our telephone inventory and accounting system bills are presented to the agencies on a monthly basis. Any differences should be called to the attention of GSA at that time by the agency so any discrepancies can be reconciled with the telephone company.

Question 10. The subcommittee is struck by the inherent inconsistency of Federal agencies paying moneys to monitor or listen in and, also, in other circumstances paying moneys for exclusion devices to prevent individuals from listening in. What is the normal operating or environmental situation for the use of such exclusion devices, and is there any better justification for them than for the highly questionable listening-in devices?

Answer. In this age of call directors, extension telephones, and other telephone equipment, the possibility of any telephone conversation being overheard by others having access to the line exists. Given this normal operating environment, where there is a need to insure that an official's telephone conversation be absolutely private, an expenditure for special exclusion equipment is justified. We believe that this is consistent with the overall position and policy that listening in and monitoring of telephone conversations should not be allowed. Exclusion devices which insure privacy support this policy.

Question 11. The three agencies—IRS, VA, and SSA—granted deviations by the GSA for installation of listening-in devices all operate teleservice centers. Is notification to the GSA needed only in those situations where service observing equipment is installed in that type of configuration, or is it needed, as well, when agencies request installation of transmitter cutoffs, listening-in circuits, and similar devices?

Answer. The agencies are required under the existing FPMR to notify GSA in not only those situations where service observation equipment is installed, but also in those cases where transmitter cutoffs, listening-in circuits, and similar devices are required and are to be provided for through GSA facilities. Where the agency procures these devices directly from the telephone company and not through GSA facilities, we do not have to be advised, but the proper written justification is required to be retained in their file.

Question 12. Since other agencies in the Metropolitan Washington, D.C., area are currently using such equipment items, have they had them installed without prior review of their justification statements by the GSA? If so, what steps are being taken to correct this situation?

Answer. A number of agencies have listening-in and monitoring devices installed on GSA facilities without the required justification being on file with GSA. We are taking our October 1973 telephone inventory list and forwarding it to each concerned agency, requesting that they make a physical review and ascertain whether these devices actually exist. Should the agencies desire to continue the use of devices presently in existence, then we will require the appropriate written justification. However, where the devices exist and the agencies do not desire to continue their use, we will have them removed. Where the devices do not exist at all, after the physical inventory, we will correct our basic inventory lists and make the appropriate billing adjustment with the telephone company and affected agency. We estimate that this physical review by the agencies will require approximately 45 days.

Mr. MOORHEAD. The subcommittee would now like to hear from three witnesses. We will ask all three to come forward: Mr. David O. Cooke, Deputy Assistant Secretary, Office of the Comptroller, Department of Defense, who is an old friend who has appeared before this subcommittee on many occasions; Mr. David R. Macdonald, Assistant Secretary for Enforcement, Operations and Tariff Affairs, Department of the Treasury; and Phillip J. Budd, Chief Data Management Director, Veterans' Administration.

While you are standing, do you solemnly swear the testimony you are about to give, this testimony will be the truth, the whole truth and nothing but the truth so help you God?

Mr. COOKE. I do.

Mr. MACDONALD. I do.

Mr. BUDD. I do.

Mr. MOORHEAD. Thank you very much, gentlemen.

Please be seated.

Welcome to the subcommittee. We will start with Mr. Cooke who is so familiar with the members of this subcommittee, he must feel at home here and his example might make the other two witnesses feel at home.

Mr. Cooke?

STATEMENT OF DAVID O. COOKE, DEPUTY ASSISTANT SECRETARY, OFFICE OF THE COMPTROLLER, DEPARTMENT OF DEFENSE; ACCOMPANIED BY DANIEL SHEERIN OF THE U.S. AIR FORCE

Mr. COOKE. Indeed I do, Mr. Chairman. It is a pleasure to be up here before you again.

My statement that you have before you covers not only, as you know, telephone monitoring, which seems to be the prime area of the subcommittee's concern this morning, but in the interest of complete coverage, I have also included our policies under a separate directive relating to electronic surveillance and wiretap in relation to criminal investigations. With your permission, sir, although I am certainly available to answer questions on the complete statement, I would like to summarize the points on the telephone monitoring, because as you pointed out, your concern is the monitoring of telephones in the day-to-day business of the Federal Government.

Mr. MOORHEAD. Well, we appreciate that, Mr. Cooke. If you will highlight your testimony and without objection the full statement, together with the attachments thereto will be made a part of the record.

[The documents referred to follow:]

PREPARED STATEMENT OF DAVID O. COOKE, DEPUTY ASSISTANT SECRETARY, OFFICE OF THE COMPTROLLER, DEPARTMENT OF DEFENSE

Mr. Chairman and members of the committee, I am here in response to your invitation to the Secretary of Defense to provide information in connection with your inquiry into the current policies and practices of Federal agencies relative to telephone monitoring and other surveillance practices, and your further inquiry into the body of knowledge about the current technology of monitoring equipment and future trends in this area.

We have made available for the record our detailed statistical sheet, together with new issuances for the period July 1, 1973, through March 31, 1974. If you have technical questions with respect to telephone monitoring, I have available Mr. Daniel Sheerin from the U.S. Air Force.

For management purposes, the Department has placed telephone monitoring and electronic surveillance activities into two separate categories.

Departmental policies and procedures which limit the use of telephone monitoring and control the use of information obtained by third parties, are set forth

in Department of Defense Directive 4640.1, "Telephone Monitoring." DOD policies which restrict the use of wiretapping and eavesdropping during the conduct of investigations for law enforcement purposes are published in DOD Directive 5200.24. "Telephone Interception and Eavesdropping." Both of these directives apply to the United States, the Commonwealth of Puerto Rico and U.S. territories. They do not apply elsewhere overseas, nor are they applicable to our foreign intelligence collection activities. Copies of the two directives were provided to your committee with our report to the General Accounting Office.

First, I would like to discuss telephone monitoring which is administrative rather than investigative in purpose. There are four classes of telephone monitoring. They are:

Office Telephone.—Listening to or recording office telephone communications by use of mechanical or electronic devices or recording by written means, for the purpose of obtaining an exact reproduction or a summary of the substance of the telephone conversation and with the consent of all parties.

Command Center Communications.—Listening to or recording telephone communications in DOD command centers for the purpose of obtaining a record of conversations, or parts thereof, for command and control purposes.

Communications Security.—Listening to or recording of the transmission of official defense information over DOD-owned or leased telephone communications, by any means, for the purpose of determining whether such information is being properly protected in the interest of national security. Notice of this action is given to users that these systems are subject to communications security monitoring at all times.

Communications Management.—Listening to or recording telephone communications on DOD-dedicated systems or the common-user systems of the Defense Communications Systems, by any means, not for the contents but for the purpose of determining whether the systems are functioning properly for official purposes. Almost every phone company has a counterpart activity.

The first class of telephone monitoring is one in which you are all familiar, called office monitoring. With the use of either a recorder equipped with "beeper" or with a stenographer, it requires the advance consent of all parties to the conversation. Office telephone monitoring, in such cases, is a valuable management tool to reflect the exact nature of agreements and understandings achieved by telephone. One of the parties to the conversation may be outside the DOD, but again, let me emphasize that all parties concerned must consent to office telephone monitoring.

The other three classes of telephone monitoring are largely internal. That is, they are directed to the manner in which DOD military and civilian personnel use telephones which are part of DOD communications systems.

Telephone monitoring in command centers, for communications security and for communications management purposes, does not require express consent in each case. The purpose of command center monitoring is to obtain accurate records for command and control purposes of official calls to a command center. Examples of the command centers are the National Military Command Center, its alternate, the Airborne Command Post, the North American Air Defense Command Post, the Military Services Operations Centers in Washington, the Military and Security Policy Operations Centers, Fire and Rescue Control Centers and Air Traffic Control Centers.

DOD monitoring for these centers closely compares with the recordings made by the Federal Aviation Agency in its many air traffic control centers. Similarly, most police, fire, and rescue control centers in our large cities and counties monitor incident reports and requests for assistance to insure accuracy and for record purposes. Furthermore, command centers are able to record messages to be rebroadcast to subordinate and lateral units.

DOD Directive 4640.1 requires for each center specific regulations be published prior to the initial operation of the recording equipment. The existence of such monitoring, however, is required by DOD Directive 4640.1 to be widely and expressly publicized throughout DOD and its components as to amount to constructive consent.

Our authority for this class of monitoring equipment and its use stems from communications common carrier tariffs which have been approved by the Federal Communications Commission. This class of monitoring is provided for in DOD Directive 4640.1, which I mentioned earlier.

Communications security telephone monitoring is the third class of administrative telephone monitoring which is used, albeit rarely, on Department of Defense telephone circuits. The purpose of Comsec monitoring is to provide a

basis for analysis of the vulnerability of telephone communications to hostile intelligence exploitation, and for determining the best means by which such vulnerabilities may be reduced or eliminated.

This monitoring may only be conducted when authorized by the commander or DOD official in charge of an installation or activity or his superior. Let me stress that security organizations organized and equipped to perform communications security monitoring are not authorized to monitor communications systems on their own initiative. Communications telephone security monitoring is employed infrequently. Less than 1 percent of our telephones are monitored for security in any given year.

The lines selected for security monitoring consist mainly of command posts, major operational headquarters, war rooms, and field exercises both in the United States and overseas.

Let me emphasize that the purpose of Comsec telephone monitoring is to advise commanders on actual or possible security compromises and improve the security protection of telephone communications.

DOD 4640.1 expressly states that the information obtained as a result of telephone communications security monitoring shall not be authorized for law enforcement purposes unless the General Counsel authorizes an exception in a specific case.

The last class of administrative telephone monitoring is communications management monitoring, often called service observation. Service observation is conducted largely by computer analysis and peg count methods rather than by actual listening to telephone conversations in progress.

It is a tool used to determine if telephone systems are functioning properly, not with the contents of conversations, but with such things as the precedence and number of calls, their duration, response to signals, number of busy signals for a given time period, and total load on a system.

The purpose of administrative telephone monitoring previously described is distinctly different from the purpose of wiretapping or eavesdropping. Telephone monitoring is to accurately preserve records of conversations as in command centers or to analyze a total system for adherence to protection of classified information as in Comsec monitoring.

Within your term "electronic interception and surveillance," we include our investigative techniques of telephone interception and eavesdropping, often referred to as "wiretapping" and "bugging."

Let me now turn to the Department's policies and procedures for telephone interception and eavesdropping techniques exactly as they are defined in title III of Public Law 90–351:

Telephone interception (wiretapping). The use of electronic, mechanical, or other devices to intercept a wire communication for the purpose of obtaining information as part of a criminal investigation.

Eavesdropping (electronic surveillance). The use of electronic, mechanical, or other devices to intercept an oral communication for the purpose of obtaining information as part of a criminal investigation.

Directive 5200.24 authorizes under controlled circumstances the use of telephone interception (or wiretapping) and non-telephonic electronic surveillance (eavesdropping) by DOD criminal and investigative agencies when there are reasonable grounds to believe that:

1. A criminal offense concerning the national security is involved; or
2. A felony has been or is about to be committed; or
3. Telephone calls involving obscenity, harassment, extortion, bribery, or threat of bodily harm have been made to a subscriber-user on a military base.

Wiretap and eavesdrop operations conducted by DOD are in full compliance with the policies and requirements established by the Attorney General and issued pursuant to 18 United States Code, Chapter 119.

Let me stress most strongly that the DOD is not in the business of conducting electronic surveillance of U.S. citizens not affiliated with the Department. DOD Directive 5200.27 expressly forbids such practices except in narrowly defined circumstances. In other words, the wiretaps or eavesdrops DOD conducts are employed only in cases involving military or, in extremely rare cases, DOD civilian personnel provided the FBI has yielded jurisdiction.

The procedures I am about to describe are those instituted by the Attorney General for consensual wiretaps and eavesdrops, in the United States and its territories. That is, at least one party has consented. All nonconsensual cases, should any arise, must be referred to the Attorney General. None has arisen in

DOD. The procedures I am about to describe are those instituted by the Attorney General for consensual wiretaps and eavesdrops, in the United States and its territories. That is, at least one party has consented. All nonconsensual cases, should any arise, must be referred to the Attorney General. None has arisen in DOD since the passage of Public Law 90–351 in 1968.

Under the Attorney General's procedures and the provisions of DOD Directive 5200.24, consensual wiretaps may be authorized by heads of DOD components or their designees for the investigation of criminal cases and harassing telephone calls. DOD components have issued regulations setting forth procedures and controls for these authorizations.

The Attorney General has adopted stricter rules in the case of eavesdrops. For consensual eavesdropping of nontelephonic conversations, prior approval normally must be obtained from the Department of Justice. Again, DOD Directive 5200.24 provides first that the head of the DOD component concerned, or his designee, must approve the proposed eavesdrop. Then it must be approved by the DASD(A) before it is sent to the Attorney General requesting his approval. Attorney General regulations provide for emergency monitoring in advance of his approval to prevent the imminent loss of essential evidence. In such cases, a full report of justification must be provided to him.

Each request for approval of proposed wiretapping or eavesdropping must contain a detailed statement as to the crimes and persons involved and a statement that the consent of one party has been obtained with his identity. All approvals are limited to 30 days, as are any renewals.

DOD Directive 5200.24 provides careful safeguards both as to the integrity of equipment and any information obtained by their use.

The wiretapping and eavesdropping devices are carefully accounted for and stored under secure conditions by the investigative agencies of our military departments. Both categories of electronic devices are only authorized for use in approved cases under the supervision of experienced agents who have been instructed in the legal and private rights aspects of their use.

With respect to the information that might be received by wiretapping or eavesdropping activities, DOD Directive 5200.24 requires that it be stored in appropriate investigative files at a central location; that the information so stored is always identified, when used for any purpose, as information which was obtained by wiretapping or eavesdropping; that access to information so stored is strictly controlled and recorded; and that this information shall not be disclosed outside of the Department of Defense unless the head of the DOD component concerned determines that disclosure is essential to governmental operations.

Finally, the directive requires quarterly reports to the Secretary of Defense concerning the employment of wiretaps and eavesdrops, including those conducted in areas of the world where the substantive provisions of the directive do not apply. We also have an annual summary and electronic equipment report to make to the Attorney General.

In recent years, wiretapping has shown an increase in cases involving telephonic bomb threats or other harassing calls. Eavesdropping activities have shown a marked increase over the last several years attributable almost completely to the narcotics and drug problem.

Consensual intercepts, particularly eavesdrops, have contributed significantly to our success in drug cases. However, because of the type and short duration of the calls, we have been only moderately successful in identifying the callers in bomb threats and similar cases. Both wiretapping and eavesdropping are essential elements in the DOD law enforcement program.

Mr. Chairman, I have appreciated the opportunity you have afforded the DOD to describe its policies and practices in the area of electronic surveillance. We realize that this is an area of balancing the rights of the individual on one hand and the legitimate needs of an organized society on the other. We believe our directives are not only in full compliance with the law and the Attorney General's regulation but also have achieved that balance.

DEPARTMENT OF DEFENSE AGENCYWIDE COMPILATION OF THE COMPONENT REPLIES TO CONGRESSMAN MOORHEAD'S LETTER OF MAY 14, 1974, CONCERNING MONITORING, AND ORAL AND WIRE INTERCEPTION EQUIPMENTS 1ST 3 QUARTERS FISCAL YEAR 1974

Questionnaire items	Army	Navy	USMC	Air Force	OSD	DIS	DCA	NSA	DIA	DSA	OJCS	Defense Telephone Service (Washington)[1]	Total events and equipment lists	Total money (costs)
1. Number of transmitter cutoff switches (including push-to-talk features) in use on component phones	1,249	(2)	100	13,271	[3] 453	0	1	312	198	0	173	1,098	16,855	
2. Total rental or other charge for above cutoff and push-to-talk switches	$4,067.10	(2)	(4)	[5] $39,434	[6] $4,336.50	0	$3.15	$4,224	0	0	$1,350	$4,311.08		$57,725.83
3. Number of listening-in circuits installed on telephone equipment assigned to component	75	(2)	0	1,721	0	0	0	0	0	0	39	0	1,835	
4. Total rental or other cost for above listening-in circuits	$263.35	(2)	0	[7] $5,183	0	0	0	(2)	0	0	$5,000	0		$10,446.35
5. Number of telephone recording devices in use in component	698	(2)	6	679	[8] 6	2	0	3	0	2	58	12	1,466	
6. Number of recorders wired into telephone circuits	161	(2)	3	679	[9] 7	2	0	3	0	0	58		913	
7. How many recorders in question 6 are equipped with a beeper or other automatic tone signal?	82	(2)	0	312	[8] 6	2	0	3	0	2	58	0	465	
8. Number of induction devices that can be used with dictating machines to record phone conversations	87	0	18	0	0	0	0	0	0	0	1	0	106	
9. Number of other devices that can be used to monitor/record phone conversations	85	(2)	(2)	14	[10] 25	0	0	0	3	0	0	0	127	
10. How many devices in question 9 are equipped with a beeper or other automatic tone signal?	1	(2)	(2)	0	0	0	0	(2)	3	(2)	0	0	4	
11. Total cost of recorders in questions 6 and 7 and their related attachments	$64,051.00	(2)	$5,000	$364,310	[11] $1,665	$271	0	$1,950	0	$110	$240,000	$942	$678,299.60	
12. Total cost of induction devices in question 8	$2,361.00	0	(12)	0	0	0	0	(2)	$478	0	$1,210	0	$3,571.00	
13. Total cost of other devices in question 9	$21,057.50	(2)	(12)	$4,097	[14] $7,662.50	0	0	(2)	1	0	0	0	$33,295.00	
14. Number of telephone service observing devices in use in component	13	0	0	[15] 320	0	0	(2)	1	0	0	0	0	334	
15. Total purchase cost or leasing charges for equipment in question 14	$330.00	0	(2)	(2)	0	0	$4,278.80	0	0	0	0	0		$4,608.80
16. Number of nontelephonic "bugging" or "eavesdropping" devices in component	615	223	(2)	26	[16] 11	0	0	0	0	0	0	0	875	

Footnotes at end table.

DEPARTMENT OF DEFENSE AGENCYWIDE COMPILATION OF THE COMPONENT REPLIES TO CONGRESSMAN MOORHEAD'S LETTER OF MAY 14, 1974, CONCERNING MONITORING, AND ORAL AND WIRE INTERCEPTION EQUIPMENTS 1ST 3 QUARTERS FISCAL YEAR 1974—Continued

Questionnaire items	Army	Navy	USMC	Air Force	OSD	DIS	DCA	NSA	DIA	DSA	OJCS	Defense Telephone Service (Washington)[1]	Total events and equipment lists	Total money (costs)
17. Total cost nontelephonic "bugging" or "eavesdropping" devices in question 16	$114,068.00	$42,020	$4,000	$22,495	[16] $2,340.00	0	0	(2)	0	0	0	0	----------	$184,923.00
Total														$1,429,140.18

[1] DTS (Washington) serves all DOD elements in National Capital region.
[2] Not available.
[3] I. & L., 1; DNA, 436; DNA, 11; M. & R. A. 5.
[4] USMC owned.
[5] $52,578 projected for year.
[6] DMA, $3,627; DNA; $687; M. & R. A., $22.50
[7] $6,910 projected for year.
[8] DCAA.
[9] DCAA, 6; M. & R. A., 1.
[10] DNA, 19; M. & R. A., 6.
[11] DCAA, $1,305; M. & R. A., $360.
[12] Unknown, old equipment.
[13] Unknown.
[14] DNA, $7,631; M. & R. A., $31.50.
[15] Chief operator/supervisor console positions.
[16] DNA.

DEPARTMENT OF ARMY PENTAGON TELECOMMUNICATIONS CENTER

Subject: Recording telephone communications at MP operations desks.

1. Ref. A provides guidance governing wiretap, investigative monitoring eavesdrop activities by DA personnel engaged in conduct of criminal or national security investigations. Ref. B, chapter 10, prescribes policy and procedures covering office telephone monitoring and communications management monitoring. Ref. C prescribes policy and procedures covering telephone monitoring for communications security purposes. Ref. D prescribes policy and procedures for monitoring telephone communications in DA Command and Control System (DACCS) Operations Center.

2. Policies and procedures contained in cited references do not specifically include definitive guidance to be applied to Command Center Communications monitoring which includes police and similar operations centers where recording of emergency telephone calls is needed for command, operational, or record purposes.

3. Recording telephone communications at MP operations desks is considered to be a form of command center communication monitoring which may be conducted to provide an uncontroverted record of emergency communications. This includes reports of emergency, analysis of reported information, records of instructions, such as commands issued, warnings received, requests for assistance, and instructions as to location of serious incident.

4. Until other regulatory policy is established, the following procedures are applicable, on an interim basis, in recording emergency telephone and/or radio communications conducted at MP operations desks within the 50 United States, District of Columbia, commonwealth of Puerto Rico, Canal Zone, and Guam.

A. Only those conversations described in para. 3, above will be recorded.

B. All telephones connected to recording equipment will be conspiciously marked "for official use only—connected to recording device" and access to use will be restricted to military police operations desk personnel.

C. Connection of voice-recording equipment with the telecommunications network or private-line service arranged for connection with telecommunications network will be performed IAW applicable telephone company tariffs which permit direct electrical connection through telephone company recorder-connector equipment. Installation of recorder-connector equipment automatic tone device is authorized.

D. Official telephone numbers for MP desk will be listed in appropriate command, activity, or installation telephone directory with statement that emergency conversations will be recorded for accuracy of record purposes. Other forms of prewarning, to include audible warning tones, are not required.

E. Recordings which contain conversations as described in para. 3 above may be used in lieu of written entries in the MP radio log (DA form 1943) and will be retained for a period of 60 days. Transcripts may be made for permanent files, as appropriate.

F. Recording telephone communications or radio transmissions by MP personnel, for other than emergency purposes at cited in para. 3, will be governed by applicable references.

G. Installation/activity commanders will issue written authorization certifying that recording emergency telephone communications will be performed exclusively for purposes as cited in para. 3. Letter of authorization will contain specific authority for type of equipment to be used and a statement limiting recordings to calls associated with an emergency situation. One copy of the authorization will be forwarded to HQDA (DAPM–PLO), Forrestal, Washington, D.C. 20314.

5. Recording telephone communications at MP operations desks outside those geographical areas defined in para. 4 above, will, in addition to instructions contained herein, be conducted within restrictions contained in international agreements between the United States and host countries.

6. Prior to implementation of policy contained herein local public announcement will be disseminated which describes installation of equipment and procedures for recording telephone communications at MP operations desks.

7. Expiration date of Alaract MSG December 1, 1974.

Subject: Army regulation 381–17, wiretap, investigative monitoring, and eavesdrop activities.

A. DA MSG 262311Z July, Subj as above.
1. Ref. A is changed as follows:
Refix text of paragraph 14f with: "Oconus."
2. Any Army investigative agency within the 50 United States, U.S. territories or possessions who may have exercised the exception stated in para. 14f, ref. A, during the period from July 26, 1973 to date of receipt of this change will report each such case to Hqda/dami-doi-s/immediately.

Subject: AR 381–17, wiretap, investigative monitoring and eavesdrop activities.
A. Paragraph 3. Add:
L. 519th MI BN (FA), which may acquire, possess or use such equipment only for training purposes when all persons involved are DOD affiliated and all are aware of the planned utilization of such equipment during the training exercise or as provided for in paragraph 14g.
M. U.S. Army Special Forces units organized under TOE 31–126H which may acquire, possess or use such equipment as authorized by affiliated and all are aware of the planned utilization of such equipment during the training exercise or as provided for in paragraph 14g.
B. Paragraph 14. Add:
C. Wiretapping, investigative monitoring and eavesdrop activities directed against a hostile force by units conducting or supporting actual combat or combat-related operations.

DEPARTMENT OF DEFENSE,
Washington, D.C., November 20, 1973.

(DIS Regulation 17–1)

COMMUNICATIONS—TELEPHONE MONITORING

1. Purpose: This regulation sets forth DOD and DIS policy and procedures concerning telephone recording devices and monitoring of telephone calls.
2. References:
(*a*) DOD Directive 4640.1, "Telephone Monitoring."
(*b*) DOD Directive 5200.24, "Telephone Interception and Eavesdropping."
3. Definitions:
(*a*) Office telephone monitoring. Listening to or recording office telephone communications by use of mechanical or electronic devices or recording by written means, for the purpose of obtaining an exact reproduction or a summary of the substance of the telephone conversation.
(*b*) Command center communications. Listening to or recording telephone communications in DOD command centers for the purpose of obtaining a record of conversations, or parts thereof, for command purposes.
(*c*) Communications security. Listening to or recording the transmission of official defense information over DOD owned or leased telephone communications, by any means, for the purpose of determining whether such information is being properly protected in the interest of national security.
(*d*) Communications management. Listening to or recording telephone communications on DOD-dedicated systems or the common-user systems of the Defense Communications System, or any means, for the purpose of determining whether the systems are functioning properly or being used for other than official purposes.
4. Monitoring policy and procedure:
(*a*) Monitoring
(1) General. Except as provided in the regulation there shall be no monitoring of telephone conversations. This does not preclude written notes being taken by parties of a telephone conversation.
(2) Office telephone monitoring devices and procedures.

(*a*) Secretarial personnel are advised that no telephone calls are to be monitored without explicit, affirmative instructions for each specific call.
(*b*) Telephone terminals connected to commercial circuits.
1. When recording of a telephone conversation is desired by a party to the conversation, the other parties must be informed that the conversation is to be monitored, and all parties must give consent prior to the monitoring.
2. The use of recording devices may be authorized by the Director of the Defense Investigative Service only when there is a specific requirement for exact reproduction of telephone conversations; and
3. When recording devices are authorized, they shall be equipped with recorder connectors containing instruments which automatically emit a distinct warning tone repeated at intervals of from 12 to 18 seconds. The use of the warning tone shall be in addition to the requirement for prior consent by all parties participating.
4. Induction-type recording devices shall not be used.
(*b*) Command center monitoring. Reference (*a*) provides that in command centers such as, but not limited to, the National Military Command Center in the Pentagon, operations centers of the Military Departments, unified and specified commands, the National Security Agency, and the Defense Atomic Support Agency, monitoring may be authorized for command and communications purposes pursuant to regulations issued by the Head of the DOD component concerned.
(*c*) Communications security monitoring.
(1) DOD telephone communications security monitoring may be undertaken only as specified by the Director of the Defense Investigative Service or other appropriate DOD component head to provide material for analysis and to determine the degree of security being afforded telephone transmissions. The results of such analyses may be:
(*a*) Furnished to appropriate commanders on an advisory basis if they concern actual or possible security compromises; and
(*b*) Used as a basis for improving the security protection of telephone transmissions against hostile intelligence exploitation.
(2) All users of DOD telephone communications systems are specifically reminded that the communications systems are:
(*a*) Provided for the transmission of official Government information only; and
(*b*) Subject to communications security monitoring at all times.
(3) Use of DOD telephone communications systems shall constitute consent to communications security monitoring.
(4) Information obtained as a result of telephone communications security monitoring shall not be used for law enforcement purposes. This prohibitio does not preclude the use of information obtained as a result of telephon communications security monitoring in connection with disciplinary actic against DOD military or civilian personnel for their unauthorized use of the communications system.
(*a*) Communications management monitoring.
(1) Telephone communications management monitoring shall be undertaken only to provide material for analyses within the DOD to determine the operational efficiency and proper use of the DOD-dedicated systems and the common user systems of the Defense Communications System.
(2) All users of DOD communications systems are specifically reminded that the communications systems are:
(*a*) Provided for the transmission of official Government information only; and
(*b*) Subject to communications management monitoring at all times.
(3) Use of DOD telephone communications systems shall constitute consent to communications management monitoring.
e. The provisions of this regulation apply to all DIS components. These instructions do not modify the policy governing telephone interception and eavesdropping set forth in DOD Directive 5200.24.
For the director.

MASON W. GANT III,
Colonel, USAF Executive.

DEFENSE NUCLEAR AGENCY,
Washington, D.C., November 28, 1973.

DNA Instruction 5200.24A

Subject: Telephone interception and eavesdropping.
Reference: (*a*) DOD Directive 5200.24, Telephone Interception and Eavesdropping, August 17, 1967. (*b*) DNA Instruction 4640.4A, Telephone Monitoring, September 20, 1971.
Enclosure: (1) Information to be included in a request for approval of proposed wiretapping or eavesdropping. (2) Information to be included in wiretapping or eavesdropping reports.

1. Purpose.

To prescribe policies and restrictions governing telephone interception and eavesdropping by DNA personnel engaged in the conduct of investigations for law enforcement purposes in the United States. It also establishes reporting requirements regarding storage, inventory, and use of interception and eavesdropping devices in the conduct of such activities. This instruction implements DOD Directive 5200.24, August 17, 1967, and OASD(A) Memorandum, subject Requirements for Prior Approval of All Eavesdropping Activities, July 9, 1973.

2. Cancellation.

DNA Instruction 5200.24, January 17, 1973; subject, telephone interception and eavesdropping.

3. Applicability.

This instruction applies throughout the Defense Nuclear Agency (DNA) to include DNA activities at Johnston Atoll.

4. Definitions.

For the purpose of this instruction, the following definitions apply:

(*a*) Wiretapping.—The act of listening to or recording of any telephonic conversation by the use of an electronic, mechanical, or other device without the advance consent of all parties to the conversation, also referred to in this instruction as interception.

(*b*) Eavesdropping.—The act of listening to or recording any conversation other than telephonic by the use of any electronic, mechanical, or other device without the advance consent of all parties to the conversation.

(*c*) Monitoring.—The act of listening to or recording official office telephone communications by use of mechanical or electronic devices or recording by written means, for the purpose of obtaining an exact reproduction or a substance of the telephone conversation.

5. Wiretapping

a. To insure the privacy of telephone conversations to the maximum practical extent, the interception of telephone conversations is prohibited unless there are reasonable grounds to believe that: a criminal offense concerning the national security is involved; or a felony has been or is about to be committed; or telephone calls involving obscenity, harassment, extortion, bribery, or threat of bodily harm have been made to a subscriber user on a military installation under the jurisdiction of the Director, DNA.

(1) National Security Investigations—one of the following requirements must be met for investigations of criminal offenses concerning national security.

(*a*) If one of the parties has freely and voluntarily consented in advance to the interception and the interception has been approved in advance by the Director, DNA and the Deputy Assistant Secretary of Defense (Administration).

(*b*) If neither of the parties has consented in advance and the interception has been approved in advance by the Director, DNA, the Deputy Assistant Secretary of Defense (Administration), and the Attorney General.

(2) Felony Investigations—the following requirements must be met for investigations of a felony that has been or is about to be committed:

(*a*) One of the parties has freely and voluntarily consented in advance to the interception, and

(*b*) The interception has been approved in advance by the Director, DNA and the Deputy Assistant Secretary of Defense (Administration).

(3) Investigations Involving On-Base Telephones—the following requirements must be met:

(*a*) The subscriber-user of the telephone has requested the investigation of telephone calls involving obscenity, harassment, extortion, bribery, or threat of bodily harm and, in writing, freely and voluntarily consents in advance to the wiretap, and

(*b*) The telephone and wiretap are located on an installation under the jurisdiction of the Director, DNA, and

(*c*) The Director, DNA has granted approval of the interception in writing prior to the interception.

b. The prohibitions and restrictions prescribed above concerning wiretapping apply whether or not the information which may be acquired through interception is intended to be used in any way or to be subsequently divulged outside the Department of Defense.

c. Any questions concerning whether the use of a particular device can be said to involve a prohibited interception of a telephone conversation shall be forwarded to HQ, DNA, ATTN: OAIS for resolution.

d. Approval. Request for approval required by paragraph 5a(1), (2) and (3) above shall include the information outlined in Encl 1.

(1) Approval will not be granted for more than 30 days and the wiretap will be terminated as soon as the desired information is obtained.

(2) Renewal requests for specified periods of not more than 30 days may be submitted to the Director, DNA for consideration. If considered justified, the Director, DNA will forward the request to the Deputy Assistant Secretary of Defense (Administration) and the Attorney General for approval. The request must be approved at each office before the renewal may be implemented. Requests will arrive at HQ, DNA five working days prior to the expiration of the current approval.

6. Eavesdropping

(*a*) To protect the rights of privacy, eavesdropping is prohibited if the listening to or recording of a conversation involves a violation of the Constitution or a statute. This prohibition includes eavesdropping in any form which is accomplished by means of physical trespass or entry. It may also include eavesdropping practices which intrude upon the conversation between persons whose relationship is traditionally considered privileged (such as lawyer-client and doctor-patient). Further, even though it may be accomplished without physical trespass or entry, it may also be unlawful if it invades the sanctity of a man's home, private office, hotel room, automobile, or other physical areas deserving protection of the right of privacy.

(*b*) Eavesdropping not prohibited by the Constitution or a statute is authorized without the consent of all of the parties only under the following conditions:

(1) There are reasonable grounds to believe that a criminal offense concerning the national security is involved, or that a felony has been or is about to be committed; and,

(2) Advance written approval has been obtained from the Attorney General. A request for approval under this paragraph must include the information outlined in Enclosure 1. Approval will not be granted for more than 30 days, and the eavesdrop will be terminated as soon as the desired information has been obtained.

(*c*) Requests for approval. Requests will be forwarded to the Director, DNA who, if he considers it justified, will forward it and subsequent renewals thereof for not more than 30 days, to the Assistant Secretary of Defense (Administration). The Assistant Secretary of Defense (Administration) will forward the request to the Attorney General if he considers it justified.

(*d*) Emergency approvals. If, in the judgment of the Director, DNA the emergency needs of an investigation preclude obtaining the advance approval of the Attorney General as required by paragraph 5b(2) above, he may, without that approval, authorize the eavesdropping required by the investigation. He shall, within 24 hours after authorizing the eavesdropping, provide the Attorney General [with a copy to the Deputy Assistant Secretary of Defense (Administration)] with the information outlined in Enclosure 1. The report will include an explanation of the circumstances upon which the decision was made that the emergency needs of the investigation precluded obtaining the advance approval of the Attorney General.

(1) Commanders of subordinate elements will only request emergency approval of eavesdropping from the Director, DNA when absolutely necessary

to the needs of the investigation. Such requests will contain the information outlined in Enclosure 1 and a complete justification of the emergency request.

(2) Requests for emergency approvals will be forwarded by the fastest available means which meet security requirements.

7. Monitoring

The policy and procedures regarding communication security monitoring of office telephones is contained in DNA Instruction 4640.4A, 20 September 1971.

8. Procedures

(*a*) Records of Conversations Obtained Through Wiretapping or Eavesdropping. The head of the investigating unit will insure that:

(1) When technically feasible, the conversations concerned are permanently recorded on tape or other recording medium.

(2) The recording, together with any logs, transcripts, summaries, or memorandum that are made concerning the conversations are preserved and stored in the case file at the headquarters of the investigative unit conducting the interception or eavesdrop.

(3) Information obtained through wiretapping or eavesdropping, when used for any purpose, is always specifically identified as information obtained through these methods.

(4) Access to such information is strictly controlled and recorded. An investigative file containing information obtained by wiretapping or eavesdropping will be conspicuously marked as such and contain an access register which will indicate all persons who have had access to the file and the date of access.

(5) Information obtained by wiretapping and eavesdropping will not be disclosed outside the Department of Defense without approval of the Director. DNA.

(*b*) Wiretap and Eavesdropping Devices.

(1) Devices will not be procured without the approval of the Director, DNA.

(2) The 901st Military Intelligence Detachment is designated to maintain and control subject devices within DNA.

(3) The 901st MID will maintain centralized records of the inventory and use of devices at the unit headquarters. Records will be maintained for six years. A record will include:

(*a*) A description of the device sufficient for positive identification.

(*b*) The date the device was assigned to an agent or investigator.

(*c*) The date the device was returned to the issuing officer.

(*d*) A report by the agent or investigator using the device (see paragraph 9a).

(4) The Commander, 901st MID will continuously evaluate the need for devices primarily designed for wiretapping and eavesdropping and immediately dispose of such items in accordance with AR 381–143 when no longer required.

9. Reports

The following reports are required:

(*a*) Agent/Investigator Reports. When wiretapping or eavesdropping is authorized, the agent/investigator conducting the interception or eavesdropping will prepare a report containing the information outlined in Enclosure 2. A copy of each report will be forwarded to the Director, DNA, to arrive no later than five working days after termination of the wiretap or eavesdrop. This is a feeder report to RCS (DD–A(Q)795).

(*b*) Report of Annual Inventory and Justification. The Commander, 901st MID will conduct an annual inventory during the month of June of all technical listening equipment primarily designed for wiretap, investigative monitoring or eavesdropping. A report of the inventory and justification for each device, will be submitted to the Director, DNA, not later than July 1, each year. The report will include a statement that the inventory is being maintained at the lowest level consistent with operational requirements. This is a feeder report to RCS (DD–A(A)796).

(*c*) Reports to the Deputy Assistant Secretary of Defense—Administration. OAIS shall prepare reports to the Deputy Assistant Secretary of Defense—Administration—as follows:

(1) Before the 10th day of the month following each calendar quarter stating whether there was any wiretapping or eavesdropping during the preceding quarter by DNA personnel in the United States, or elsewhere if any party to the conversation was a citizen of the United States. The report will include all information in Enclosure 2. (Reports Control Symbol DD–A(Q)795.)

(2) Before July 10, annually, giving a complete inventory of all devices in DNA that are primarily designed for wiretapping or eavesdropping. The report shall include a statement that the inventory is being maintained at the lowest level consistent with operational requirements. (Reports Control Symbol DD–A(A)796.)

For the director:

J. D. EXUM,
Captain, USN, Chief of Staff.

DONALD B. POLATTY,
Captain, USN, Director for Personnel and Administration.

INFORMATION TO BE INCLUDED IN A REQUEST FOR APPROVAL OF PROPOSED WIRETAPPING OR EAVESDROPPING

1. Indicate whether the request is for a wiretap or an eavesdrop.
2. The purpose. To the extent possible, describe the conversation expected to be intercepted.
3. Identity of all persons under investigation, or affected.
4. Statement if any party has consented, and if so, his identity.
5. With respect to the particular operation: a. Identity of the operating unit; b. types of equipment to be used, if any, to include method of transmission and recording device; c. manner or method of installation; d. physical location, to include the address, telephone number, room number, whether inside or outside a building, public or private property, and the means of access; e. the expected period of time for the operation. (The period should be as short as possible compatible with operational necessity.)

INFORMATION TO BE INCLUDED IN WIRETAPPING OR EAVESDROPPING REPORTS

1. Indicate whether the report is on a wiretap or an eavesdrop.
2. Identity of the persons against whom directed.
3. Location.
4. Identity of the performing organizational unit.
5. Type of equipment used and manner and method of installation.
6. Approval authority.
7. Duration.
8. Purpose served.
9. Evaluation of results of operations that were completed during the reporting period.

DEFENSE SUPPLY AGENCY,
Alexandria, Va., September 14, 1973.

TELEPHONE INTERCEPTION AND EAVESDROPPING

DSA Regulation No. 5700.1 [1]

(RCS DD–A(Q)795) (RCS DD–(A)796)

I. Purpose and scope

To implement DOD Directive 5200.24 and set forth the policies and restrictions governing telephone interception and eavesdropping by DSA personnel engaged in the conduct of investigations for law enforcement purposes in the United States. It also establishes reporting requirements regarding storage, inventory, and the use of interception and eavesdropping devices by DSA activities in the conduct of such activities. This DSAR is applicable to HQ DSA and all DSA field activities. It does not apply to activities which are related directly to the protection of the national security.

II. Policy

It is the policy of HQ DSA to ensure the privacy of telephone conversations to the maximum practical extent. The interception of telephone conversations (wiretapping) is prohibited unless there are reasonable grounds to believe that:

A. A criminal offense concerning the national security is involved and:

1. One of the parties has freely and voluntarily consented in advance to the interception. If none of the parties has consented in advance, the interception

[1] This DSAR supersedes DSAR 5700.1, 18 Oct. 67, and Changes 1 and 2.

must be approved by the Attorney General of the United States. See paragraph V C. below.

2. The interception has been approved in advance by the Deputy Assistant Secretary of Defense (Administration).[2]

B. A felony has been or is about to be committed and:

1. One of the parties has freely and voluntarily consented in advance to the interception.

2. The interception has been approved in advance by the Deputy Assistant Secretary of Defense (Administration).[2]

C. Telephone calls involving obscenity, harassment, extortion, bribery, or threat of bodily harm have been made to a subscriber-user on a military base under the jurisdiction of the Department of Defense and:

1. The subscriber-user of the telephone has requested the investigation of telephone calls involving obscenity, harassment, extortion, bribery, or threat of bodily harm and, in writing, freely and voluntarily consents in advance to the wiretap.

2. The telephone and wiretap are located on an installation under the jurisdiction of the Department of Defense.

3. The interception is approved in advance by the head of the DSA field activity concerned.

D. The prohibitions and restrictions listed above apply whether or not the information which may be acquired through interception is intended to be used in any way or to be subsequently divulged outside the Department of Defense. Any question as to whether the use of a particular device can be said to involve a prohibited interception of a telephone conversation will be submitted to the General Counsel of the Department of Defense for consideration in accordance with procedures in paragraph V G. below.

E. To protect the rights of privacy, eavesdropping is prohibited if the listening to or recording of a conversation involves a violation of the Constitution or a statute. This prohibition includes eavesdropping in any form which is accomplished by means of physical trespass or entry. It also may include eavesdropping practices which intrude upon the conversations between persons whose relationship is traditionally considered privileged (such as lawyer-client and doctor-patient). Further, even though it may be accomplished without physical trespass or entry, it may also be unlawful if it invades the sanctity of a man's home, private office, hotel room, automobile, or other physical areas deserving protection of the right to privacy.

F. In order to limit eavesdropping not otherwise prohibited by subparagraph E above, eavesdropping is authorized without the consent of all of the parties only under the following conditions:

1. There are reasonable grounds to believe that a criminal offense concerning the national security is involved or that a felony has been or is about to be committed.

2. Advance written approval has been obtained from the Attorney General of the United States.

G. No device for wiretapping or eavesdropping will be obtained without the approval of the Director, DSA. No approval will be given for obtaining such devices except to the extent necessary for use in conformance with this DSAR.

H. When approval is obtained, DSA Chiefs of Security Divisions will be responsible for the security and control of wiretapping and eavesdropping devices for DSA, during time of possession.

III. Definitions

For the purpose of this DSAR, the following definitions apply:

A. *Eavesdropping.*—The act of listening to or the recording of any conversation other than telephonic by the use of any electronic, mechanical, or other device without the advance consent of all of the parties to the conversation.

B. *Wiretapping.*—The act of listening to or the recording of any telephone conversation by the use of any electronic, mechanical, or other device without the advance consent of all of the parties to the conversation; sometimes referred to herein as interception.

IV. Responsibilities

A. The Director, DSA, will:

1. Make required reports to the Deputy Assistant Secretary of Defense (Administration). (See subpar. D 1 below.)

[2] Denotes change.

2. Approve and forward, as necessary, to the Deputy Assistant Secretary of Defense (Administration) or disapprove, as appropriate, all requests for the installation of wiretaps and eavesdrops.

B. The heads of DSA field activities will:

1. Insure that no wiretaps or eavesdrops are installed unless fully in compliance with the provisions of this DSAR.

2. Submit reports required by paragraph VI below.

C. The Chiefs of Security Division are designated as responsible for the security and control of devices primarily designed or used for wiretapping and eavesdropping and will:

1. Report to the Provost Marshal, DSA (DSAH–XP) the make, type, serial number, and person responsible for custody for each device primarily designed for wiretapping or eavesdropping in its geographic area.

2. Reevaluate the need for such devices annually and advise DSAH–XP of the results of this reevaluation.

3. Maintain records required in paragraph V below.

4. Submit reports required by paragraph VI below.

D. The Provost Marshal, DSA, will:

1. Prepare and sign for the Director, DSA, reports to the Deputy Assistant Secretary of Defense (Administration) as follows:

(*a*) Before the 10th day of the month following each calendar quarter stating whether there was any wiretapping or eavesdropping during the preceding month by personnel of the Defense Supply Agency in the United States or elsewhere, if any party to the conversation was a citizen of the United States. The report will include all information in paragraph V below.

(*b*) Before July 10, annually, a complete inventory of all devices in the Defense Supply Agency that are primarily designed for wiretapping or eavesdropping. The report will include a statement that the inventory is being maintained at the lowest level consistent with operational requirements.

2. Review the inventory of all devices in DSA that are primarily designed for wiretapping or eavesdropping and all requests for additional devices to ensure that the inventory is maintained at the lowest level consistent with operational requirement.

3. Review all requests for installation of eavesdrops or wiretaps and make recommendations to the Director, DSA as to action to be taken concerning each request.

4. Maintain a central file of inventory and use of wiretapping and eavesdropping devices. The central record will include the date device was assigned, the date returned, and the report of the use made of the device. (See paragraph V F 1 below.)

5. Maintain this DSAR in a current status and review it annually, and forward two copies of superseding, supplementing, or amending issuances to the Deputy Assistant Secretary of Defense (Administration) no later than 15 days after publication.

V. Procedures

A. Requests from Heads of DSA field activities for authorization for wiretapping or eavesdropping will be sent to HQ DSA, ATTN: DSAH–XP and will include the information outlined below:

1. Whether the request is for a wiretap or an eavesdrop.

2. The purpose. To the extent possible, describe the conversation expected to be intercepted and the basis for belief that a criminal offense concerning the national security is involved or that a felony has been or is about to be committed.

3. Identity of all persons under investigation or affected.

4. Statement if any party has freely and voluntarily consented, and if so, his identity. (A copy of the signed consent will be forwarded with the request when any party has consented to a wiretap or eavesdrop.)

5. With respect to the particular operation:

a. Identity of the operating unit.

b. Types of equipment to be used, if any, to include method of transmission and recording device.

c. Manner or method of installation.

d. Physical location, to include the address, telephone number, room number, whether inside or outside a building, public or private property, and the means of access.

e. The expected period of time for the operation. (The period should be as short as possible compatible with operational necessity.)

B. The Heads of DSA field activities, before authorizing a wiretap in connection with an investigation of telephone calls involving obscenity, harassment, extortion, bribery, or threat of bodily harm made to a subscriber-user on a military base under the jurisdiction of DSA, will ensure that:

1. A written request from the subscriber-user of the telephone that telephone calls involving obscenity, harassment, extortion, bribery, or threat of bodily harm be investigated and a statement that the subscriber-user freely and voluntarily consents in advance to the wiretap.

2. The telephone and the wiretap are located at the activity.

C. *Approvals.* The Heads of DSA field activities may approve requests for wiretaps in connection with an investigation of telephone calls involving obscenity, harassment, extortion, bribery, or threat of bodily harm made to a subscriber-user on a military base under their jurisdiction. Advance approval of the Deputy Assistant Secretary of Defense (Administration) is required for wiretaps and eavesdrops involving National Security and Felony Investigations. Advance written approval of the Attorney General is required for all eavesdrops except in emergency and for wiretaps in connection with National Security Investigations unless one of the parties has freely and voluntary consented in advance to the wiretap. Approval will not be granted for more than 30 days, and the wiretap or eavesdrop will be terminated as soon as the desired information is obtained. Renewal requests for specified periods of not more than 30 days may be submitted to the appropriate approval authority for consideration.

D. All requests for approval of a wiretap or eavesdrop will be reviewed by the Office of the Provost Marshal, the Office of Counsel, and in cases involving national security, the Intelligence and Security Division. If the review indicates that the request is in accordance with the policies and procedures established herein and a recommendation for approval of the wiretap or eavesdrop is appropriate, approval will be requested from Deputy Assistant Secretary of Defense (Administration).

E. *Emergency Approval of Eavesdrops.* When in the judgment of the Director, DSA the emergency needs of an investigation preclude obtaining the advance approval of the Attorney General and the Deputy Assistant Secretary of Defense (Administration), he may authorize the eavesdropping required by the investigation. However, within 24 hours after authorizing the eavesdropping, the Director, DSA will provide the Attorney General, with a copy to the Deputy Assistant Secretary of Defense (Administration) with the information outlined in subparagraph A above, and an explanation of the circumstances of the emergency needs of the investigation that precluded the obtaining of the advance approval of the Attorney General and the Deputy Assistant Secretary of Defense (Administration).

F. *Conduct of Authorized Wiretapping or Eavesdropping.* When wiretapping or eavesdropping is authorized, the investigative agent will:

1. If technically feasible, permanently record the conversations on tape or other recording medium.

2. Preserve the recording, together with any logs, transcripts, summaries, or memoranda that are made concerning the conversations.

3. Report, in writing, to DSAH–XP describing the uses made of each device for wiretapping or eavesdropping.

G. When some doubt exists as to whether the use of a particular device involves a prohibited interception of a telephone conversation, the following information will be sent to DSAH–XP: Common and technical nomenclature of the device; the way it is being or planned on being used; and the reasons for its use. DSAH–XP will refer questions to Counsel, DSA for consideration, who will forward inquiries to General Counsel, Department of Defense, if appropriate.

H. The information obtained by wiretapping or eavesdropping will:

1. Be stored in an appropriate investigative file at a cental location, with access to the information strictly controlled and recorded.

2. Always be identified in storage and, when used for any purpose, as information obtained by wiretapping and eavesdropping.

3. Not be disclosed outside the Department of Defense unless the Director, DSA determines that disclosure is essential to governmental operations.

I. All records relating to inventory, use and information obtained by wiretaps and eavesdrops will be maintained for a period of 6 years.

VI. Forms and reports

Negative reports are not required when wiretapping and eavesdropping activities have not been conducted by DSA personnel; however, procedures will be established by the head of each DSA field activity and each chief, Security Division to insure that acts of wiretapping or eavesdropping are reported to HQ DSA, Attn.: DSAH–XP as follows:

A. Before the second day of the month following each calendar quarter any/all wiretapping or eavesdropping during the preceding quarter by personnel of the activity in the United States or elsewhere, if any party to the conversation was a citizen of the United States. The report will include the following for each action of eavesdropping or wiretapping:

1. Whether the report is on a wiretap or an eavesdrop.
2. Identity of the persons against whom directed.
3. Location.
4. Identity of the performing organizational unit.
5. Type of equipment used and manner and method of installation.
6. Approval authority.
7. Duration.
8. Purpose served.
9. Evaluation of results of operations that were completed during the reporting period.

B. Before July 2, annually, give a complete inventory of all devices in the DSA field activity concerned that are primarily designed for wiretapping or eavesdropping. The report will include a statement that the inventory is being maintained at the lowest level consistent with operational requirements. Negative reports are required.

C. The reports required by subparagraphs A and B have been assigned Report Control Symbol DD–A(Q)795 and Report Control Symbol DD–A(A)796. respectively.

By order of the director, Defense Supply Agency.

G. L. HEASLEY,
Captain, SC, USN, Executive.
GEORGE W. JOHNSON, Jr.,
Colonel, USAF, Staff Director, Administration.

Mr. COOKE. Thank you very much.

We have also made available our detailed statistical sheets from July, 1973 to March, 1974 as you requested. If you have technical questions with respect to telephone monitoring equipment, I have available Mr. Daniel Sheerin of the U.S. Air Force who is behind me.

Incidentally, I have two old colleagues whom I am sure the committee recognize, Mr. Robert T. Andrews and Mr. Joseph J. Liebling.

Departmental policies and procedures which limit the use of telephone monitoring and control the use of information obtained by third parties, are set forth in Department of Defense Directive 4640.1, "Telephone Monitoring." These directives apply to the United States, the Commonwealth of Puerto Rico and U.S. territories. They do not apply elsewhere overseas, nor are they applicable to our foreign intelligence collection activities.

Our telephone monitoring is administrative rather than investigative. The directive classifies it into four categories.

The first is office telephone, listening to or recording office telephone communications by use of mechanical or electronic devices or recording by written means, for the purpose of obtaining an exact reproduction or a summary of the substance of the telephone conversation and with the consent of all parties.

Second is command center communications. Listening to or recording telephone communications in DOD command centers for the purpose of obtaining a record of conversations, or parts thereof, for command and control purposes.

Third is communications security. Listening to or recording of the transmission of official defense information over DOD-owned or leased telephone communications, by any means, for the purpose of determining whether such information is being properly protected in the interest of national security. Notice of this action is given to users that these systems are subject to communications security monitoring at all times.

The last is communications management. Listening to or recording telephone communications on DOD-dedicated systems or the common-user systems of the Defense Communications System, by any means, not for the contents but for the purpose of determining whether the systems are functioning properly for official purposes. Almost every phone company has a counterpart activity.

The first class of telephone monitoring is one in which you are all familiar, called office monitoring. With the use of either a recorder equipped with "beeper" or with a stenographer, it requires the advance consent of all parties to the conversation. Office telephone monitoring, in such cases, is a valuable management tool to reflect the exact nature of agreements and understandings achieved by telephone. One of the parties to the conversation may be outside the DOD, but again let me emphasize that all parties concerned must consent to office telephone monitoring.

The other three classes of telephone monitoring are largely internal. That is, they are directed to the manner in which DOD military and civilian personnel use telephones which are part of DOD communications systems.

Telephone monitoring in command centers, for communications security and for communications management purposes, does not require express consent in each case. The purpose of command center monitoring is to obtain accurate records for command and control purposes of official calls to a command center. Examples of the command centers are the National Military Command Center, its alternate, the Airborne Command Post, the North American Air Defense Command Post, the military services operations centers in Washington, the military and security police operations center, fire and rescue control centers, and air traffic control centers.

DOD monitoring for these centers closely compares with the recordings made by the Federal Aviation Agency in its many air traffic control centers. Similarly, most police, fire, and rescue control centers in our large cities and counties monitor accident reports and requests for assistance to insure accuracy and for record purposes.

DOD directive 4640.1 requires for each center specific regulations be published prior to the initial operation of the recording equipment. The existence of such monitoring, moreover, is required by DOD directive 4640.1 to be widely and expressly publicized throughout DOD and its components as to amount to constructive consent.

Our authority for this class of monitoring equipment and its use stems from communications common carrier tariffs which have been approved by the Federal Communications Commission. This class of monitoring is provided for in DOD directive 4640.1, which I mentioned earlier.

The third class is communications security telephone monitoring of administrative telephone monitoring which is used albeit rarely on Department of Defense telephone circuits. The purpose of COMSEC monitoring is to provide a basis for analysis of the vulnerability of telephone communications to hostile intelligence exploitation, and for determining the best means by which such vulnerabilities may be reduced or eliminated.

This monitoring may only be conducted when authorized by the commander or DOD official in charge of an installation or activity or his superior. Let me stress that security organizations organized and equipped to perform communications security monitoring are not authorized to monitor communications systems on their own initiative. As a matter of fact, communications telephone security monitoring is employed infrequently. Less than 1 percent of our telephones are monitored for security in any given year.

The lines selected for security monitoring consist mainly of command posts, major operational headquarters, war rooms, and field exercises both in the United States and overseas.

Let me emphasize that the purpose of COMSEC telephone monitoring is to advise commanders on actual or possible security compromises and improve the security protection of telephone communications.

DOD directive 4640.1 expressly states that the information obtained as a result of telephone communications security monitoring shall not be authorized for law enforcement purposes unless the general counsel of the DOD authorizes an exception in a specific case.

Parenthetically, I found no evidence that that event has ever happened.

The last class of administrative telephone monitoring is communications management monitoring, often called service observation. Service observation is conducted largely by computer analysis and peg count methods rather than by actual listening to telephone conversations in progress.

It is a tool used to determine if telephone systems are functioning properly, not with the contents of conversations, but with such things as the precedence and number of calls, their duration, response to signals, number of busy signals for a given time period, and total load on the system.

Mr. Chairman, this completes our summary of the provisions and our practices in telephone monitoring.

Thank you very much. I and my colleagues are, of course, available to answer your questions.

Mr. MOORHEAD. Thank you, Mr. Cooke. We will look forward to that shortly.

The subcommittee would now like to hear from Mr. David R. Macdonald.

STATEMENT OF DAVID R. MACDONALD, ASSISTANT SECRETARY FOR ENFORCEMENT, OPERATIONS AND TARIFF AFFAIRS, DEPARTMENT OF THE TREASURY; ACCOMPANIED BY J. ROBERT McBRIEN, STAFF; WILLIAM A. MAGEE, JR., ASSISTANT COMMISSIONER, CUSTOMS FOR SECURITY AND AUDIT; DOUGLAS A. McCOMBS, SENIOR SPECIAL AGENT, SPECIAL INVESTIGATIONS BRANCH, OFFICE OF INVESTIGATIONS, U.S. CUSTOMS SERVICE; WILLIAM J. HULIHAN, DIRECTOR, INTERNAL SECURITY DIVISION, OFFICE OF THE ASSISTANT COMMISSIONER (COMPLIANCE), INTERNAL REVENUE SERVICE; JACK PETRIE, CHIEF, OPERATIONS BRANCH, TAXPAYER SERVICE DIVISION, INTERNAL REVENUE SERVICE; AND ROBERT R. SNOW, SPECIAL AGENT-IN-CHARGE, SPECIAL INVESTIGATIONS AND SECURITY DIVISION, OFFICE OF INVESTIGATIONS, U.S. SECRET SERVICE

Mr. MACDONALD. Thank you, sir.

My name is David R. Macdonald, Assistant Secretary of the Treasury for Enforcement, Operations, and Tariff Affairs. Accompanying me today are Mr. J. Robert McBrien of my staff and several representatives of other components of the Treasury Department: Mr. William A. Magee, Jr., Assistant Commissioner of Customs for Security and Audit; Mr. Douglas A. McCombs, Senior Special Agent, Special Investigations Branch, Office of Investigations, U.S. Customs Service; Mr. William J. Hulihan, Director, Internal Security Division, Office of the Assistant Commissioner (Compliance), Internal Revenue Service; Mr. Jack Petrie, Chief, Operations Branch, Taxpayer Service Division, IRS; and Mr. Robert R. Snow, Special Agent-in-Charge, Special Investigations and Security Division, Office of Investigations, U.S. Secret Service.

I am pleased to report to you today on the policies and practices of the Treasury Department relating to polygraphs, psychological stress evaluators, telephone monitoring, and other surveillance procedures.

In November of 1973, the Treasury Department submitted to the General Accounting Office a report requested on behalf of this subcommittee concerning Treasury's use of polygraphs, psychological stress evaluators, and telephone monitoring and surveillance procedures. We have submitted for the record today information which updates several of the questions previously answered. I would like at this time to submit this additional information for the record.

Mr. MOORHEAD. Without objection, it will be made a part of the record.

[The material referred to follows:]

THE DEPARTMENT OF THE TREASURY,
Washington, D.C., June 12, 1974.

Hon. WILLIAM S. MOORHEAD,
Chairman, Foreign Operations and Government Information Subcommittee, Government Operations Committee, House of Representatives, Washington, D.C.

DEAR MR. CHAIRMAN: This is in response to your letter of May 14, 1974, to the Secretary requesting that the Treasury Department update the information on monitoring procedures submitted in response to the October 5, 1973, questionnaire survey of the General Accounting Office. The attachments to this letter include the few changes which have been made to the original Treasury Department response of November 28, 1973.

I wish to submit this updated information for inclusion in the record of the hearings on monitoring procedures to be conducted by this subcommittee on Thursday, June 13, 1974.

Sincerely yours,

DAVID R. MACDONALD,
Assistant Secretary for Enforcement, Operations and Tariff Affairs.

Enclosures.

Summary of polygraph uses by Treasury Department enforcement agencies,[1] fiscal year 1974

Alcohol, Tobacco and Firearms Bureau	24
Customs Service	0
Internal Revenue Service	3
Secret Service	40
Total	67

[1] Numbers are estimated since close of fiscal year 1974 will reflect a more accurate final accounting for fiscal year 1974.

U.S. SECRET SERVICE

The U.S. Secret Service reports no changes in the information previously submitted to the General Accounting Office.

Please note that for fiscal year 1974 the Secret Service reports approximately 40 cases of utilization of polygraph tests.

BUREAU OF ALCOHOL, TOBACCO AND FIREARMS

OFFICE OF CRIMINAL ENFORCEMENT

Answer No. 4.—The survey of Code-A-Phone automatic telephone answering equipment reflects a total of 53 instruments, 40 of which are in use and 13 of which are inoperative.

Answer No. 7.—(a) $56,000 ($4,000 increase for two devices); (c) $57,000 (reflects above $4,000 increase).

Please note that ATF estimates that approximately $15,000 worth of the equipment referred to in No. 7 is inoperative.

DEPARTMENT OF THE TREASURY—OFFICE OF THE SECRETARY

POLYGRAPHS AND PSYCHOLOGICAL STRESS EVALUATORS

There is no change in the information previously reported. However, answer No. 3 to part A of the October 1973, GAO questionnaire reflected that a revised issuance of the Instructions for Conducting Security Investigations was in preparation at that time. That revision has not yet been issued but will continue to contain instructions prohibiting polygraph use without prior Civil Service Commission clearance.

MONITORING PRACTICES AND DEVICES

The remaining eight transmitter cutoff switches located in the office of officials subordinate to the Secretary and the one in the Office of the Comptroller of the Currency have been removed or otherwise rendered inoperative.

MONITORING PROCEDURES

Attached are copies of three memoranda which supersede the June 9, 1961, version of Administrative Circular No. 41, signed by Secretary Douglas Dillon.

(1) Administrative Circular No. 41 Revised, December 13, 1973, issued by Secretary Shultz.

(2) Supplement No. 1 to Administrative Circular No. 41, January 23, 1974, issued by Secretary Shultz.
(3) Memorandum of Clarification, January 14, 1974, issued to Assistant Secretary Edward L. Morgan.

THE SECRETARY OF THE TREASURY,
Washington.

ADMINISTRATIVE CIRCULAR NO. 41 REVISED, DECEMBER 13, 1973

To: The Deputy Secretary
The Under Secretary for Monetary Affairs
The Under Secretary
The Assistant Secretaries
Director, Executive Secretariat
Heads of Bureaus

It is the policy of the Department of the Treasury that no telephone calls to or from Treasury offices be monitored by or for Treasury officials. "Monitoring," as used here, means recording the conversation through the use of mechanical equipment or a stenographer for the purpose of producing a verbatim record of what was said.

Officials of the Department of the Treasury shall have individual discretion as to whether they will permit secretaries to listen and record names, dates, summaries, or similar material, but verbatim transcriptions of telephone conversations shall be made only when both parties to the conversation agree that this is necessary. Such transcriptions are to be considered as an exception to normal procedure, and no mechanical or electronic equipment including transmitter cut-off switches or similar devices will be used for this purpose.

The right to use mechanical or electronic telephone recording or monitoring equipment by any official of the Department of the Treasury under any circumstances shall be subject to the prior approval of the Secretary or his designated representative. Officials who have received such authorization under previous regulations must resubmit a request for approval under the provisions of this circular within one month from the date of this circular. Requests for continuing approval for the right to use this equipment will be submitted annually prior to June 30.

Administrative Circular No. 41, dated June 9, 1961, is superseded.

GEORGE P. SHULTZ.

THE SECRETARY OF THE TREASURY,
Washington.

ADMINISTRATIVE CIRCULAR NO. 41 REVISED, SUPPLEMENT NO. 1,
JANUARY 23, 1974

To: The Deputy Secretary
The Under Secretary for Monetary Affairs
The Under Secretary
The Assistant Secretaries
Director, Executive Secretariat
Heads of Bureaus

The Deputy Secretary, General Counsel, and Assistant Secretary for Enforcement, Tariff and Trade Affairs, and Operations are designated as my representatives for the approval of requests to use mechanical or electronic telephone recording or monitoring equipment in accordance with current laws and regulations governing their use.

GEORGE P. SCHULTZ.

THE DEPARTMENT OF THE TREASURY,
Washington, D.C., January 14, 1974.

Memorandum to: Heads of Treasury enforcement bureaus and offices.
From: Edward L. Morgan, Assistant Secretary for Enforcement, Tariff and Trade Affairs, and Operations.
Subject: Administrative Circular No. 41 Revised, December 13, 1973—Monitoring Procedures.

You are hereby advised that the provisions contained in Treasury administrative Circular No. 41 Revised, issued December 13, 1973, relative to the use of mechanical or electronic recording or monitoring equipment by any official of the Department of the Treasury, apply only to administrative telephone conversations and not those involving criminal investigations or protective intelligence operations conducted by law enforcement officers.

U.S. CUSTOMS SERVICE

All updated information developed by the Customs Service is contained in the attached memorandum from the Office of Investigations. It relates only to monitoring practices and devices of the Office of Investigations. No updated or additional information would apply to the questions relating to the use of polygraphs and psychological stress evaluators. The Office of Security and Audit has advised that all information provided in their report of November 1973 is currently accurate and complete.

U.S. CUSTOMS SERVICE

Subject: Update of a report submitted to the U.S. General Accounting Office for information on the use by Treasury of polygraphs, psychological stress evaluators, and telephone monitoring, or other surveillance procedures.

Below is an updating of our information concerning the above subject for your use in coordinating a Customs Service response to the House Subcommittee on Foreign Operations and Government Information.

PART B

Question 3. If telephone recording devices are used to monitor or record telephone calls, how many such devices are in use in your agency? Is a beeper or other warning devices required to notify the other party that the call is being recorded by the devices?

Answer. The Office of Investigations has a current inventory of 293 tape recorders and 74 induction coils which are used to monitor or record telephone calls. No beeper or other warning devices is utilized to notify participating parties. In the case of an administrative monitoring, all parties acknowledge and agree to the monitoring prior to the conversation.

Question 4. If telephone recording devices are used, please specify the number of recorders wired into telephone circuits, the number of induction-type attachments that can be used to record telephone conversations on dictation machines without being wired into the circuit, and any other types of instruments that can be used to monitor or record telephone conversations. Please indicate which of these devices, if any, are equipped with a beeper or warning signal.

Answer. No recording devices are wired directly into telephone circuits. The Office of Investigations has 74 induction coils for recording telephone conversations.

Question 6. Does the agency ever utilize nontelephonic "bugging" devices? If so, of what type and for what purpose?

Answer. The Office of Investigations does, in carrying out its enforcement responsibilities, utilize nontelephonic "bugging" devices. The use of such equipment is strictly controlled and in full compliance with 18 U.S.C. 2510–2520 and directives from the Departments of Justice and Treasury.

The current inventory for the Office of Investigations' nontelephonic "bugging" devices is:

Intelligence kits	26
Microphones	11
Transmitters and receivers	3
Transmitters and recorders	1
Transmitters	20
Receivers	12
Video recorders/monitors	12

Question 7. Please furnish the best available estimate of the total cost of these (a) recorders and attachments, (b) telephone service observing devices, (c) nontelephonic "bugging" devices.

Answer. The best available estimate of cost is:

(a) 293 tape records	$58, 600
(b) None	
(c) Nontelephonic "bugging" devices	90, 975
Total	149, 575

GEORGE C. CORCORAN, Jr.

INTERNAL REVENUE SERVICE

1. Instructions implementing a previously reported revision in IRS policy on consensual monitoring have been issued. See attached Manual Supplement 93G–142, dated April 11, 1974.

2. An information notice on use and control of electronic surveillance equipment was issued by the Commissioner on March 25, 1974. See attached information notice.

3. Updated information regarding the use of polygraph devices and changes in the inventories and costs of electronic surveillance equipment is included for the Office of the Assistant Commissioner for Compliance and the Office of the Assistant Commissioner for Inspection. The inventory and cost changes result either from new purchases or identifying equipment not previously recorded in inventory counts.

The Internal Revenue Service reports no other changes.

[Manual Supplement Nos. 93G–142, 94G–52, 99G–24, (10) 1G–24]

DEPARTMENT OF THE TREASURY INTERNAL REVENUE SERVICE

CONSENSUAL MONITORING OF PRIVATE CONVERSATIONS IN CRIMINAL INVESTIGATIONS—APRIL 11, 1974

Section 1. Purpose

This supplement implements policy statement P–9–35 (approved Oct. 26, 1973), and Department of Justice guidelines on monitoring private conversations dated October 16, 1972.

Section 3. Background

The monitoring of conversations with the consent of one of the participants is an effective and reliable investigative technique but must be sparingly and carefully used. The Department of Justice has encouraged its use by criminal investigators where it is both appropriate and necessary to establish a criminal offense. While such monitoring is constitutionally and statutorily permissible, this investigative technique is subject to careful regulation in order to avoid any abuse or any unwarranted invasion of privacy.

Section 3. Designated Officials

.01 The monitoring of telephone conversations with the consent of one or all parties may be authorized by the Chief, Intelligence Division; the Assistant Regional Inspector (Internal Security); the Chief of the National Office Investigations Branch (Internal Security); the Chief of National Office Operations Branch (Intelligence); or in the absence of any of them, the person acting in his place. This authority cannot be redelegated.

.02 Other than in criminal investigations, the recording of telephone calls by use of mechanical, electronic or any other device is prohibited.

.03 The monitoring of nontelephone conversations with the the consent of one party requires the advance authorization of the Attorney General or any designated Assistant Attorney General. Requests for such authority may be signed by the Director, Intelligence Division; the Director, Internal Security Division; or, in their absence, the Acting Directors. This authority cannot be redelegated. These same officials may authorize temporary emergency monitoring when exigent circumstances preclude requesting the authorization of the Attorney General in advance. If the Director, Internal Security Division, or the Director, Intelligence Division, cannot be reached, the Assistant Commissioner (Inspection) or the Assistant Director, Intelligence Division, may grant emergency approval. This authority cannot be redelegated.

.04 There are no restrictions on any nontelephone monitoring when all parties to the conversation consent.

.05 The use of monitoring equipment as authorized by the designated officials in section 3.01 and section 3.03 above, is limited to criminal investigators (GS–1811 series) or to persons acting under the direction of criminal investigators. The prohibitions and limitations outlined in policy statement P–9–35 apply equally to Service personnel and to non-Service persons who act at the direction of criminal investigators.

.06 Monitoring of private conversations will be authorized only when, in the considered judgment of the designated official, such action is warranted and necessary to effective law enforcement.

Section 4. Annual Reports

The Assistant Commissioner (inspection) shall submit to the Assistant Attorney General, Criminal Division, an annual report during July of each year containing: an inventory of all the Service's electronic and mechanical equipment designed for monitoring conversations; and a brief statement of the results obtained during the prior fiscal year by the use of such investigative monitoring.

Section 5. Other Restrictions

A device, such as a "pen register," designed solely to identify telephone numbers, may be employed only when authorized by an appropriate order in the nature of a search warrant under Rule 41, Federal Rules of Criminal Procedures.

Section 6. Effect on Other Documents

.01 This amends and supplements IRM 9383.5, 9453.2, MS CR 94G–34, dated July 10, 1967, and 682 of IRM (10)111, Instructional Handbook for Inspectors of the Internal Security Division. This also supplements IRM 9900, Handbook for Special Agents.

.02 The above "effect" should be annotated in pen and ink on the cited text and supplement, with a reference to this supplement.

DONALD C. ALEXANDER, *Commissioner.*

Attachment: Policy statement.

ATTACHMENT TO MS 93G–142, CR 94G–52, 99G–24 AND (10)1G–24

P–9–35 (Approved 10–26–73)

LEGAL RIGHTS OF PERSONS INVESTIGATED TO BE OBSERVED

The Internal Revenue Service is charged with responsibility for administering internal revenue laws with uniform fairness and impartiality. A vigorous enforcement effort is necessary to bring to justice willful offenders of tax laws. At the same time, the integrity of Service personnel in respecting and observing the constitutional and other legal rights of all persons being investigated must be maintained. The methods which the Service will use in investigating alleged violations of law may vary with the circumstances, but will in all respects stay within the bounds of the law.

LIMITATIONS ON USE OF EAVESDROPPING DEVICES

In accordance with the above stated principles, the Service will at all times conform to the Department of Justice guidelines on monitoring private conversations. Mechanical, electronic, or other devices will never be used illegally.

MONITORING OF TAXPAYER SERVICE AND OFFICE COLLECTION TELEPHONE CONVERSATIONS

The use of telephone equipment enabling supervisors to monitor telephones used by office collection interviewers and employees performing Taxpayer Service work, to determine employee courtesy and accuracy, is permitted provided such conversations are not recorded and the telephones monitored are conspicuously labeled so that employees may distinguish them from ordinary telephone service and know that telephone calls may be monitored.

INTERCEPTION OF TELEPHONE CONVERSATIONS

The interception of telephone conversations without the consent of at least one of the parties to the conversation is prohibited, whether or not the information is intended to be used in any way or to be subsequently divulged outside the Service.

The use of eavesdropping devices to intercept telephone conversations with the consent of one party to the conversation must be approved by an official designated by the Commissioner.

OVERHEARING OR RECORDING NONTELEPHONE CONVERSATIONS

The use of eavesdropping devices to overhear or record any nontelephone conversation without the consent of all parties to the conversation, but with the consent of at least one, must be approved in writing by the Attorney General or his designee; except for emergency situations when an official designated by the Commissioner may grant prior approval. The use of eavesdropping devices to overhear or record a nontelephone conversation without the consent of at least one of the parties to the conversation is prohibited without a specific court order.

Approved:

DONALD C. ALEXANDER, *Commissioner*

Date: October 26, 1973.

[Information Notice No. 74-5]

U.S. TREASURY DEPARTMENT INTERNAL REVENUE SERVICE

USE AND CONTROL OF ELECTRONIC SURVEILLANCE EQUIPMENT—MARCH 25, 1974

To: All Employees.

I am sure that all of you are aware of the tremendous obligation which the Service has concerning possible misuse of electronic surveillance devices. There are certain conditions under which our investigative personnel may employ electronic devices to monitor telephone calls. These are spelled out in Policy Statement P-9-35 and IRM 9383.5, IRM 125 (16) provides the Treasury policy that no telephone calls on administrative matters to or from the Treasury will be monitored. "Monitoring," for these purposes, means recording the conversation producing a verbatim record of what was said. The term does not include the "listening-in" of calls to the Taxpayer Service function to determine the quality of the response to an inquiry.

Within the Service, the procurement and control of surveillance equipment is centralized in the National Office Intelligence Division. A recently completed check of the national inventory records of induction coils disclosed a considerably fewer number than that which was found on hand in district offices. Also, it was learned that some of these devices were in the possession of employees in functions other than Intelligence. Many of these coils had been purchased by employees with their own funds without obtaining the approval of the appropriate Property Officer as required by Policy Statement P-1-109, approved August 26, 1960.

Your management officials will meet with you in the immediate future to reaffirm the Treasury and Service policies on the use and control of electronic surveillance equipment. I must caution each of you that it is extremely important that you adhere to these requirements. Any violation of these regulations could result in appropriate disciplinary actions.

DONALD C. ALEXANDER, *Commissioner*

INTERNAL REVENUE SERVICE

JUNE 7, 1974.

Memorandum:
To: Assistant Commissioner (Planning and Research)
Attention: Planning Officer Frank M. Malanga.
From: Assistant Commissioner (Compliance) CP:I:T
Subject: Questionnaire on Polygraphs, Psychological Stress Evaluators and Monitoring Practices and Devices.

The following material is to provide up-to-date information concerning Treasury use of polygraphs, psychological stress evaluators, and telephone monitoring or other surveillance devices. The original material was submitted to the Assistant Secretary for Enforcement, Tariff and Trade Affairs, and Operations by memorandum from the Commissioner dated November 7, 1973. We are submitting this response for your use in coordinating the overall IRS response to Treasury.

Unless specifically identified, all answers, policy statements, regulations, and so forth, remain the same as shown in our original response.

PART A

QUESTIONNAIRE ON POLYGRAPH AND PSYCHOLOGICAL STRESS EVALUATORS

The Intelligence Division does not possess polygraph or psychological stress evaluators. We normally do not use this equipment. In 1973 one of our districts twice utilized polygraph equipment and operators borrowed from the U.S. Postal Service to evaluate sensitive information furnished in a narcotics investigation. We know of no other use of this type equipment within the Intelligence Division. We do not anticipate any future use of this equipment.

PART B

QUESTIONNAIRE ON MONITORING PRACTICES AND DEVICES

Questions 3 and 4

How many devices are used to monitor or record telephone calls:

The Intelligence Division has forty-eight (48) induction coils and one telephone line recording actuator. The one telephone line recording actuator was an unauthorized acquisition by a field office. We are advised that there was no use of this equipment and that it is being sent to the Intelligence Division National Office where it will be destroyed.

No beeper or other warning device is required with an induction coil. The induction coils are used in conjunction with ordinary tape recorders to record telephone calls. We have no other types of instruments designed to monitor or record telephone conversations.

Question 6

Our current inventory of electronic surveillance equipment to conduct consensual eavesdropping on non-telephone conversations is: 51 miniature transmitters; 14 surveillance tape recorders; 22 miniature receivers; 4 microphone amplifiers.

The equipment listed above comprises the components of five "kits" maintained at one location under National Office control.

Question 7

The best available estimate of total cost of (a) telephone induction coils and the telephone line actuator is $330 and (b) non-telephone devices is $47,914.00.

Question 8

Agency rules and regulations covering telephone monitoring recording and surveillance.

Attached manual supplement 93G-142 dated April 11, 1974, provides the designated officials that may authorize the monitoring of telephone conversations with the consent of one or all parties. Prior regulations provided for authorization with the consent of one party to the conversations.

Attached policy statement P-9-35 dated October 26, 1973, provides that the Commissioner will designate an official that could authorize monitoring of telephone conversations with the consent of one or all parties and will designate an official that can grant emergency approval to monitor non-telephone conversations. Prior regulations provided that the Deputy Commissioner could make these designations.

Attachments.

JOHN F. HANLON.

INTERNAL REVENUE SERVICE

Memorandum JUNE 6, 1974.

To: Assistant Commissioner (Planning and Research) Attn: Planning Officer Frank M. Malanga.
From: Office of Assistant Commissioner (Inspection) I:IS:P.
Subject: Questionnaire on Polygraphs, Psychological Stress Evaluators and Monitoring Practices and Devices.

The following material is to provide up-to-date information concerning Treasury use of polygraphs, psychological stress evaluators, and telephone monitoring

or other surveillance devices. The original material was submitted to the Assistant Secretary for Enforcement, Tariff and Trade Affairs, and Operations by memorandum from the Commissioner dated November 7, 1973. We are submitting this response for your use in coordinating the overall IRS response to Treasury.

Unless specifically identified, all answers, policy statements, regulations, etc. remain the same as shown in Inspection's original response.

PART A

QUESTIONNAIRE ON POLYGRAPH AND PSYCHOLOGICAL STRESS EVALUATORS

Questions 4 (l) and (m)

Polygraph examinations conducted by the Internal Security Division or at the request of the Internal Security Division. None previously reported.

The Internal Security Division has participated in one polygraph examination since November 1973.

The examination was:

Initiated at employee's request—verbally March 29, 1973 and in writing November 12, 1973.

Approved by the National Office of Inspection—March 20, 1974.

Examination was conducted on April 15, 1974 and April 16, 1974.

Examination was conducted by United States Postal Service.

Status of case—pending.

PART B

QUESTIONNAIRE ON MONITORING PRACTICES AND DEVICES

Questions 3 and 4

How many devices are used to monitor or record telephone calls. Forty-five induction coils previously reported.

The Internal Security Division utilizes 79 induction coils in conjunction with ordinary and/or battery operated tape recorders which can be used to record telephone calls.

Question 7

The best available estimate of total cost of (a) recorders and attachments and (c) non-telephone devices. $81,250 previously reported.

The best available estimate of the total cost is $83,630. It should be noted that the cost for surveillance recorders and devices has not changed and this only increases the cost of standard type recorders from $30,150 to a cost of $32,530. These recorders can be used in conjunction with transmitters or induction coils and sometimes are but they are normal size recorders that are also used for regular office use. Therefore, they are not necessarily considered "surveillance devices" in the normal use of the term.

Question 8

Agency rules and regulations covering telephone monitoring, recording and surveillance.

Attached manual supplement 93G–142 dated April 11, 1974, provides the designated officials that may authorize the monitoring of telephone conversations with the consent of one or all parties. Prior regulations provided for authorization with the consent of one party to the conversations.

Attached policy statement P–9–35 dated October 26, 1973, provides that the Commissioner will designate the official that could authorize monitoring of telephone conversations with the consent of one or all parties and will designate the official that can grant emergency approval to monitor nontelephone conversations. Prior regulations provided that the Deputy Commissioner could make these designations.

Attachments.

Director, Internal Security Division.

Mr. MACDONALD. I believe these materials clearly indicate that the Treasury Department is not engaged in "snooping" on its employees or in "peering over the shoulder" of the American people. While the Treasury Department believes that its present procedures and practices

are reasonable, we are, nonetheless, taking the precaution of a careful scrutiny of our rules and operations; and we will institute whatever new procedures are needed and authorized.

As the report to GAO and our current information indicate, we have eliminated from Treasury those transmitter cutoff devices which are not needed to screen excessive background noise. That leaves only 10 operative cutoff devices remaining of the 108 we reported in September, 1970. All of the 10 operative transmitter cutoff devices are needed and used for purposes other than monitoring. Some cutoff devices have been rendered inoperative, but have not yet been physically removed from the premises.

PERSONNEL AND ADMINISTRATIVE PROCEDURES OF THE TREASURY DEPARTMENT

In reviewing your subcommittee's 1970 report, Mr. Chairman, and the questionnaire submitted to us by the General Accounting Office, I noted that emphasis appeared to be placed upon the utilization of polygraph examinations or other mechanical evaluations in connection with the testing of Treasury employees concerning their character, fitness, and stability. As our response to GAO points out, the Treasury Department is not using polygraph devices or psychological stress evaluators to measure the character and fitness of its employees, and we have no intention of doing so.

I might add, parenthetically, we do have one psychological stress evaluator in the Department. His name is William Simon and if you can survive that particular taxing demand, you should be able to survive the other stresses and strains.

Mr. MOORHEAD. I thing we ought to have the record show he has been under some stress and strain in the past months, too.

Mr. MACDONALD. Nor does the Treasury Department use surveillance or monitoring practices in connection with its administrative functions, unless the taxpayer service program of the Internal Revenue Service could be deemed to be such a practice.

The taxpayer service program of the IRS involves telephonic tax advice given by IRS service representatives to thousands of taxpayers. These service representatives are told in advance that their advice will, from time to time, be monitored by supervisors in order to assure accuracy, completeness and courtesy. This is an instance where with the use of monitoring equipment the employee's advice to taxpayers can be judged by a supervisor. It balances, we believe, the great importance of assuring accurate, complete and courteous tax advice to our citizens with fundamental fairness and respect for employees. We believe that the foreknowledge of and consent to the fact that their calls will be periodically audited gives to the taxpayer service personnel of the Internal Revenue Service an adequate opportunity to consider whether they desire to work at a task which demands such high quality and uniform advice as tax counselling for millions of Americans.

CRIMINAL ENFORCEMENT OPERATIONS

As you are aware, the Treasury Department, through the Secret Service, has the responsibility for protecting the President, the Vice President, and other important functionaries against physical violence.

The Secret Service also is the vehicle through which Treasury is charged with protecting the integrity and confidence of the Nation's currency by suppressing counterfeiting and forgery of Government checks. Through the IRS, Treasury is required to enforce the Nation's revenue-raising laws, in order to assure that nonfilers and fraudulent filers of income tax returns are discovered and prosecuted. Through the Customs Service and the Alcohol, Tobacco and Firearms Bureau, smugglers, illicit still operators, and illegal dealers and handlers of firearms are brought to justice by Treasury enforcement personnel.

In connection with these enforcement activities, monitoring and surveillance practices conforming to legal requirements are employed and polygraph tests are administered. I should add that psychological stress evaluators are not used by any branch of the Treasury Department in enforcement functions just as they are not used in our administrative operations.

Fifty-seven polygraph tests were administered by Treasury enforcement agencies in fiscal year 1973 and approximately 67 through May in fiscal year 1974. Most of these tests have been administered by the Secret Service in connection with investigations of counterfeiting cases. In all cases, the polygraph is used by Treasury enforcement agencies with the consent of a suspect or informant as an aid in evaluating information developed as part of a criminal investigation. It is used in those cases where other circumstances indicate it may have some value to the investigation. No individual is ever compelled to subject himself to a polygraph examination.

There were in calendar year 1973 approximately 1,080 cases in which monitoring of conversations occurred in connection with criminal investigations by various enforcement operations of the Treasury Department. Through May 1974, there have been an estimated 240 such cases. Those are calendar year cases, Mr. Chairman, calendar year numbers.

Monitoring is used when believed to be necessary and only under standards and procedures which conform to the current state of the law. Of the 1,080 monitorings in 1973, four cases of court-ordered surveillance of communications were conducted pursuant to title III of the Omnibus Crime Control and Safe Streets Act of 1968, and the remainder were consensual monitorings. That is consent by one party.

Mr. MOORHEAD. Consent by one party?

Mr. MACDONALD. Yes, sir.

Mr. MOORHEAD. But there are two parties to a conversation.

Mr. MACDONALD. There are two parties and the term "consensual monitoring" comes out of title III as being an exemption to the court-ordered requirement for tapping. These are known, therefore, as consensual monitorings as to which no prior court approval is required.

We at Treasury have committed ourselves to instituting periodic reporting procedures for those monitoring practices engaged in by enforcement components of the Treasury Department. We will continue to use these periodic check mechanisms to help evaluate the need for monitoring and the success of each type. Where a procedure does not measure up to the standards of providing a genuine operating need for Treasury, it will be improved or eliminated. I would be less than candid if I did not say that hearings such as this have some effect in continually goading us on in this.

Mr. MOORHEAD. We hope so.

Mr. MACDONALD. Our goal is to provide the American people with a professional quality of both service and law enforcement which is simultaneously effective and considerate of human rights. In order to do this, we must not treat cavalierly or otherwise abuse the rights of either our citizens or our employees. That is the combined and balanced standard of integrity and effectiveness that we have set for ourselves and which we believe we are achieving.

The few changes since our rather extensive report of last November are described in the materials submitted for the record. I will be pleased to answer any questions you may have.

I would like to add a couple of points which are not in the statement and which I think are relevant to the general picture.

With respect to the Secret Service, one division, the Executive Protective Service, is charged with the protection of the foreign missions here in Washington. They are very analogous to a police department, and they do record and monitor, as most police and fire departments do, all of their telephone and radio traffic. They keep this for 30 days and at the end of 30 days, they destroy it. One purpose is to know when somebody makes an emergency call with an address where they want the EPS to go, that the EPS has the right address and that they do not have to locate and ask the person for that address again.

Second, we have not included in our number of monitoring practices, those cases in which the White House switchboard switches to the Secret Service crank calls which sometimes are threats against persons at the White House. The Secret Service then monitors that call and talks to the individual. If the individual turns out to be harmless in the opinion of the Secret Service agent who is talking to him, he will erase the monitor in the next call that comes in. If the individual turns out to be a threat in the opinion of the Secret Service agent who is listening to the call that will then be recorded as one of the monitoring cases which we have reported here in this statement.

Mr. MOORHEAD. Does that complete your statement, Mr. Macdonald?

Mr. MACDONALD. Yes, it does.

Mr. MOORHEAD. We would now like to hear from Mr. Philip J. Budd, Chief Data Management Director, Veterans' Administration.

STATEMENT OF PHILIP J. BUDD, CHIEF DATA MANAGEMENT DIRECTOR, VETERANS' ADMINISTRATION; ACCOMPANIED BY WILLARD D. WHITFIELD, DIRECTOR, TELECOMMUNICATIONS SERVICE; JOHN P. TRAVERS, DIRECTOR, VETERANS' ASSISTANCE; AND KENNETH MEYER AND HOWARD DENNY, REPRESENTATIVES OF GENERAL COUNSEL

Mr. BUDD. I have with me Mr. Willard Whitfield, also Mr. Travers who is representing the veterans benefits and two officers from the general counsel's office, Mr. Denny is one and Mr. Meyer.

Mr. Chairman and members of the subcommittee, I welcome this opportunity to testify concerning, and furnish additional data on, the current telephone recording and monitoring and other surveillance practices of the Veterans' Administration.

The VA has for many years been cognizant of the need to respect the privacy of telephone calls. Complete instructions are available to

VA central office and field station personnel concerning agency recording and monitoring practices as detailed in our VA policy and practices. A copy of each of the relevant policy and practices was furnished to the General Accounting Office when we responded to their October 5, 1973 questionnaire survey which was undertaken at the request of this subcommittee.

Where mechanical or electronic recording devices are used by the VA, we comply with local State and Federal public utility regulations governing their use. The VA's applications for recording and monitoring on telephone facilities may be categorized as follows:

1. RECORDING BY MECHANICAL OR ELECTRONIC DEVICES

a. Verbatim record: When an exact transcript of a telephone conversation is needed for subsequent reference in conducting official business, the participants are advised at the beginning of the conversation that a recording will be made only with their agreement. A recorder is then connected to the line which is equipped with an automatic tone warning device. If the other party objects to the recording, the recorder is disconnected and the party is so informed.

b. Dictation: Many VA locations are equipped with dictation facilities which are interfaced with the VA or GSA telephone private branch exchange—PBX/Centrex—systems. At such installations VA personnel are able to dictate into centralized recording equipment for local official records. A typed transcript of their dictation is later prepared. Such systems are used in lieu of individual desk recorders or using secretaries for taking manual dictation.

c. Telephone answering-message recording: At selected locations the VA has installed telephone equipment which automatically answers incoming telephone calls, plays a prerecorded announcement to the caller and advises the caller that after hearing a tone the caller may place a message on the recorder. This equipment has proven advantageous where after normal business hours telephone coverage is required. It is also used at selected locations which are not fully staffed throughout the entire day.

2. MONITORING

a. By secretaries or other personnel: Officials of the VA are authorized to have secretaries or other personnel make a verbatim record of part or all of a conversation for future official use provided all other parties to the conversation are notified adequately of the monitoring.

b. Veterans assistance quality evaluation: Periodically selected Veterans Assistance Division officials are required to evaluate the quality of telephone interviews conducted by Veterans Assistance personnel.

During evaluation periods, the Veterans' Assistance personnel are notified that quality performance observations will be made on the calls they are handling. Silent observations where the transmitter is off circuit are conducted at only those field stations where it is not contrary to local or State public utility regulations since neither the caller nor the VA personnel are notified of the specific observation.

3. OTHER SURVEILLANCE PRACTICES

a. Clinical use of closed circuit television: Most of the recordings made of patients is done using cameras in the open, that is the patient can see the camera and is aware of being recorded and has previously consented to it.

With respect to hidden cameras there are only a few locations within the VA where this is used. One camera being mounted behind a mesh screen where the system was designed for equipment protection. To the best of our knowledge, only one of these installations exist. Its use is for violent patient observation while tranqualizing drugs are taking effect and to protect medical personnel when entering the room to observe that no one is hiding behind the door and to monitor the medical personnel in case of attack.

We have some areas where cameras are hidden behind one-way glass. This is done so that the patient is not distracted during interviews or discussions.

In all instances where this form of observation is used the patient has been previously advised that as part of their treatment they are being monitored or taped.

b. Security use of closed circuit television: All surveillance cameras used by the VA are in the open and are used to observe entrances, hallways, interconnecting passageways and other areas where 24-hour-a-day surveillance is required.

I believe it is of importance to repeat at this time VA's original response to part A of the GAO questionnaire regarding the use of polygraphs and psychological stress evaluators.

The Veterans' Administration does not make use of the polygraphs and psychological testing and evaluation equipment for any purpose except medical treatment. The Department of Medicine and Surgery uses various forms of psychological testing and evaluation equipment and techniques in the treatment of psychiatric patients. Since this equipment and its uses do not fall in the category covered by your guidelines, the answer to Part A is negative.

In part B of our response to the questionnaire we advised GAO as to the number of telephone transmitter cutoff switches—including push-to-talk—and their cost for fiscal year 1973. A new partial agency survey has been completed which indicates a reduction with only eight transmitter cutoff switches remaining at the VA Central Office, VACO, connected to telephones which have access to the commercial telephone network facilities.

We now have 571 push-to-talk switches at our field station locations and 14 at the Central Office in Washington, D.C., which are installed on the various dedicated private line voice conference systems, SS–1, connecting VACO and field stations. These dedicated conference systems are not accessible to the public and the push-to-talk switches have been provided upon the considered advice of telephone engineers to eliminate background room noises which experience has shown will seriously disrupt conferences. We are initiating a new agency survey to update other figures which were previously provided to GAO. The results of this survey will be provided to you at the earliest possible date. I am submitting a copy of the results of our most recent survey of the numbers of transmitter cutoff switches

at VACO and details of the number of push-to-talk switches on the SS–1 systems both at VACO and in the field.

I again thank you for this opportunity to appear and present the views of the Veterans' Administration on this important subject. I will be pleased to attempt to answer any questions that members of the subcommittee may wish to ask.

Mr. MOORHEAD. Thank you very much, Mr. Budd, for your testimony, all three of you.

[The document referred to follows:]

COMPARISON OF PREVIOUS REPORT TO GAO AND JUNE 1974 PARTIAL AGENCY SURVEY OF TRANSMITTER CUTOFF AND PUSH-TO-TALK SWITCHES

	Fiscal year 1973 report to GAO				June 1974 partial survey			
	Field		VACO		Field		VACO	
	Number	Amount	Number	Amount	Number	Amount	Number	Amount
Transmitter cutoff switches:								
VACO			55	$165			8	$24
SS–1 push-to-talk switches:								
DDM	5	$60	2	24	5	$60	1	12
D.M. & S	489	5,868	7	84	510	6,120	11	132
DVB	63	756	2	24	56	672	2	24
Total	557	6,684	66	297	571	6,852	22	192

Mr. MOORHEAD. I will start with Mr. Cooke. Mr. Cooke, when you engage in the Comsec monitoring, what kind of equipment do you use?

Mr. COOKE. That may be mechanical or electronic recording equipment or actual listening, sir.

Mr. MOORHEAD. But you are just picking up in effect an extension phone; there is not any tapping?

Mr. COOKE. No; as I indicated it may be actual recording equipment which is physically attached to the line for the purpose of Comsec.

Mr. MOORHEAD. Is this one of the devices like a broadcaster attaches to a telephone?

Mr. COOKE. Yes; it could be, a recording by any means, mechanical or electronic.

Mr. MOORHEAD. Not only thinking of the recording, but also the method by which the recorder is connected or attached.

Mr. COOKE. Mr. Sheerin, am I correct?

Mr. SHEERIN. Yes; it is a hard line attached to the telephone. I am Mr. Sheerin of the U.S. Air Force, a technical expert.

Mr. MOORHEAD. Mr. Cooke, the communications security listening, is this, as you described it, solely to DOD owned or leased wires?

Mr. COOKE. It is DOD owned or leased circuits that are part of the Defense Communication System, sir, and as I indicated, the primary use is in the command centers, op-centers, field exercises where we are concerned with the vulnerability of communications on an unsecure telephone line which, although one specific communication may not reveal much, a series of communications taken in toto could reveal classified information.

The other purpose of the Comsec monitoring is to suggest to the commander concerned better procedures to protect such classified communications.

Our rules, of course, say that there shall be no classified communications on unsecured phone lines, but there is a temptation to use the ease of the phone, and as I said, a whole aggregate series of conversations, in which anyone alone may not be helpful, could build up a pattern which demonstrates vulnerability.

Mr. MOORHEAD. Are you also testing to see whether officers or enlisted men are too relaxed in their conversations?

Mr. COOKE. Not the individual. As I pointed out, the directive expressly forbids the use of this for any type of court-marital or judicial proceeding against an individual. We are there to just state, if I may use the phrase, "security awareness" of the personnel and commanders on unsecure phones.

Mr. MOORHEAD. But it could be used to caution a particular officer you are being too casual in your conversations about matters that——

Mr. COOKE. It could be, Mr. Chairman, but my understanding is that once a communications security check has been made of a command circuit, the analysis does not reveal individual names.

Mr. MOORHEAD. Mr. Macdonald, first your testimony that you reduced the cutoff devices from 800 to 10, we applaud you for doing that. We think all of these devices should be kept at the absolute minimum to do the job.

In your Internal Revenue Service taxpayers' service program I understand your objective—which is to see that the Government employee is doing the best job he can—is there any way or any known device that could only listen in to the IRS employee talking and not listen to the citizen who has no way of knowing that he is being monitored?

Mr. MACDONALD. I refer that question to the IRS representative who is here who is in specific charge of that program.

Mr. MOORHEAD. It is a technical question?

Mr. MACDONALD. Yes, that is Mr. Jack Petrie.

Mr. PETRIE. Yes, sir.

I know of no such device, Mr. Chairman, that would allow us to listen only to the assistor. We could stand next to the assistor and hear his conversation out loud, but the probem here is we do not know what the question was, and unless it is such a bad answer like "Yes, you can claim your 5-year-old dog as an exemption," we would not know that it was a wrong answer.

Mr. MOORHEAD. I see.

I think that problem could be solved by instructing the personnel to repeat the question. Say you have asked me such and such and here is the answer, but there is no technical device that you know of?

Mr. PETRIE. Not that I know of; no, sir.

Mr. MOORHEAD. Now, Mr. Macdonald, I want to ask you about this consensual monitoring. You describe that as where one party to the conversation consents, the one party could be the Government employee, a member of the Secret Service.

Mr. MACDONALD. That is what it usually is, a setup device recording information on a counterfeiter if it is the Secret Service, or narcotics trafficker, if it is Customs, or an illicit still operator or illegal firearms dealer if it is Alcohol, Tobacco and Firearms. This is the usual case in connection with criminal investigations.

Mr. MOORHEAD. But the Crime Control and Safe Streets Act permits that kind of monitoring?

Mr. MACDONALD. Correct; as long as one party to the telephone conversation consents.

Mr. MOORHEAD. Without the consent of the private citizen?

Mr. MACDONALD. Without consent of the party whom we will call a citizen but who is invariably a suspected criminal or an informant of some kind. It is used only in connection with a criminal investigation.

Mr. MOORHEAD. This could be a two-part conversation——

Mr. MACDONALD. Exactly.

Mr. MOORHEAD. It is not a three-way conversation that the agent is listening in to a suspect talking to another citizen?

Mr. MACDONALD. No; there were four of those, as the testimony says, four of those without either party knowing. Those were all court ordered.

A typical case would be where an arrangement is being made by an agent posing as a buyer, let us say for example, of counterfeit money, who calls up the supplier and arranges to make the purchase. He will record that for later evidentiary purposes so that the other——

Mr. MOORHEAD. In these consensual calls, does the suspected citizen know that it is a Treasury agent calling?

Mr. MACDONALD. Absolutely not. If he did, it would not work.

[A chart referring to the above-mentioned subject was submitted for the record and follows:]

Calendar Year	ATF	Customs	IRS	USSS	Annual total
Consensual monitoring:					
1968	11	219	111	20	361
1969	17	137	164	12	330
1970	32	147	199	36	414
1971	70	106	290	117	583
1972	86	430	406	223	1,145
1973	107	234	545	190	1,076
Total	323	1,273	1,715	598	3,909
Court-ordered electronic surveillance:					
1968	0	0	0	0	0
1969	0	1	1	1	3
1970	0	2	0	1	3
1971	0	4	1	3	8
1972	1	10	0	6	17
1973	0	4	0	0	4
Total	1	21	2	11	35
Total, both consensual and court-ordered	324	1,294	1,717	609	3,944

Mr. MOORHEAD. Let me ask you about your testimony about the Secret Service—a typical case of the crank call that the White House transfers—it is one you decided not to erase. Do you then put all the information you can get out of that caller into a computer system?

Mr. MACDONALD. Yes; it is put into a bank system where, hopefully, that man will be identified; if not, certain characteristics of his will be in the file.

Mr. MOORHEAD. And also you keep a computer file?

Mr. MACDONALD. Yes.

Mr. MOORHEAD. I do not want to ask you any classified information, but can you give us any idea of the magnitude of that list of people considered dangerous to the President, Vice President and so forth? Again, I do not want to ask you if there is a reason it should not be made public.

Mr. MACDONALD. We would rather give that information in executive session.

Mr. MOORHEAD. All right. Maybe you can supply it on that basis.

Mr. Alexander?

Mr. ALEXANDER. Thank you, Mr. Chairman.

I would first like to, not observe, but I agree that there are legitimate government needs for investigations, especially along the lines of criminal investigations and national security reasons, and that is not why we are here.

I would observe, in addition, that it is alarming that most Federal agencies, apparently even the Department of Agriculture from the data—information that we have received here, which is not created for the purpose of protecting our national security by a long shot, are equipped to bug the citizens whom the agencies and departments were created to serve. When an American citizen seeks the assistance of his Government today by telephone, I think it is a fair presumption that his conversation stands a good chance of being monitored by electronic devices. This is more to me than can be illustrated by the expression "a kid with a new toy." It appears to me that our Government has been overcome by some sort of snooping mania or syndrome that corrupts the purpose for which many of our agencies were established.

I again appreciate the forthrightness with which you have appeared today and testified before this committee. I think that we are on the right track, and I hope to get to the bottom of this mania, and I hope that we can find some medicine to cure it quickly before it overcomes the whole nation.

Thank you, Mr. Chairman.

Mr. MOORHEAD. Mr. Gude?

Mr. GUDE. Thank you, Mr. Chairman.

Mr. Macdorald, have there been instances where personnel have objected to the fact that they know in certain instances that their conversations are being monitored in your agency?

Mr. MACDONALD. Are you speaking, Mr. Gude, of the IRS taxpayer assistance service? That is the only area that I am aware of in the administrative field where the Treasury does what might be known as monitoring, that is, using electronic devices to listen in without the knowledge of the other side.

Mr. GUDE. What is the general attitude of the employees to that type of monitoring?

Mr. MACDONALD. Let me refer that to Mr. Petrie.

Mr. PETRIE. Mr. Gude, I think the general attitude of our employees has been very receptive. They really feel they want to serve the taxpayer and in doing so are obligated to give the right answer. They feel if they can be constructive or caught in giving the wrong answer, this is very beneficial to them and the next time they will give the right answer. It is beneficial to them and they have been very receptive.

Mr. GUDE. Mr. Budd, can you respond to that same question?

Mr. BUDD. I think the answer is essentially the same, but I have Mr. Travers, the director of the program for the Veterans' Administra-

tion, and I suggest he would be better qualified to respond to your question.

Mr. TRAVERS. Mr. Gude, I agree with the man from IRS. Basically, our employees are aware this is a training mechanism by which supervisory personnel can develop by training guidelines to shore up people in weak areas, and again, if they find out the correct answer they will not make the same mistake the second time and so on.

In addition to the accuracy of information, we are concerned about courtesy, because this is something that the Veterans' Administration has been getting some flack on, lately.

We are also concerned about the fact that a VA counselor can, to some extent, control the interview and keep it on the subject at hand rather than going off all over the map and unnecessarily extending a phone call, because our phone activity is such that there are usually other calls waiting to be answered.

Mr. GUDE. Thank you, Mr. Chairman.

Mr. MOORHEAD. Mr. Cornish?

Mr. CORNISH. Thank you, Mr. Chairman.

Mr. Cooke, I notice in the regulations which you made a part of your testimony regarding telephone monitoring, in relation to communications security monitoring the states that DOD telephone communication systems shall constitute consent to communications security monitoring. Now, I assume by that, that you mean the employees of the Government have been notified that their phones may be monitored, but how about those people that they talk to on the outside, U.S. citizens, are they aware of any monitoring, are they given any caution or warning as to monitoring?

Mr. COOKE. They are not, Mr. Cornish. By the way, you are quite correct as to our own employees. For example, here is a typical sign which is on most phones which says "this telephone is for official business only, subject to monitoring, do not discuss classified information."

Now, as to the citizens not affiliated with the Department of Defense, as I noted, less than 1 percent of our telephones are monitored in any one given year and the phones selected for monitoring are generally not the phones on which a private citizen is calling into the Department. They are the phones in command centers, in op-centers and the like where there is a real possibility that classified information may inadvertently be released on unsecure lines. So I would suspect, obviously there may be exceptions, but I would suspect the vast majority of communications are internal to the dedicated or leased lines of the Department.

Mr. CORNISH. How about the mass of telephones like at the Pentagon, are those all included in the system?

Mr. COOKE. Categorically the telephone system is not subject to communications monitoring. We do not monitor for security the Defense Telephone System for Washington (DTS).

Mr. CORNISH. And yet, this is the center, actually where most of the important defense decisions—

Mr. COOKE. That is true, but they would not be on the circuits normally connected with DTS.

Mr. CORNISH. But are any of the Pentagon phones under security monitoring?

Mr. COOKE. As I said, none of the phones in the DTS. There are command phones in our command centers which go out to command

centers in the field, and I would certainly hope those would be subject at one time to communications security management. But our DTS, our phone system in the Washington area, let me say again, is not.

Mr. CORNISH. So that is completely safe, so to speak?

Mr. COOKE. And you may call me at any time.

Mr. CORNISH. I may call you with complete candor and privacy at any time?

Mr. COOKE. Yes.

Mr. CORNISH. I was going to say there are probably hundreds of pay phones that I recall in the Pentagon so that if anybody really wanted to leak any information of a sensitive nature, they would simply have to step out into the hall; is that not true?

Mr. COOKE. There are many devices by which people not only in Defense, but elsewhere can leak information and we tried to combat that by an active program by developing security consciousness in all our employees, military and civilian.

Mr. CORNISH. Let us take the telephones that you do monitor.

Mr. COOKE. May I point out these are not the same phones.

Mr. CORNISH. How many spies or security violators did you catch last year by this security monitoring?

Mr. COOKE. Bear in mind our purpose is not to catch spies or security violators but to judge the security procedures of the total system.

As I pointed out before in a response to the chairman, what we are really talking about in this area is that our efforts show it is a very rare occurrence when an individual telephone conversation results in a security violation of possible compromise of classified information. Instead, we are looking at a series of conversations, which compiled with others on the same or related subjects do provide an insight into classified projects, programs and operations. We are not out to catch an individual. We are out to judge the communications security of essentially command center lines that are not secure lines, and to recommend appropriate procedures to the commander concerned to improve that security if the survey deems it necessary.

Mr. MOORHEAD. Mr. Daniels?

Mr. DANIELS. No questions. Thank you.

Mr. MOORHEAD. Do you have further questions?

I will get back to you.

Mr. CORNISH. Thank you.

Mr. MOORHEAD. Mr. Phillips?

Mr. PHILLIPS. Mr. Cooke, I was very interested to note that the regulations you appended to your testimony all bear a date which is after the commencement of these investigations by this subcommittee. Does that mean that perhaps they were in response to our interest or were these merely updating of earlier regulations?

Mr. COOKE. Mr. Phillips, as I observed before, we welcome a responsibility in the oversight of this subcommittee. Going back to the date of your original hearings, we took into consideration the activities of this subcommittee at the time we developed these directives.

Mr. PHILLIPS. These are all dated from September to November of 1973. Does that mean that you had no regulations on various aspects of telephone monitoring prior to that date?

Mr. COOKE. No, as a matter of fact, as you know, our basic directive, 4140.1, on telephone monitoring is dated September 3, 1969.

The issues I attached were to update material in the same area for which we had previously furnished information.

Mr. PHILLIPS. For the record, these are the Defense Investigative Service, which issued regulations on November 20, 1973, the Defense Nuclear Agency which issued regulations on November 28, 1973, and the last one that you include here is the Defense Supply Agency, which is dated September 14, 1973.

Am I to understand that these three agencies did not have regulations prior to these days?

Mr. COOKE. Well, as your request stated: "If your component issued new and revised procedure regulations relative to telephone monitoring subsequent to our reply of October 10, 1973, please provide three copies of such issuances." I would like to look at each one to see whether it is a revision or a new publication; with regard to the Defense Investigative Service, it is a relatively new agency and this may be their first issuance.

Mr. PHILLIPS. These agencies would have been covered under your earlier directive?

Mr. COOKE. Yes, it applies to all DOD components and there is a standard phrase in it which says two copies of implementing regulations will be forwarded, et cetera.

Mr. PHILLIPS. Then these are merely refinements?

Mr. COOKE. Putting them into the services distribution setup. As a matter of fact, as Mr. Liebling points out, the DSR supersedes 57.1 of October 1967.

Mr. PHILLIPS. Thank you.

On page 2 of your testimony, Mr. Cooke, you indicate that the directives, two general directives of DOD on telephone monitoring and telephone interception and eavesdropping only apply within the United States, the Commonwealth of Puerto Rico and U.S. territories, but do not apply elsewhere overseas. Do you believe that the constitutional safeguards of U.S. citizens abroad who are part of the military complex stop at the water's edge? Why should they only apply here in the United States?

Mr. COOKE. You raise a very complicated legal question as to the way constitutional safeguards apply outside the United States, the Commonwealth, the district, and its territories and possessions. As you might well know, in response to a recent court case, the Department of Justice has supplied about a 100-page memorandum of law. This is in the case we discussed at one of your previous hearings, of the suit against the Secretary of Defense and others regarding certain alleged activities in Germany. I will be very pleased to supply at least the pertinent part of the Department of Justice's memorandum of law.

Mr. PHILLIPS. I think that might be helpful for the record, Mr. Chairman. I have in mind the current investigation of surveillance and eavesdropping activities of some U.S. personnel in West Germany who organized a support group for Senator McGovern during the 1972 campaign. We would also appreciate if you would supply for the record a statement, if it is not included in your earlier legal statement, as to the policy of the Department toward personnel engaging in such activities.

Mr. COOKE. I will supply a copy for your record.

[The brief of *Department of the Army* v. *Berlin Democratic Club* is in the subcommittee files.]

Mr. PHILLIPS. Of course, you are aware of Senator Ervin's investigation of domestic surveillance here in the United States over civilians?

Mr. COOKE. I have had the privilege of appearing before Senator Ervin earlier this year.

Mr. PHILLIPS. That is why I am about to ask this question because I know you are very familiar with it. Can you tell us if bugging and telephone monitoring were used in that operation by military intelligence units against civilians?

Mr. COOKE. Mr. Phillips, Senator Ervin's activities relate to difficulties arising out of situations we all found ourselves in the mid- or late-1960's. As a matter of fact, our DOD directive 5200.27 expressly forbids such practices except in very narrowly defined circumstances where there is an actual threat to personnel or property. I will be glad to furnish the statement I gave to Senator Ervin. We have undertaken many great improvements in control in that area, not the least of which is the addition of the very explicit policy directives. The investigative agencies are now under the control at the military department level of the Under Secretary of the military department. We have at the DOD level a Defense Investigative Review Council, that I happen to chair, with the Under Secretaries whose business it is to announce inspections and to insure these inspections are carried out. As Senator Ervin himself recognizes, there has been a marked improvement, I am using the Senator's words, with respect to these problems since he initiated the hearings.

Mr. PHILLIPS. We are all very glad to hear that. We are sorry it happened in the first place, and I am sure you are, too, at least I hope so.

Mr. MOORHEAD. Mr. Stettner?

Mr. STETTNER. Mr. Cooke, we have had the GSA people tell us they believe telephone monitoring of their people is not really necessary. We have in our file a letter from the Social Security Administration indicating that at the direction of the Secretary of Health, Education, and Welfare, their monitoring of approximately 250,000 telephone calls a week is being terminated.

We have information from the Internal Revenue Service that approximately 500,000 telephone calls a week are subject to their monitoring system. We do not have data from the Veterans' Administration on the volume of calls subject to monitoring, but we know that approximately 60 locations are doing this.

In light of what GSA and SSA have done, would you explain why there is the continued need for your two agencies to continue this practice?

Mr. MACDONALD. Which two agencies?

Mr. STETTNER. Treasury and Veterans' Administration.

Mr. MACDONALD. Continued need—I am sorry.

Mr. STETTNER. To continue with the widespread monitoring of taxpayers and veterans of annuitants' call to your two departments?

Mr. MACDONALD. Well, I suppose that there are—let me say first in response to what Mr. Alexander said so eloquently that we also agonized over these problems and have agonized more since this com-

mittee has started its questionnaires and its hearings and that has caused us to reevaluate our administrative monitoring practices and the result has been quite startling. We agonize in the criminal enforcement area, but we are not at present embarrassed over the monitoring and wiretapping policies and activities that we administer in that area.

In the IRS situation, there are two points, I think, that might be considered. One is the employee and the other is the taxpayer. I hope that as far as the employee is concerned, we have reduced the matter as much as you can reduce it to one of consent. If we had the money, we could probably monitor all the calls and assure that everybody got exactly the right advice. Then we could be certain that there was consent because the employee would know that he was being monitored at all times. This program is trying to achieve as much of that result as we can at a lesser cost.

As far as the taxpayer is concerned, I believe, and I think this is a legitimate interest, that the taxpayer in most cases never gives his name. The only time he usually gives his name, it is my understanding, and correct me if I am wrong, is when he is asking for a form of some kind or he is asking a question that the service agent cannot answer and therefore, he says, "I have got to call you back. I have got to go back and talk to my supervisor because your question is too complicated for me to answer."

I suppose that the way we feel about it, that supervisor has just the same responsibility as the original service agent does. They are both involved with the taxpayers calling in, whether one is listening or two are listening, they are both part of the same organization. While I agree that you could argue the other way, nevertheless, it seems to us that the benefits from trying to assure accurate service in a situation where the law, as everyone here knows, is extremely complex, outweighs any possible infringement of that particular individual's rights. It is a judgment call.

Mr. STETTNER. I am certain there would be less objection on the part of the subcommittee if the taxpayer knew all this and had the option of expressing his own view.

Mr. BUDD. I would like to indicate from the veterans standpoint, we have a situation that needs attention. It represents the best solution that we know of at this time. We have as you point out almost 60 locations where we handle our veterans benefits, exclusive of the medical facility hospitalization. We have some 29 million veterans. We provide to our veterans a telephone capability so anybody can reach us at Government cost, we have WATS lines in all States, practically, not all at this point so our veterans can call in. Once they call in we have to be sure they get quality service. The sole purpose of the Veterans' Administration is to make certain that the veteran and his dependents get quality service. We do not know of a better way to do this.

As you can imagine, this is a massive operation with lots of employees and there is turnover. We do our best to train employees to carefully select employees, but we also know with employees there are always some deficiencies and lapse in this type of employment there has to be a way for managers and supervisors to assure themselves that everybody is doing the job properly and find out what our weaknesses are. We will never be perfect, but we can certainly aim for it. The sole purpose the Veterans' Administration has is to try to improve the service we render.

Mr. MOORHEAD. Mr. Kronfeld.

Mr. KRONFELD. Thank you, Mr. Chairman.

I noticed Mr. Budd referred in his statement to the fact that VA complies with local, State, and Federal public utility regulations. You may be aware that the State of Georgia Public Utility Commission requires all users of monitoring devices to be licensed by the State and in most cases to have an asterisk placed next to their name in the phonebook alerting citizens that calls to these numbers may be monitored. In many cases, looking at the Atlanta phonebook, we find that private businesses do engage in this employee service monitoring.

I think it is commendable that the Veterans' Administration, although not legally required to abide by this regulation, has done this.

I wonder why IRS has refused in Georgia to comply with the licensing requirement or the notice requirement, recognizing that you are probably not legally required to. Can you explain the policy reasons for that?

Mr. PETRIE. According to the best reasons I have, the Attorney General for the State of Georgia has given a ruling that the Internal Revenue Service or any other Federal agency is not required to be licensed. I guess that would cover the first part of the question.

I do understand we will be asterisking our numbers in the telephone book in the future.

Mr. KRONFELD. You will be?

Mr. PETRIE. That is my understanding.

Mr. KRONFELD. I understand the legal aspects of the situation. You are not required to do so. That is fairly clear. But are there any policy reasons why IRS would not want to comply when other agencies, such as the VA, have complied?

Mr. MCBRIEN. If I may, I think a response to that would be that once we have done that, we have said in effect, that the Federal Government and its agencies are no longer the supreme law of the land under the Constitution, and that we will, in the future, be subjecting ourselves to all these licensing procedures. It is a judgment call, but there is a legal premise to it. It is not essential to subordinate the Federal Government in such a case, especially if we do go ahead and conduct ourselves in a way that does not infringe upon citizens' rights.

Mr. KRONFELD. You do not want to get yourselves in a situation of having to comply with other obvious State standards.

Mr. MCBRIEN. No; I said it was a matter of whether the Constitution and the laws and treaties of the Federal Government are going to have supremacy over those of the State and local governments.

That is a constitutional doctrine.

Mr. MOORHEAD. Mr. Cornish?

Mr. CORNISH. Thank you, Mr. Chairman. You know, I am just sitting here wondering if all this service monitoring is designed to improve the quality of service rendered to the taxpayers, why we do not just monitor the calls of all Government officials to check on the performance of their duties, not just the Indians, but the chiefs, too. I do not know whether you have any comment about that or not. That is a little grist for the mill that you might want to——

Mr. MACDONALD. It certainly is.

I had to check the figure of 500,000 calls per week that the IRS did in monitoring and it is quite accurate. There are 21.6 million calls

that the IRS receives in its taxpayer service, which I think partially explains the fact that they sprinkle their supervisory monitoring around and, of course, I do believe if there is any area where uniformity has got to be obtained and a quality for all our citizens that certainly is one of them, in advice on the payment of their taxes.

As Mr. Stettner said, these are 500,000 calls per week that are subject to monitoring. That is not the number that are monitored.

Mr. STETTNER. Right, but any one of them might be.

Mr. MACDONALD. Anyone of which might be, correct.

Mr. CORNISH. I wonder if it is necessary for the Treasury Department or the IRS to continue this practice, and I doubt that it is, but if you find it to be necessary would you have any objection at all to—on the cover of the tax form which is sent out to taxpayers—to list the numbers that were to be called, whether you could also caution the taxpayer that his call may be monitored for these purposes so that he knows?

Mr. MACDONALD. That is an idea worth considering. I will pass that on to Mr. Alexander. Would you like a response from him?

Mr. CORNISH. Yes, Mr. Chairman, I think that would be appropriate if so desired.

[A letter submitted for the record follows:]

DEPARTMENT OF THE TREASURY,
INTERNAL REVENUE SERVICE,
Washington, D.C., July 3, 1974.

HON. WILLIAM S. MOORHEAD,
Chairman, House Subcommittee on Foreign Operations and Government Information, House of Representatives, Washington, D.C.

DEAR MR. MOORHEAD: Treasury Assistant Secretary David Macdonald asked that I respond to you relating to hearings on June 13, 1974 of the House Subcommittee on Foreign Operations and Government Information. Specifically, he asked that I reply to Mr. Cornish's suggestion that tax packages include a notation that the service monitor, for quality purposes, a random sample of tax information telephone calls.

I have discussed this suggestion with my staff and we are in complete agreement with it. I have asked that each tax package be so noted for the next filing period.

I would like to take this opportunity to express some further views on our taxpayer service telephone monitoring. I share your concern that governmental agencies should not engage in activities that infringe on the right of privacy of any citizen. I do feel strongly, however, that our taxpayer service monitoring does not fall into this category; rather it serves as a very real benefit to our citizens through the improved quality of answers given to their tax inquiries.

In a great majority of calls that are monitored, the taxpayer remains completely anonymous. Only the taxpayer's question and the tax assister's answer is heard. When an incorrect answer is given, immediate corrective action can be taken. In addition, periodic (sometimes daily) training sessions are held with all tax assisters covering areas where discrepancies are found. Often, through monitoring, supervisors can became aware of an unusual problem affecting a large number of taxpayers in the area, and alert all tax assisters in the event of similar calls. Finally, through monitoring, we can determine if our tax assisters are providing courteous service in responding to telephone inquiries.

In summary, I feel that supervisory monitoring of tax information calls is a vital part of our overall taxpayer service program and its objective to provide quality service to the taxpayer. I appreciate this opportunity to respond to you on this most important subject.

With kind regards,

Sincerely yours,

DONALD C. ALEXANDER,
Commissioner.

Mr. MOORHEAD. Mr. Phillips?

Mr. PHILLIPS. No further questions, Mr. Chairman.

Mr. MOORHEAD. Mr. Stettner?

Mr. STETTNER. No, Mr. Chairman.

Mr. GUDE. I would just like to direct one question. How analogous is this type of monitoring to the type of supervision of employees who provide information to citizens who come personally to IRS offices or VA offices? Aren't these employees subject to supervision as far as rudeness or accuracy of information is concerned?

Mr. PETRIE. Yes, sir. Many of the people that work on the phone do so 8 hours a day. That is their job. So by monitoring, we are able to tell on a sample basis whether these persons are accurate, are courteous, et cetera.

In the walk-in area, a supervisor can walk behind or mingle with and overhear the answers being given and in the same way determine the same information, strictly by listening to what the taxpayer assister is saying.

Mr. GUDE. The employee who is giving this information is perfectly aware that there is a supervisor present and that the information he is giving might well be heard by the supervisor.

Mr. PETRIE. Yes.

Mr. GUDE. A citizen who has occasion to either call the Veterans' Administration or IRS for a piece of information may be making one of his very rare contacts with Government over a long period of time. If the citizen receives a rude response, a discourtesy, or receives misinformation, this constitutes his impression of Government. I think there is something very important to be said for this technique. I think Government employees are interested that their part of Government be well received by the citizenry. The large majority have a pride in the quality of their work as Government employees.

Mr. PETRIE. Yes, sir. I would like to add one point, In the walk-in area where the supervisor is behind, he does also listen to the taxpayer's question which is similar to his listening to the question on the phone.

Mr. GUDE. Thank you, Mr. Chairman.

Mr. MOORHEAD. Mr. Kronfeld?

Mr. KRONFELD. No questions, Mr. Chairman.

Mr. MOORHEAD. Thank you very much, gentlemen. We appreciated your testimony.

[Questions submitted to the Department of Defense, the Veterans' Administration, the Department of the Treasury and the replies thereto follow.]

QUESTIONS FOR THE DEPARTMENT OF DEFENSE

Question 1. Testimony describing DOD's communications management monitoring includes the statement that service observation is conducted largely by computer analysis and peg count methods rather than by actual listening to telephone conversations in progress. Under what circumstances is such service observation done by actual listening to telephone conversations?

Answer. Service observation is only conducted by audio means when the more modern electronic or computer facilities are not available. In many of our base or installation telephone systems the only method of quality control and management supervision is through the facilities of supervisors' switchboards. In such in-

stallations the supervisor' board has equipment which allows a supervisor to listen to activities on any of the subordinate operators switchboards. Component instructions prohibit the supervisor from "listening" to the conversation. The supervisor's action is limited to determining if calls are placed promptly and courteously, and that the quality of the circuits is adequate. Service observation monitoring is not recorded on tape.

Question 2. When telephone calls are monitored (and recorded either mechanically, electronically, or manually), is a "true" copy of the conversation furnished to each of the parties who has consented to the monitoring?

Answer. The DOD directive does not require that transcripts or "true copies" be provided all parties involved. Of course, all involved must be informed of and agree to the recording; however, the dissemination of transcripts is left to the dictates of those concerned.

Question 3. Isn't each party to such a monitored (i.e., recorded) conversation equally concerned with knowing exactly what agreements were reached, arrangements made, etc?

Answer. We agree that persons involved in recorded conversations involving decisions and other important actions would be concerned with the exact record of the transaction. However, the Department has not found it necessary, to date, to prescribe procedures for the preparation and dissemination of recordings. Again, we have left this to the desires of the parties involved.

Question 4. Is it safe to assume that many transmitter cutoff devices are installed in administrative or executive areas, as opposed to noisy industrial-type areas and command and control centers?

Answer. We agree that some transmitter cutoff devices may have been installed in offices or administrative areas for convenience purposes. However, our prior inquiries to our components produced the information that such cutoff devices were used primarily for the security of classified information and to reduce feedback in noisy areas.

Question 5. In light of testimony previously given the subcommittee, would it not be a desirable course of action for your agency to reassess the current, continued need for so many of these devices?

Answer. We agree that a review of our needs for transmitter cutoff and similar devices might be in order. As we review our policy directives with respect to monitoring, we will give full consideration to inserting appropriate provisions for the acquisition and use of these devices.

Question 6. What is the most common use or application of those telephone recording devices that are not wired into the circuits, and are not equipped with beepers?

Answer. Those recording devices (offline) used in conjunction with telephones in accordance with the provisions of our DOD directive 4640.1, are used primarily by the Armed Forces radio and television service under provisions of telephone common carrier tariffs. The large number of such offline telephone recording devices not equipped with beepers is accounted for by the inclusion of our inventories of investigative recorders. These recorders are used in accordance with the provisions of 18 U.S.C. 25–11, the Attorney General's memorandum of October 16, 1972, and our DOD directive 5200.24.

Question 7. What is the special need at the National Security Agency for the Alston Model 370/389 service observing equipment, since NSA is not the type of Government office that large numbers of citizens would be telephoning, seeking information on a relatively limited subject matter area, as is the case of IRS, VA, and SSA?

Answer. The Alston 370/389 service observation equipment was purchased in 1973 for the sole purpose of conducting communications management monitoring under the provisions of DOD directive 4640.1, "telephone monitoring."

Question 8. Telephones at the FAA flight control centers and the Coast Guard search and rescue centers have recording devices with audible signals wired into the telephone circuits, to provide an uncontroverted record of emergency communications. In contrast, telephones at the Army's Military Police Operations Desks, countrywide, which also are equipped to record emergency telephone conversations, are not required to include audible warning signals, notifying callers-in of the recording. What is the rationale for this Army policy and practice?

Answer. We were not aware that all of the switching systems and telephones at FAA Flight Control Centers and Coast Guard Search & Rescue Centers which had monitoring equipment were provided with beeper devices. However, with respect to the use of recorders on military police operations center telephones, we have found that the use of audible signals or beepers inhibits the reporting of crimes or other indications of suspicious activities. To our knowledge, it is standard practice throughout the country for police, fire, and rescue switchboard recorders not to be equipped with beepers. We do provide printed and other public notice of the fact that our operational telephones in police stations may be monitored.

VETERANS' ADMINISTRATION RESPONSE TO SPECIFIC QUESTIONS FROM THE FOREIGN OPERATIONS AND GOVERNMENT INFORMATION SUBCOMMITTEE OF THE COMMITTEE ON GOVERNMENT OPERATIONS, HOUSE OF REPRESENTATIVES

1. Where exact transcripts of a telephone conversation are made, in conducting official business, with the agreement of participants (p. 2 of your prepared statement), what is your policy and your practice with respect to furnishing a copy of the transcript to the other party?

Response: Agency policy does not require furnishing a transcript of the conversation to the other party. When such a transcript is desired it is this agency's practice to provide a copy upon request.

2. If the other party objects to having his conversation recorded, does this make the transaction of business impossible?

Response: No, transaction of business is possible even though the other party objects to having his conversation recorded. However, this might well cause a delay in providing an appropriate response in service to veterans.

3. In what respect does that absence of recording/transcript compromise any legal rights of the Veterans' Administration in transacting its business?

Response: We are not aware of instances in which the absence of a recording/transcript compromised the legal rights of the Veterans' Administration in transacting its business.

4. Does this occur frequently? When was the last such suit lost, where absence of an exact transcript resulted in court decision against the Government?

Response: See answer to question 3.

5. Could the telephone calls received by veterans at hospital centers be subject to monitoring?

Response: Patient telephone calls are usually completed over "pay station" telephones which exclude access by VA staff. When official telephone calls are completed through the hospital's private branch exchange (PBX) telephone system, it is technically possible for calls to be monitored. However, it is not agency policy to permit the monitoring of patient calls.

6. If veterans were to call their physicians or attorneys, might such calls be monitored?

Response: No, any personal calls placed by a veteran would not be monitored by VA.

7. What current plan does the Veterans' Administration have for expanding the scope of its monitoring of telephones (through use of automatic call-directors), at locations not yet so equipped?

Response: Currently 12 VA Regional Offices/Centers are equipped with automatic call-directors (technically known as Automatic Call Distributors or ACD's) to handle veterans' requests for information and assistance. It is anticipated that 18 additional ACD's will be installed to improve service to veterans. Monitoring (service observing for training purposes) is expected to continue as presently defined in agency policy and practices. Two VA Hospitals have operational ACD's for scheduling outpatient clinic appointments. Additional ACD's may be installed at VA Regional Offices/Center locations when the volume of incoming public monitored.

8. How large a VA operation must exist before automatic call-director equipment is installed?

Response: Automatic call distributor equipment is authorized for installation at VA Regional Offices/Center locations when the volume of incoming public calls reaches 20,000 per month. It is expected that ACD equipment will be installed at hospitals/clinics that schedule 100,000 or more outpatient visits per year.

9. Of the three agencies with teleservice centers (IRS, VA, and SSA) only the VA has elected not to have supervisors discuss with the individual employee the quality of his performance. Please explain the rationale behind such a decision.

Response: The foregoing statement is incorrect. For training purposes, the VA has elected to have supervisors discuss with the individual employee the quality of his performance to maintain the highest possible quality of service to those who telephone the VA for information, advice and assistance.

10. Since the supervisor doing the monitoring does not discuss his observations or views with the employee observed, how does the practice contribute to training of an individual or upgrading the quality of service rendered by that individual.

Response: See answer to question 9.

11. When do you think that your study of need and justification for those hundreds of such devices in the field will be completed and the results made available to the subcommittee?

Response: It is expected that the results of our latest survey will be forwarded to your office by September 15, 1974.

12. There appears to be an inconsistency of policy in that agreement of all parties is needed for connection of a recorder when used to make a verbatim record whereas secretarial monitoring and making of a verbatim record (in whole or in part) needs only notification to all parties to the conversation. Please explain that difference, if a difference does in fact exist.

Response: We appreciate the apparent inconsistency you drew from two paragraphs of the testimony of the Veterans' Administration witness at the June 13, 1974 hearing before the committee. However, no such inconsistency exists since the same policy is followed in the two situations mentioned. The apparent inconsistency arose from the choice of language employed. If a recording of a conversation is to be made or if a secretary or other person is to make a verbatim record of part or all of a conversation, the participants are advised of this fact at the beginning of the conversation. If a party objects to either type of recording of the conversation, the recording (whether by machine or by a secretary) is not made and the parties to the conversation are so informed. While we recognize that in the case of a secretarial transcript, the parties are not reminded periodically by an automatic tone warning device, we feel sure that if a given party to the conversation questions the agency participant's agreement not to make a secretarial transcript, he or she would terminate the telephone conversation.

Response to Mr. M. Stettner's June 20, 1974, telephone request to Mr. P. J. Budd:

During the 12 month period, April 1, 1973, through March 1974, 13,750,984 incoming telephone calls were received by Veterans Services Division personnel at VA Regional Offices/Centers. Of this number 22,118 service observations were made.

TREASURY DEPARTMENT

Question 1. What with 263 induction coil devices (not wired in) how is there any insurance that conversations are being recorded only when both parties agree?

Answer. An examination of the Treasury Department's report of November 28, 1973, to the subcommittee reveals that the 263 induction coil devices described therein are for use by the law enforcement components of the Treasury Department in conducting criminal investigations in which one-party consensual monitorings of conversations are necessary.

In our June 13, 1974, testimony before the subcommittee, we stated that 1,076 instances of consensual monitoring by Treasury enforcement agents occurred during calendar year 1973. The use of induction coil devices is one method of accomplishing this investigative technique.

As I testified and as Mr. McBrien of my office advised Mr. Kronfeld of the subcommittee's staff, consensual monitoring is a longstanding criminal investigative technique in which a conversation is monitored with the prior knowledge and consent of a law enforcement agent, informant or other person but without the knowledge and consent of the criminal suspect. Consensual monitoring is used for corroboration of informant allegations, for preservation and corroboration of incriminating conversations to serve as best evidence, to protect informants and undercover agents, and to coordinate the timing of raids on criminal operations.

A consensual monitoring can be accomplished through use of a transmitting or recording device on the person or premises of a consenting undercover agent or other person, or it may involve an agent listening in on an extension phone or using a recorder with a telephone (by means of an induction coil device) while a consenting informant or other individual is one of the parties to the conversation.

This important law enforcement investigative technique is carried out under standards and procedures promulgated by our Treasury enforcement components and the Justice Department. These, of course, conform to the statutory requirements of 18 U.S.C. § 2511 (2) (c) and the decisions of the U.S. Supreme Court in *United States* v. *White*, 401 U.S. 745 (1971); *Lopez* v. *United States*, 373 U.S. 427 (1963); *Rathbun* v. *United States*, 355 U.S. 107 (1957); and *On Lee* v. *United States*, 343 U.S. 747 (1952).

Consequently, the 263 devices described in our November 1973 report are not intended to be used with the consent of all parties. We believe that the internal procedures of our bureaus and the integrity of our Treasury enforcement personnel are the best assurances we have that this law enforcement technique and the equipment to accomplish it are not used improperly. We should also note that the 1961 version of administrative circular No. 41 and the December 13, 1973, revised version, which we submitted to the committee, are applicable to administrative telephone conversations only and not to those involving criminal law enforcement investigations.

As the materials submitted with our June 13 testimony indicate, our law enforcement bureaus now report an inventory of 361 induction coil devices.

Question 2. More than $600,000 was reported to the subcommittee as the acquisition cost of recorders, service observing devices, and nontelephone bugging equipment (exceeded only by DOD). What are the peculiar needs of the Treasury Department which dictate that it use so much of this type of equipment?

Answer. A breakdown of the $600,000 figure reported to the subcommittee in November 1973, reflects that $120,000 of the total is for rental of taxpayer service program telephone monitoring equipment through which IRS taxpayer service representatives are, from time to time, monitored by supervisors in order to assure accuracy, completeness and courtesy to citizens who seek tax assistance from the Internal Revenue Service. The taxpayer service program was explained in detail during our June 13 testimony, in Commissioner Alexander's July 3 letter, and in the answers to questions 3–11 herein.

The remaining $480,000 is attributed to the law enforcement components of four Treasury bureaus: Bureau of Alcohol, Tobacco and Firearms, U.S. Customs Service, Internal Revenue Service, and U.S. Secret Service. As you are aware, the cost figures involved respond to question No. 7 of the October 5, 1973, questionnaire from the General Accounting Office:

> Please furnish the best available estimate of the total cost of these (a) recorders and attachments, (b) telephone service observing devices, (c) nontelephonic bugging devices.

The enforcement bureaus' responses, therefore, include simple devices (such as induction coils), all tape recorders, and the expensive and sophisticated body recorders used for many consensual monitoring and equipment for nonconsensual court-ordered electronic surveillance. Tape recorders which are used principally for nonmonitoring functions, but which could be used for monitoring, were included in the estimates of most bureaus and accounted for an estimated $80,000 of the $600,000 figure.

The $400,000 worth of monitoring equipment is divided among four major Federal law enforcement agencies which carry about 50 percent of the Federal law enforcement work load. The equipment involved is spread among the hundreds of offices throughout the United States from which the Treasury Department performs its law enforcement duties.

As we testified, the Treasury Department, through the Secret Service, has the responsibility for protecting the President, the Vice President, and other important functionaries against physical violence. The Secret Service also is the vehicle through which Treasury is charged with protecting the integrity and confidence of the Nation's currency by suppressing counterfeiting and forgery of Government checks. Through the IRS, Treasury is required to enforce the Nation's revenue raising laws, in order to assure that nonfilers and fraudulent filers of income tax returns are discovered and prosecuted. Through the Customs Service and the Alcohol, Tobacco and Firearms Bureau, smugglers, illicit still operators, and illegal dealers and handlers of firearms are brought to justice by Treasury enforcement personnel.

With these responsibilities in law enforcement, $400,000 is a very small investment in highly necessary and appropriate investigative equipment.

Question 3. Does the IRS employee working at the teleservice center make substantive notations of conversations coming in, perhaps in connection with IRS

interest in the subject matter areas on which callers most frequently raise questions?

Answer. We do not make substantive notations of conversations on incoming calls except when some notation is made about the nature of the inquiry because a call back is necessary. Most questions do not require a call back; however, there are occasions where extensive research is required to completely answer the question. This procedure is not limited to telephone inquiries, but is applicable to both telephone and walk-in inquiries. When a call back is required, it is necessary to note the question in detail and to obtain the taxpayer's name and phone number or address.

We also have a procedure whereby the subject matter of both telephone and walk-in inquiries is categorized to determine the type of questions most frequently asked. Examples of categories are filing requirements, exemptions, refunds, etc. Data is collected on a sample basis with at least one district within each of the seven regions participating each week. Employees selected note only the category of the questions asked, not the name of the taxpayer.

Question 4. Aren't there circumstances where the question cannot immediately be answered, and it is necessary for an IRS employee to call back to convey information?

Answer. Yes, as mentioned in answer 3, there are instances when it is neither feasible nor desirable to hold a taxpayer on the line or in the office while research is performed on a complex question. Additionally, when a caller has questions relative to a post-filing problem, it may be necessary to research the specific tax return prior to attempting to answer the taxpayer's question or give other advice. In these cases, the employee would call back or write the taxpayer.

Question 5. Would he not then be expected to record the name and telephone number of the incoming caller and when the question was researched, he would return the call?

Answer. Yes, as explained above, the employee would note the name and telephone number of the incoming caller and when the question was researched, he would return the call.

Question 6. Would that then be a means for associating an individual's name with a specific tax matter or problem?

Answer. No, the employee only notes the taxpayer's name for call back purposes. Upon the return call to the taxpayer and the satisfaction of his question, the documents relating to the call are destroyed.

Question 7. Is it not possible, at your telephone service center operations, to issue instructions that all inquiries relating to a particular subject be transferred to a single monitoring position for disposition?

Answer. It is possible through the use of telephone equipment to transfer incoming calls to a single answering position and in certain very complex areas such as questions about Estate and Gift Tax, Pension, Trust and the recent Stabilization program, we do utilize special referral stations. However, since we handle such a broad range of questions, and in many instances taxpayers have several questions that can range between several subjects, it would not be practical to set up a system by subject matter.

Question 8. Would this not then overcome the frequently referred to "control" imposed by random assignment of incoming telephone calls through automatic call distributor equipment?

Answer. No, the purpose of the automatic call distributor is to automatically distribute the incoming taxpayers' calls to answer positions in the order in which they are received. Additionally, the automatic call distributor has transfer capabilities among employees' supervisors and/or technical backup. As mentioned above, the caller will first discuss his problem with the generalist. If the question is not within the technical capabilities of the employee, then he or she should refer the caller to the specialist who is more technically proficient and can answer the specific question.

Question 9. Why was it necessary recently to supplement the regular service monitoring practices by the introduction of "planted" or "test" questions called into the teleservice centers by Treasury employees?

Answer. The use of "planted" or "test" questions is not a recent practice, but has been in use for several years. This practice is one method of determining the accuracy and courtesy of our responses and the effectiveness of our training courses. While we find the test questions are a useful tool in measuring accuracy and courtesy of responses, we find that they do not measure up to the real life situations presented by taxpayers. Thus, the test questions are only used to supplement the regular monitoring practices.

Question 10. Did those employees calling in these questions make written reports on questions asked, identifying the individual who received the call, and evaluate that employee's response in terms of courtesy, correctness, etc.?

Answer. Employees who made test calls did evaluate responses in terms of courtesy and correctness. Tables are maintained on the number of calls made by subject matter and the number of correct or incorrect answers. In those instances where the employee was blatantly discourteous or provided incorrect information, the supervisor was advised so that corrective action could be taken to avoid a recurrence.

Question 11. What assurance is there that this practice did not lead to disciplinary action against individuals?

Answer. We know of no disciplinary action that was taken during the past filing period as a result of a sample test call. The purpose is to let the supervisor know that incorrect information is being furnished or that the service does not measure up to the degree of courtesy that we expect an employee to meet. We expect the supervisor to counsel the employee and to help him improve his performance.

Mr. MOORHEAD. The subcommittee is now adjourned.

[Whereupon, at 12 noon, the subcommittee adjourned, to reconvene subject to the call of the Chair.]

○

END