Exploding The Phone

www.explodingthephone.com

Bibliographic Cover Sheet

db480

Title	**Surveillance: Hearings before the Subcommittee on Courts, Civil Liberties, and the Administration of Justice of the Committee on the Judiciary of the United States House Of Representatives**
Date	1975-02-18
Author(s)	Caming, H. W. William (United States House of Representatives)
V/I/P	p. 207
Abstract	Testimony of H. W. William Caming, attorney, General Departments, American Telephone and Telegraph Company, and John E. Mack, Director, switching administration and maintenance systems Center, Bell Telephone Laboratories, and Earl Connor, Staff Supervisor, Security, Chesapeake and Potomac telephone company, regarding the Greenstar toll fraud surveillance system.
Keywords	H. W. William Caming; John E. Mack; Earl Connor; Greenstar; blue box
Notes	Includes appendix with: speech given by Zane Barnes, president, Southwestern Bell on wiretapping; C&P Telephone pamphlet on secrecy of communications; copy of St. Louis Post Dispatch article on Greenstar; copy of Washington Post article on Greenstar and AT&T security; and a transcript of a television interview with Caming

Mr. BADILLO. When do you investigate the political views to find out how they propose to carry out their objectives, if there are any number of organizations who want to carry out their objectives in different ways.

Mr. SHATTUCK. Well, criminal conspiracies can be conducted with political overtones, but I think that the demonstration that would have to be made by the investigative agency, in order to get the information it was seeking, would have to be similar to the demonstration it would have to make to a magistrate if it were an organized crime case. There would have to be some showing that there was criminal activity flowing from the other, lawful activity of a particular group, and I think that any lesser standard than that invites the kind of abuse of discretion that we see in many of these cases.

Mr. BADILLO. Yes; but the point is in that case it would not be against a total ban, as you indicated here, but where there is a probable cause, it would be permitted, is that not so?

Mr. SHATTUCK. That is right.

Mr. KASTENMEIER. If there are no further questions, on behalf of the committee I would like to express our gratitude to you both for the very lengthy but extraordinary helpful presentation. This is the beginning of a series of hearings today, which I anticipate will lead to legislation within the subcommittee, and we may have reason to again ask for your assistance at some point.

And so I conclude today by expressing our thanks to you both.

Having concluded with today's witnesses, the subcommittee is adjourned.

[Whereupon, at 1:25 p.m., the hearing was recessed, subject to the call of the Chair.]

SURVEILLANCE

TUESDAY, FEBRUARY 18, 1975

U.S. HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON COURTS, CIVIL LIBERTIES,
AND THE ADMINISTRATION OF JUSTICE
OF THE COMMITTEE ON THE JUDICIARY,
Washington, D.C.

The subcommittee met, pursuant to notice, at 10:10 a.m., in room 2141, Rayburn House Office Building, Hon. Robert W. Kastenmeier [chairman of the subcommittee] presiding.

Present: Representatives Kastenmeier, Drinan, and Pattison.

Also present: Bruce A. Lehman, counsel; Timothy A. Boggs, professional staff member; and Thomas E. Mooney, associate counsel.

Mr. KASTENMEIER. The subcommittee will come to order.

This morning the subcommittee will continue its hearing on the issue of surveillance techniques, concentrating today on the practices of the Nation's major telephone company, American Telephone & Telegraph. We are very pleased to have three witnesses before the subcommittee: Mr. H. W. William Caming, attorney for security matters for A.T. & T., Mr. Earl Connor, staff supervisor for security of the Cheasapeake & Potomac Telephone Co., an operating company of A.T. & T., and Mr. John E. Mack of Bell Laboratories.

Mr. Caming, of course, testified before this subcommittee last spring regarding company policy on wiretapping and electronic surveillance. At that time, Mr. Caming stated, "I wish to stress the singular importance the Bell System has always placed upon preserving the privacy of telephone communications."

Since that time, however, there have been a number of serious allegations raised regarding the Bell System's commitment to the preservation of privacy and its practices in the area of surveillance.

First: It has been revealed that the Bell System randomly recorded over 30 million phone calls between 1965 and 1970 in order to develop a procedure to apprehend fraudulent callers.

Second: A former executive of the Southwestern Bell Telephone Co. has charged that employees of that company commonly exchanged wiretap information with Federal and State law enforcement personnel without a court order as required by title III of the Omnibus Crime Control and Safe Streets Act of 1968.

Third: There was evidence presented during this committee's recent impeachment proceedings indicating that Bell System staff directly assisted in effecting 17 wiretaps against newsmen and White House staff.

Also: Testimony before this subcommittee at our last hearing indicated that Bell System personnel have in the past delivered on request very revealing telephone toll records to investigators without any legal process whatsoever.

Further: It has been established that the Bell System electronically monitored a room used for meetings of Communication Workers Union members. The subcommittee is releasing today documents supporting this particular allegation.

Last: There are serious questions raised regarding pointed discrepancies between past testimony before Congress of Bell System officials and a number of these revealed practices.

Hopefully many of these serious questions of veracity can be answered for the record in today's proceeding. Today's testimony, as I indicated the last time, will be taken under oath in order to establish the seriousness and credibility of these hearings. I would like to now call the three witnesses forward.

I understand Mr. Caming has a short statement but I would like to call Mr. Connor and Mr. Mack to come forward to join Mr. Caming, if you would, at the table, as the three witnesses this morning.

And, gentlemen, if you will stand and please raise your right hand.

Do you, Mr. Caming, Mr. Connor, and Mr. Mack, and each of you solemnly swear that the testimony you are about to give this subcommittee will be the whole truth and nothing but the truth, so help you God?

Mr. CAMING. I do.

Mr. CONNOR. I do.

Mr. MACK. I do.

Mr. KASTENMEIER. You may be seated, and Mr. Caming, you may proceed, sir, with your statement.

TESTIMONY OF H. W. WILLIAM CAMING, ATTORNEY, GENERAL DEPARTMENTS, AMERICAN TELEPHONE & TELEGRAPH CO.; ACCOMPANIED BY JOHN E. MACK, DIRECTOR, SWITCHING ADMINISTRATION AND MAINTENANCE SYSTEMS CENTER, BELL TELEPHONE LABORATORIES, NEW JERSEY; AND EARL CONNOR, STAFF SUPERVISOR, SECURITY, OF CHESAPEAKE & POTOMAC TELEPHONE CO. OF WASHINGTON, D.C.

Mr. CAMING. Thank you.

With your indulgence, I will keep Mr. Mack for the moment back here because I have a briefcase there.

I might say before initiating my statement, Mr. Kastenmeier, that should any members of the subcommittee have any difficulty hearing me in the absence of microphones, I would greatly appreciate being apprised of that.

Mr. KASTENMEIER. Yes. It is unfortunate that the judiciary committee is itself short handed electronically, paradoxical as that may be.

Mr. CAMING. I would also like to make one more comment that with respect to the questions which the chairman addressed himself to, I will be very pleased to discuss each of those in depth subsequent to my statement.

As the chairman knows, the statement is just an opening frame of reference for the inquiry of the subcommittee and to assist it.

Mr. KASTENMEIER. Mr. Caming, that will of course, be acceptable. I would hope we can develop it through a colloquy, through questions and through answers, and I should point out that we appreciate your being here, and Mr. Connor and Mr. Mack and other officials on very short notice. You would have preferred, I believe, a longer period of time in which to prepare your testimony, but you graciously agreed to come today and the committee does appreciate that.

Mr. CAMING. Thank you very kindly. I might say that we did prepare a statement that we feel will be complete, irrespective of the short time which we had at our disposal.

I am William Caming, attorney in the general departments of American Telephone & Telegraph Co. My areas of primary responsibility have since 1965 and to date included from a legal standpoint, oversight of matters pertaining to industrial security and privacy as they affect the Bell System. I might just say it is a pleasure to have with us today Mr. John E. Mack, who is the director of switching administration and maintenance systems center at Bell Telephone Laboratories, and with expertise in the fields particularly of electronic toll fraud; and Mr. Earl Connor, the staff supervisor in charge of security for the Chesapeake & Potomac Telephone Co., Washington.

It is a pleasure to appear before your subcommittee once again. I wish to thank you for the opportunity to reaffirm the Bell System's dedication and commitment to privacy of communications; to delineate again briefly our experiences with electronic surveillance, primarily in the area of wiretapping; and to discuss those measures we employ to combat the theft of telephone service by those clandestinely using electronic toll fraud devices.

You may recall that during my prior appearance before this subcommittee on April 26, 1974, I reviewed in depth the manner in which we safeguard privacy, and those statements are of equal efficacy and validity today. I adverted to our longstanding public espousal of legislation that would make wiretapping as such illegal. We have consistently said we strongly oppose any invasion of privacy of communications by illegal wiretapping and accordingly welcome Federal and State legislation designed to strengthen such privacy. This is still, of course, our position.

I described, too, how all Bell System companies conduct a vigorous program to ensure every reasonable precaution is taken to preserve privacy of communications through physical protection of plant and records and thorough instruction of employees.

I also mentioned how yellow pages directory advertising relating to wiretapping, eavesdropping, and debugging has long been banned.

I explained, too, our concern for privacy and how it is reflected in the manner in which we thoroughly investigate every incident of alleged wiretapping, whether found by our employees in the course of their work or through a customer's request for a wiretap check.

I have also reviewed the limited assistance we provide to law enforcement authorities engaged in the execution of court-ordered wiretaps, and to the Federal Bureau of Investigation in national security cases involving hostile acts of a foreign power and the like, upon

letter request personally signed by the Director of the Federal Bureau of Investigation, or the Attorney General of the United States.

Because of its continued timeliness, with the subcommittee's permission I would like to incorporate my statement of April 26, 1974, into my statement of today and for the convenience of the subcommittee, a copy of this statement is attached.

Turning now to another area of the subcommittee's initial inquiries, the Bell System has traditionally and consistently and unequivocally been concerned with the preservation of its customers' privacy. We firmly believe that whenever a communication is lawfully placed, its existence and contents must be afforded the full protection of the law.

But when wrongdoers break into the telephone network and by use of an electronic device seize its circuits so that calls can be illegally initiated—and the key word is initiated—we are faced with the formidable problem of gathering evidence of such fraud for purposes of prosecution and billing.

The Communications Act of 1934 imposes upon us the statutory obligation and duty to prevent such thefts of service. In essence, the act imposes upon each telephone company the duty to require all users of its services to pay the lawful charges authorized by tariffs on file with the appropriate regulatory bodies. No carrier may discriminate under the law between its customers by granting preferential treatment to any. Knowingly to allow those committing electronic toll fraud to receive "free service" would constitute such discrimination, in our opinion.

Furthermore, each telephone company is enjoined, under pain of criminal penalty, from neglecting or failing to maintain correct and complete records and accounts of the movements of all traffic over its facilities. Each carrier is also obliged to bill the Federal excise tax on each long-distance call.

To put for a moment the matter of electronic toll fraud into historical perspective, in the early 1960's a most ominous threat burst upon the scene, the advent of the so-called black and blue boxes, the first generation of a number. It was immediately recognized that if such fraud could be committed with impunity, losses of staggering proportions would ensue. This threat continues at flood level today, despite our constant vigilance and a large number of successful prosecutions over the past decade.

These devices are relatively inexpensive to make, and their use has grown at an alarming rate. We estimate blue boxes can be mass-produced at a cost of $25 to $50 per unit, and black boxes at a cost of a dollar or less. Our experience has shown that, among others, these devices have a unique appeal to the criminal element, whether it be a member of organized crime or an unethical, unscrupulous businessman. Not only may payment of the lawful telephone charges be evaded, but often more importantly, any record of the communication made concealed.

Perhaps at this point some brief definitions would be helpful. A black box is operated by the called party, so that anyone calling that particular number is not charged for the call. Contrariwise, a blue box is operated by the calling party and, because of its small size and portability, can be hidden on the person and at any time used to place an illegal call from any telephone to anywhere in the world.

Thus, from the outset, these and similar electronic toll fraud devices have been matters of serious concern. Telephone service is our only product, and its wholesale theft results in losses ultimately borne by the honest telephone user.

Such crimes have never enjoyed the protection of the law, neither before nor after the passage of title III of the Federal Omnibus Crime Control and Safe Streets Act in June 1968. A substantial number of distinguished courts, including several U.S. Circuit Courts of Appeals, have unequivocally held that persons stealing telephone service by trespassing upon the telephone network place themselves outside the protection of section 605 of the Communications Act, and of title III. In these criminal cases, our entire process of gathering evidence has been subjected to close and thorough and repeated judicial scrutiny: This jurisdictional oversight has continued to date, with some 270 convictions and a number of pending cases indicating the extent to which the courts at Federal and State levels have reviewed telephone company procedures for gathering such evidence. With virtual unanimity, the courts have held that the methods used have been lawful, independent of cooperation with law enforcement authorities, and wholly in the public interest.

It should be stressed, too, that prosecution has been and continues to be the only effective deterrent. As to the specific methods employed by the telephone companies to gather evidence of electronic toll fraud, we have found that a minimum amount of recording of a limited number of calls is indispensable, if a prosecution is to succeed.

Since the goods being stolen are the communication itself, for example, by a blue box user, there is no alternative at this state of the art, and I must emphasize that, but to make a limited recording of each illegal call, at least of the fraudulent dialing, ringing, and opening salutations for the following purposes: To identify the calling party, who the criminal is, the user of the blue box, and others with whom he may be acting in concert. Identification of the telephone line from which the fraudulent calls are originating must be followed by the more difficult identification of the specific individual making the calls. This is of paramount importance if prosecution and proper billing are to occur.

Establish the location from which the calls are originating. Most blue boxes are portable devices, some as small as a package of cigarettes, which are used by holding the device against the telephone mouthpiece, without the necessity of a direct electrical connection, that is, connecting by wiring into the telephone system, the telephone line.

Third, it is necessary to record the multifrequency tones being dialed, key pulsed, by the blue box after the line is illegally seized. And lastly, to determine whether the fraudulent call or a series of calls all being made through one seizure, were completed by the called party answering.

Distance as well as time is a factor in determining the proper billing charge for a long distance call. It is, therefore, necessary to ascertain each specific location called after the wrongdoer seizes the circuit. Let us assume, for example, that a blue-box user places a call from Washington, D.C. to the directory assistance operator at Chicago, which is 312-555-1212. I mention, Mr. Kastenmeier, that this is a small device. It is—well, I think it is—if I can find the box, it is

about the size of a Marlboro cigarette pack, and they are even getting smaller. And to show the graphic comparison, I have taken the liberty of bringing one down, to show that we are talking about something that is virtually able to fit into it.

Now, going on, by then emitting a specific tone from his blue box device, which tone you can understandably recognize, we prefer not to mention in public, the user seizes the line, disconnecting the operator at Chicago, and he has the long distance circuit. He can then, by pressing a single button, and then dial a number such as my home number in Summit, N.J.—I don't know if you can hear that from here, but it is duplicative of the tones that the operators themselves have. He can dial from that point to any part of the country. He can also dial to London, Moscow, Sydney, and other parts of the world. And this is done regularly.

The ultimate destination of each blue-box call can, therefore, be determined only by recording the multifrequency tones key pulsed. Also, as I have previously explained, after seizing the circuit the blue-box user can make not only one but a series of calls, terminating one, say, to Sydney after 15 minutes, and then he can immediately send a call to Hawaii and follow that with a call to Durban, South Africa.

Should such fraudulent calls be key pulsed, the location of each party called and the determination of whether each such call was completed and answered can only be made through recording the telltale tones. Unless the tones are recorded at the very moment they are emitted, they are, of course, lost forever.

None of the foregoing information can be obtained by use of our regular plant testing equipment, such as a peg count register, which is a simple electromechanical counting device that will count blue-box tones, as they appear. Such equipment cannot identify the fraudulent caller, nor record the multifrequency tones key pulsed after the blue-box tone is emitted, nor determine whether one or a series of fraudulent calls were dialed in succession, nor whether each such call was completed, nor produce other necessary evidence. These essential evidentiary elements can only be adduced through recording.

Nor will inspection of the suspect location usually uncover the small, readily concealed devices. Moreover, seizure of the device would not in and of itself, establish that fraud by wire had been committed, nor by whom, nor the extent of the fraud. Nor can the automatic message accounting equipment that normally obtains the information essential for billing purposes produce the necessary evidence of electronic toll fraud.

Most importantly, the limited recording done is solely to gather evidence of calls illegally placed. This is not a wiretapping case, where the contents of the conversations themselves are sought as evidence of some crime other than the theft of telephone service itself.

Limited recording by the local telephone company is done from secure locations, admission to which is tightly controlled on a need-to-know basis. This is done to maximize the protection of customers' privacy by preventing intrusion by unauthorized personnel. These quarters are kept under lock and key when not in use.

To assure the privacy of lawful communications, the telephone companies first employ a series of investigatory measures other than voice

recording to carefully evaluate the accuracy of any preliminary indications of electronic toll fraud. Only when a reasonable suspicion of such fraud has been firmly established, the possibility of plant trouble ruled out, and all other investigative measures exhausted, do the telephone companies engage in limited recording.

Nor does the recording begin until the caller's blue box emits a tone to seize the line, the one you first heard. The recording is brief and usually includes the ensuing dialing of the multifrequency tones of the number being illicitly called after the line was seized, the ensuing ringing cycle of the call, and the opening salutations of the parties after the call is answered. Usually only 60 seconds or less of conversation is necessarily recorded. The equipment generally is adjusted to cut off automatically at the end of this recording cycle.

In conclusion, we have shown that at best, detection of electronic toll fraud is difficult. We can only conjecture at the full scale of the substantial revenue losses sustained by the telephone industry and its customers. As in many criminal areas where detection is difficult, the instances of electronic toll fraud unearthed by the telephone companies represent merely that portion of the iceberg visible to the eye. The actual losses currently being sustained may be 10 or 20 times as great as our provable losses.

In none of the cases prosecuted, State or Federal, has any judge ever subscribed to the thesis that the telephone companies do not have the statutory obligation to collect, through limited recording, the evidence necessary to identify those placing calls in an illegal manner. To hold otherwise would in effect herald to the racketeer, the corrupt businessman, and all others that they have carte blanche to operate with relative impunity.

The virtually unchecked use of electronic toll fraud devices which would ensue if the threat of detection and prosecution is removed would impose an overwhelming financial burden on the telephone industry and its honest customers, who would be required to underwrite the entire cost of these depredations, including the total loss of revenue and the substantial expense of the circuits, facilities, and equipment tied up by such illegal use. These losses would rapidly reach staggering proportions, soaring into the tens and hundreds of millions of dollars and jeopardizing our very ability to provide telephone service to this Nation.

I shall be most pleased to answer any of the subcommittee's questions.

[The prepared statement of Mr. Caming follows:]

STATEMENT OF H. W. WILLIAM CAMING, ATTORNEY, AMERICAN TELEPHONE & TELEGRAPH CO.

I am H. W. William Caming, Attorney in the General Departments of American Telephone and Telegraph Company. 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, and 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 ensure 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 18,000,000 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 ensure 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 ensure 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 of 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 circuitry might be exposed to a wiretap. If no evidence of a wiretap is found, the customer is so informed. Where evidence of a wiretap is found, the practice generally 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 manifestations. 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 twenty-four 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, above-ground 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. KASTENMEIER. Thank you, Mr. Caming.

In connection with the practices of the phone company in connection with fraudulent toll calls, blue box calls, on February 2 the St. Louis Post-Dispatch reported that between 1965 and 1970, over 30 million telephone calls in six cities were randomly recorded, and over 1.5 million of these were retained for analysis, or perhaps that is a point you substantively made.

Was this basically an accurate statement of telephone company practices during this period?

Mr. CAMING. Yes, but I would like to clarify it for the subcommittee if I may.

First, I would like to say that the number of calls recorded for analysis were on the order of 1.5 to 1.8 million and not 30-plus million. The 30-plus million, as I will indicate, were merely scan tested without any human ear being possibly able to hear it, and erased automatically by equipment. This is purely a scanning process.

Now, why was this introduced? Was it necessary, and did it in any sense imperil our commitment to privacy of communications, or was it in furtherance of the public interest, I think, are fair questions. I

would like to address myself to them, with the permission of the Chair.

Mr. KASTENMEIER. You may proceed, sir.

Mr. CAMING. First, I think as I mentioned in my statement, we have to look at this in historical perspective so that you can appreciate the problems that the telephone industry as a whole, including the Bell System, of course, faced.

First, the advent of the black and blue boxes in the early sixties, and I think the first one was found in the State of Washington at the latter part of 1961, created a problem that we had never faced before, one that jeopardized the very integrity of our billing system and our ability to serve this Nation, and it was the fact that it could, by seizing the line in various ways, circumvent the billing equipment so that the calls would not be chargeable, seize and control indefinitely lines and clog our facilities accordingly.

At that time we recognized—and we can say this more confidently in public in retrospect—that we had no immediate defense. This was a breakthrough almost equivalent to the advent of gunpowder, where the hordes of Genghis Khan faced problems of a new sort, or the advent of the cannon.

To us the problem required an immediate course of action if the public interest was to be protected, because it was feared that if these devices, which I had shown, and I might just, so Mr. Drinan could be aboard with the others, sir, with the indulgence of the Chair, since I may allude to it again, just show you.

This is a Marlboro cigarette pack which I had mentioned earlier, and this is one of the devices, and they are even smaller than this. It has on the back—and I did not mention to the committee earlier, an ability to transmit by placing it against the mouthpiece so that you can carry this in your—in the pocket. It is completely concealable, and there are smaller ones. Then you take it out anywhere, any phone in the world. You can be in Hong Kong, London, it will work just as well, or in the United States, and usually, of course, our references are wholly to the United States. The others were an unlearned statement which my learned colleague, Mr. Mack, may correct.

Can you use these outside the United States?

Mr. MACK. No, technically you cannot. But the technique can be worked outside of the United States, but you need different sequences and frequencies.

Mr. CAMING. But it is similar in principle?

Mr. MACK. In principle, yes.

Mr. CAMING. Thank you.

The point is you can just press this and that is all it needs to seize the line because that specific tone is the tone on our equipment which indicates to it the line is under the dominion of the operator, say, at the toll center, and she is going to send a long-distance call through by key pulsing, and then all you do is pulse these through and it proceeds.

Mr. KASTENMEIER. Mr. Caming, I would like to go into the question of losses.

Mr. CAMING. Surely.

Mr. KASTENMEIER. I say this because at least one person has asserted, that in the Southwestern Bell Telephone Co. case, the cost of security personnel exceeded any losses attributable to the blue box or

anything else in the region. And so the question is, what provable losses do you have.

I notice you have 270 cases, apparently, you have won, or that have been pursued, prosecuted, according to your testimony. What in fact is the loss over all of these years due to these mechanisms?

Mr. CAMING. Sure, I will go into that, and then we will revert back to what we started on before I diverted myself, to produce the box for Mr. Drinan.

We estimate our provable annual losses, Bell System wide—and it is difficult to segment them by a particular location—in the order of $1 million. But let me emphasize to you very graphically how understated that figure is. First, we, because of our concern for privacy of communications, only record a limited number of calls. For example, there was a gentleman who bore the sobriquet of Captain Crunch, who for years had been making a great many calls from all over. He was finally tracked down through various methods and necessary evidence gathered. Now we only gathered a few calls in his case, and in those instances, the calls were perhaps six in number for which he was indicted, yet we know definitely, and I think this is the norm, that probably thousands of calls were placed.

To give you another order of magnitude, we understand the market price today because we have been offered these devices in the underworld, is close to between $2,500 and $3,500 for a device you can make for $25 to $50, and if you mass-produced it you could probably make it for less.

This indicates the importance attached to it and the use placed of it. We have found businessmen have been constantly using this to have their salesmen call in or considering using it for that purpose, yet when we prosecute, in order to minimize any intrusion on privacy of communications, we only take a few calls. And that is why I say that even despite the constant threat—and we do prosecute every case that we can, because we have found unless we do that there is no deterrent of effective measures—despite that, it is still at a flood level.

But our annual losses, to respond again, are in the order of, we estimate, $1 million, and it would be 10 or 20 times that at the least.

Mr. KASTENMEIER. You say you prosecute every case you can. To date it is your testimony you have some 270 convictions, is that correct?

Mr. CAMING. Yes.

Now, it must be borne in mind, just to clarify that, that the policy of prosecution was not initiated for a period of time. We tried through the preliminary equipment, scanning equipment I was adverting to earlier, to gain a measure of the magnitude of the fraud, and so we have not really—we did not initiate during the 1960's any but several landmark cases such as the *Hanna* case, the *Nolan* case, the *Beckley* case, *D'Amato*, and the like, and it was in the early 1970's.

Now, detection second, is a very difficult process because of the portability, because it may be used from a number of sources, although we have a large number of methods that we employ and we are getting increasingly effective. It is still a problem, and as I say, 270. There have been over 1,000 boxes picked up. That might be another statistic.

And then there are other devices. There is the cheese box, which is often used with a black box to interconnect two telephones. There is the so-called purple box or the red box which reflects the action of a

blue box by having the tones rather than the buttons, so that you just can on a tape bring out the tone.

Mr. KASTENMEIER. Mr. Caming, let me return to the Post-Dispatch report. I would like to deal with the 30 million telephone calls. These were randomly recorded by electronic device, and of those, apparently you had selected out 1.5 million of the 30 million which were randomly recorded or screened in some sense, is that correct?

Mr. CAMING. Yes. If I may, perhaps if I gave it to you in sequence now it would be helpful. The answer to that is "yes." As I said, we had the problem burst upon the scene, but we did use some of the finest minds that Bell Laboratories could muster on a task force to attempt to obtain a first generation detector, something that could scan and give us some idea of the magnitude of the problem because one of the questions was do we have to redesign the entire nationwide telephone network to put in a new signaling system, the costs of which would vary in estimates from a quarter of a billion to a billion dollars, and many, many years.

The second question was, in order to make an intelligent determination and to be able to justify it in the public interest, we had to have statistics, and therefore we devised six experimental units which were placed at representative cities. Two were placed in Los Angeles because of not only activity in that area, but also different signaling arrangements, and one was placed in Miami, two were originally placed in New York, one shortly thereafter moving to Newark, N.J., and one was placed in Detroit, and then about January 1967 moved to St. Louis.

Now, these were put in place not until about the end of 1964, and that was still extremely speedy. It was not a novel breakthrough. We used a great deal of standard equipment.

Now, the purposes were first to gather statistics of toll fraud, and it was decided that the prosecution should not be undertaken except in a few salient cases because it could alert the users and distort the statistics that were the basis of the decision whether or not to modify the network at a cost that would have to be borne ultimately by the ratepayers, and with no assurance at all that if we did modify it, that that in turn would not be overcome, too, by a different signaling system.

Second, we felt that we could obtain some ideas of the number who were committing it in these particular representative systems, only outgoing direct distance dialed calls going through the switching machines were scanned. Now, the way they were scanned is very simple to understand because—I have a fair grasp of it. There were in each of these locations a hundred trunks selected out of a large number, and the equipment which was logic equipment, would select a call. There were five temporary scanners which would pick up a call and look at it with this logic equipment and determine whether or not it had the proper direct current supervisory signals, whether, for example, there was return answer supervision.

When we have a call, we have a supervisory signal that goes to and activates the billing equipment which usually we call return answer supervision. That starts the billing process and legitimatizes the call, and if you find voice conversation without any return answer signal, and that is what it was looking for, it is an indication, a strong indication of a possible black box that the caller called in; and if, for example, you heard the tell-tone, blue box tone—and remember, this is a first generation development—this was a very strong indication of illegality because that tone has no normal presence upon our network at that point.

Now, all this equipment did was look at these calls. This equipment at these locations was not within the dominion, control, or ability to penetrate, of the local company. It was in locked cabinets. It was all automatically done. I know at least in one or two locations that I visited at the time, it was actually behind fences within the plant central office. So you would have to really penetrate that, too.

And the equipment then would determine whether there was a preliminary indication of illegality, either the lack of voice or the like.

Then we had another problem, particularly on black box calls, which were most prevalent at first, and were very easily concealable at the called end—and as I say, these can be made for less than a dollar apiece without really any great mass-production development. We would then be able to discern the extent of the problem in this regard.

Now, what happened when there was a preliminary indication, and remember, we had to make a decision, how long do we observe, in order to determine preliminary indications, and we tried to do the minimum possible. For example, with a black box call it was, I think, 90 seconds and then reduced to 60 seconds by the end of 1966, early 1967. In a blue box call it was first complete because of other reasons I will advert to, and then reduced to 5 minutes.

Now, these calls—and I must indicate to you, were calls the signals of which indicated abnormalities that would only be present normally if there was a plant irregularity or a preliminary indication of illegality. We were not looking at the contents of the calls to try to establish anything else at that stage.

These calls were then selected by the equipment randomly, the scanning was random, but it was specific selection on designated logic principles of the particular call, and only then would they be transferred over to a four-track recorder.

Now, this recorder was called a master recorder. It had a four-hour capacity. All it did on the first track was dub in the 90 seconds or so of recording of the call. That was taken and scanned and then later it would be fitted together in the analysis bureau. A second track would take the rest of the call if there was any, on a live basis, both the voice and also the tones of the conversation, and any signals.

The third took care of the so-called supervisory signals, such as direct current, the billing signals, and the like, and the fourth was a time announcement machine that gave you the time in which the call took place.

Now, what was done with this information? Whenever the reel was completed at these five locations, remembering there are six units, no more than five locations at any one time, and that is all, it was then accessed after an audible signal, and the reel removed by one of two local plant supervisors, who were very carefully selected, and they were the only two that had access from the local company, merely for the purpose of putting it in a container and sending it by registered mail to an analysis bureau we established in New York City under the supervi-

sion of A.T. & T. to insure that the maximum privacy would be given to this, so that no one in the local companies even had access to these random calls which were outgoing DDD calls.

At the bureau there was first a very small group working on it. They were in a single room closely supervised, working together, using equipment such as some of our traffic service position and other computer equipment, to analyze these calls. There was a preliminary analysis made first before there was even a further analysis, to weed out any except those that gave very strong indications [that] of illegality; if there was any doubt about illegality, the calls were immediately destroyed. Our tests were so vigorous that we winnowed out almost the great bulk of it.

Remember, no one has seen these at all.

Mr. KASTENMEIER. You had 1.5 million of these transferred to New York?

Mr. CAMING. Exactly, 1.5 to 1.8 million, somewhere in that order. I am not sure of the exact figures now, but in that order.

They were then the ones that were examined. They came from these five locations, only. They had not been seen or not been heard by any human ear until they reached the analysis bureau.

Now, at the analysis bureau they were subject to rigorous tests to attempt to determine whether they were illegal in fact.

Mr. KASTENMEIER. How many of these were illegal in fact?

Mr. CAMING. Well, let us put it this way. It is hard to determine under our regular standards whether or not there may have been more calls with indications of illegality, but we had at least 25,000 cases of known illegality, and we projected for example in 1966, which was the early stage when toll fraud was just getting underway, that we had on the order of 350,000 calls nationwide.

Mr. KASTENMEIER. The 25,000 calls you referred to, were they directly attributable to the analysis of the 1.5 to 1.8 million?

Mr. CAMING. Yes, they were, but these were only preliminary indications of illegality. Now, more than 60 percent of those were almost completely winnowed out at once because we had only recorded very limitedly on the black box, that is, voice without any return answer supervisory signal.

Now, there are many other types of telephone calls where there is no real privacy problem as far as overhearing the customer-to-customer conversation. That fell within that group, and let me name some of them because I think it is a very valuable insight to assure you that this type of equipment in no sense constituted a threat to privacy.

The calls were intercept calls, calls to intercept, calls to a vacant number where they would be routed, and calls where you had what we would call free line service. If you called a plant repair office to report your telephone needed some adjustment, or calls to a business office bureau to order an extension telephone.

I have a list of them, and just to be complete, I will just advert to that if I may. And then the other would be in the area of service irregularities or plant trouble. Now we estimate of that group, for example, only something like the minute fraction of 0.006 percent were really in the service irregularity group. Would that be generally correct?

Mr. MACK. Certainly less than a half percent.

Mr. CAMING. Certainly less than a half percent.

Mr. KASTENMEIER. Is this random monitoring program still in effect?

Mr. CAMING. No.

Mr. KASTENMEIER. When was it terminated?

Mr. CAMING. It was terminated, Mr. Kastenmeier, just as soon as we had the capability of developing the second generation, so to speak, in computer technique and knowledge. In May 1, 1970, we had closed down fully although we were tapering off before that, and the reason we did that is, we developed a second generation, which was on the boards from the very first, of an effort to develop that which is more sophisticated equipment. It did not require voice recording, and the moment we had something that would permit scanning of this nature, we terminated the other. It has given us broader coverage, and therefore, we did terminate as of May 1, 1970.

Mr. KASTENMEIER. Is it your view that the program, if conducted today, would be legal pursuant to law?

Mr. CAMING. I think there is no question that the program then and now—when I say then, from the beginning, prior to the passage of the Crime Control Act, clearly was not violative of section 605, and subsequent thereto in no way violated section 25(11)(2)(a) proviso which speaks about service observing or random monitoring.

Mr. KASTENMEIER. Right.

Mr. CAMING. That proviso states, as you are well aware, that service observing or random monitoring, using those terms synonymously, and I can point that out, is not to be used except for service quality control or mechanical check purposes.

Mr. KASTENMEIER. Title 18, United States Code, section 2511, subsection 2(a) reads in part as follows, "provided that said communication common carriers shall not utilize service observing or random monitoring, except for mechanical or service quality control checks."

I would submit to you that the practice that you followed between 1965 and 1970 is outside of that, and as a result is not legal.

Mr. CAMING. With due respect to the chairman's request for consideration, may I address myself to that?

Mr. KASTENMEIER. Well, yes, of course.

Mr. CAMING. I take it yours was a question.

Mr. KASTENMEIER. Yes.

Mr. CAMING. First, of course, as I pointed out to you, one of the basic purposes of this entire scanning program is its close confinement to a handful of people, its use only for information, and not—the contents were not used. It was purely to give us preliminary indications of the specific character of specific calls, which had appeared to be illegally placed.

We are not talking about lawful calls with unlawful content.

Mr. KASTENMEIER. With what you said, I agree. I understand the purpose.

Mr. CAMING. Fine.

Now, second, if I may address myself to the question of the Chair after that preparatory language. I personally am very familiar, coincidentally, with the proviso because I was involved in the legislative history preparation of it, and in following that, as you can well understand at that time, the legislative history's landmark decision appears

in Senate Report No. 1097 of the Committee of the Judiciary of the U.S. Senate, which was dated April 29, 1968, during the consideration in the later stages by the Senate of the bill that became the Crime Control Act.

Now, in looking at the proviso—and I might say that it is our interpretation, which I think I can establish to the satisfaction of the committee—and permit me to assure you that if there had been any doubt whatever, we would never have continued this practice at that time. I think that goes without question.

I might also say that up until the passage of the Crime Control Act, a large number of circuit court cases and the U.S. Supreme Court having affirmed in the *Sugden* case and denied cert in the *Hanna* case, had upheld our practices as lawful and not violative of section 605. This is prior to the passage of the Crime Control Act.

The courts have since then repeatedly scrutinized. Now, it is my position, based upon what I would like to say, that service observing and random monitoring are interchangeable synonymous terms. That service observing is random monitoring, as we use that term in the industry, and I refer to page 93 which also appears at 2 U.S. Congressional and Administrative News, 1968, at page 2182.

It states, "paragraph 2(a) provides that it shall not be unlawful for an operator of a switchboard or employee of the telephone company to intercept, disclose, or use wire communications in the normal course of their employment, while engaged in any activity which is a necessary incident to the rendition of service or the protection of the rights or property of the carrier." It is intended to reflect existing law. The *United States* v. *Beckley*, a case that I handled in the district courts of Georgia, as far as the telephone company's aspect, which clearly held that our course of conduct in recording was proper and that those who were illegally placing calls were not entitled to the protection of section 605 of the Communications Act.

Mr. DRINAN. Mr. Chairman, may I intervene here and go back?

Did you say that service observing and random monitoring are synonymous in the statute?

Mr. CAMING. I did, sir.

Mr. DRINAN. Then why were both terms included? And you indicated you had something to do with drawing up this particular statute in 1968? Is it just absolutely superfluous? Could we just say you cannot utilize service observing, and just eliminate random monitoring?

Mr. CAMING. Yes.

Mr. DRINAN. Well, you included it. You insisted, I imagine, that that language be there. Why did you want it to be redundant?

Mr. CAMING. The reason we did at the time—and in hindsight, it may not have been clarifying—it's hopeful it was clarifying—that frequently in service observing—and I'm talking about official service observing of a statistical, anonymous nature—is used the term "random monitoring". It is so frequently used, in our use of it—and it had been over the years by our officials in describing it.

For example, in 1966 Herbert Kertz in September 1966, appeared before the Congress, the Long committee, and again in 1967. In both cases the stress was on the random monitoring character of service observing.

Now, if I may go on, there are a few words that may help. The proviso came into being, by the way, as an afterthought. It was put in, I understand, at the request of several of the telephone unions to assure that service observing was not used for what we would call "supervisory observing" purposes, that is, on a position of an employee.

Sir, the Senate report did say that further provides section—I'm sorry paragraph 2(a), that is after saying existing law shall prevail on toll fraud—if I may read just a little further. Further provides about the service observing or random monitoring. "Service observing is the principal quality control procedure used by these carriers for maintaining and improving the quality of telephone service. Such observing is done by employees known as 'Service Observers' and this provision, the proviso, was inserted to insure that service observing will not be used for any purpose other than mechanical and service quality control."

I would also say, Mr. Drinan, in retrospect, despite what we thought was crystal-clear language—and that is we said is known as "service observers" and it is only to apply to that—it seems to have caused more confusion that clarification.

Mr. DRINAN. It demonstrates we should not allow telephone lobbyists to put in things as an afterthought.

Mr. CAMING. It was not a lobbyist, but merely a respectful consideration of the Congress, and it does demonstrate that too, but certainly it was our position in view of this—and let me, may I go one step further, as to this process, because there is another aspect of this problem in addition to the legislative history.

Mr. KASTENMEIER. Incidentally, Mr. Caming, let me only interrupt to say that I would like to move on from this point, but at best there is a great deal of ambiguity in section 2511(2)(a). Notwithstanding the Senate legislative history—and that is not clear in and of itself—one has to look at the context in which the entire section was written. At the very best there is ambiguity. I would say a precise reading of the cases you have cited indicates that they were not based on random recordings. For example, the *Beckley* case did not involve random recording. Frankly, I did assume that in 1970 you discontinued the practice because you did not think it conformed with the 1968 statute.

Mr. CAMING. That is categorically, sir——

Mr. KASTENMEIER. That was just an assumption.

Mr. CAMING. That is categorically not the case. We did it as soon as we had voice recording. If we had any doubt at all—I'm sorry, as soon as we had voice recording capability eliminated, if we had any doubt at all, we could have done it in June of 1968. We were not at that time prosecuting, and we were advanced in our second generation. There was no question. This never became a problem.

As I mentioned in this legislative history, which I adverted to, it states specifically that it refers solely to service observing, as done by service observers. And that is the term of art known in the industry. And there is another point there, if I may just very briefly touch on it.

This is not random monitoring. The recording, the scanning and testing initially done of the 30-odd million calls was random monitoring. It was done at random, picking calls, each of five units having 20 trunks under its dominion of outgoing DDD calls, but when there was

recording, it was done only in specific cases where there was a preliminary indication to the mechanical equipment that this was an illegally placed call, and recording was limited to that, and the courts have since, as well as before, upheld this as nonrandom monitoring, where it is on a specific indication of fraud.

And, for example, in Milwaukee recently the *United States* v. *DeLeuw* case, the Federal district court itself stated that the only recording was in those instances where a blue box frequency was applied thereto, and it was nonrandom monitoring sanctioned under section 25(11)(2)(a) because it was only in cases of specific indications of illegality, and the only calls that were recorded for analysis were those where there were those specific indications.

There were many other cases of a similar nature which took this position.

Third, and perhaps——

Mr. KASTENMEIER. I think I would be less likely to argue with you on this point except for your concession that the original 30 million calls were, in fact, cases of random monitoring. Even though you describe them as essentially electronic, they were not ordinarily accessible to phone company personnel.

I think, technically, this was random monitoring, and at least according to the face of the statute is forbidden. This art of random monitoring, I would say, may be a different character than service observing.

Mr. CAMING. May I address myself to that?

Mr. KASTENMEIER. Yes.

Mr. CAMING. I think I could say something that is very opposite. Section 2510(4) of the Crime Control Act provides that the term "intercept" is defined as the aural acquisition—A-u-r-a-l—acquisition of the contents by use of a device.

This requires, according to the interpretation, for example, by the Supreme Court recently in a Pen Register case, the human ear to listen, and that is exactly our point. I could not have said it better that you did say it, Mr. Kastenmeier, that the random monitoring was of the 30 million, and those calls, as I have stressed, were not listened to by the human ear.

Accordingly, they were not within the aural acquisition, and therefore are not within title III of the Crime Control Act. There is no question whatever about that. The U.S. Supreme Court has held that, that aural acquisition must be by the ear, and there are also a host of other cases.

Now, in addition, there is one other last point. This is a very—and I must respectfully state that I do not wish to seem to be throwing things around, but it is a very complicated statute, and I am not sure I, after many years of studying it, really understand all of the nuances, and the best point was one Mr. Drinan pointed out, that we did more to confuse than to clarify.

But section 2510(5) defines the term "device," and it must be borne in mind that as I mentioned 2510(4) defines intercept as aural acquisition and also not only by the ear but with the use of a device, and excluded from the term device is equipment used by the telephone company in the ordinary course of its business, and certainly any

plant-testing equipment we use for purposes of detecting fraud has over the years been uniformly accepted by the courts, and I think by the Congress, as being in the ordinary course of business, therefore it is excluded from the term device, so for those three reasons——

Mr. KASTENMEIER. Well, Mr. Caming, you have a case, or cases, which give judicial approval to this particular monitoring program from beginning to end. We would be very happy to receive them. I do not know if there may be such things. I am not aware of them.

Mr. CAMING. Certainly. There are a host of cases that have approved of the type of recording we do, and I think I have discussed a number of them with Mr. Lehman in the past, and I know the Congressional Library called me Friday, and I gave them some 15 cases or more, but for those reasons we were firmly of the opinion—and I think it is helpful to the committee to know what our opinion was—that this, for those three reasons: One, it was not aural acquisition; two, the proviso does not apply except to service observing; and three, it was use of equipment which is used by the telephone company in the ordinary course of its business and therefore excluded from the term device.

[The material referred to follows:]

AMERICAN TELEPHONE & TELEGRAPH CO.,
New York, N.Y., March 18, 1975.

BRUCE LEHMAN, Esq.,
Majority Counsel, Subcommittee on Courts, Civil Liberties and the Administration of Justice, Committee on the Judiciary, Rayburn House Office Building, Washington, D.C.

DEAR MR. LEHMAN: In accordance with Mr. Kastenmeier's suggestion, I am enclosing for your information a list of citations of representative judicial decisions upholding the lawfulness of the methods employed by Bell System Companies (including limited recording) in gathering evidence, for billing and prosecutory purposes, of the commission of electronic toll fraud, accomplished through the use of devices such as the so-called black and blue boxes. These cases span a period from the mid-Sixties to the present. They uniformly hold that the illegal "placing" of calls through the use of these devices was not protected, either under § 605 of the Communications Act of 1934 or under the Federal Omnibus Crime Control and Safe Streets Act of June 1968.

The Courts have stated that the Communications Act imposes upon common carriers the statutory obligation to prevent such thefts of service. In essence, all users of telephone service must be required to pay the lawful, tariff-prescribed charges. No carrier may discriminate between its customers by granting preferential treatment to any. Knowingly to allow those committing electronic toll fraud to receive "free service" would constitute such discrimination and be violative of the carrier's statutory duties. [See §§ 202, 203(c) of 47 U.S.C.] Further, each telephone company is enjoined, under pain of criminal penalty, from neglecting or failing to maintain correct and complete records and accounts of the movements of all traffic over its facilities. [§ 228 of 47 U.S.C.]

These cases are illustrative of the judicial holdings at federal and state level to the effect that such crimes have never enjoyed the protection of the law, neither before nor after the passage of Title III of the Federal Omnibus Crime Control Act. A substantial number of distinguished courts, including several United States Circuit Courts of Appeals, have uniformly held that persons stealing telephone service by trespassing upon the telephone network place themselves outside the protection of § 605 of the Communications Act and of Title III.

In these criminal cases, the telephone companies' methods of gathering evidence has been subjected to close and thorough judicial scrutiny and oversight. With virtually unanimity, the courts have held that the methods used have been lawful, independent of cooperation with law enforcement authorities in the evidence-gathering stage, and wholly in the public interest. Further, such evidence gathering was not violative of the Fourth Amendment or other constitutional strictures.

These cases are to be associated with and are supportive of the Statement that I presented in behalf of the Bell System to the Subcommittee on Courts, Civil Liberties, and the Administration of Justice of the House of Representatives Committee on the Judiciary on February 18, 1975.

Should you have any questions with respect to the foregoing, I shall be pleased to discuss them with you.

Sincerely,

H. W. WILLIAM CAMING,
Attorney.

Enclosure.

CITATIONS OF REPRESENTATIVE JUDICIAL DECISIONS UPHOLDING THE LEGALITY OF THE METHODS EMPLOYED BY ASSOCIATED OPERATING COMPANIES OF THE BELL SYSTEM TO GATHER EVIDENCE (INCLUDING LIMITED RECORDING), FOR PROSECUTORY AND BILLING PURPOSES, OF THE COMMISSION OF ELECTRONIC TOLL FRAUD THROUGH THE USE OF SO-CALLED BLUE AND BLACK BOXES OR OTHER ELECTRONIC DEVICES

United States v. Sugden, 226 F. 2d 281 (9th Cir. 1955), aff'd per curiam, 351 U.S. 916 (1956)
United States v. *Beckley*, 259 F. Supp. 567 (N.D. Ga. 1965)
United States v. *Hanna*, 260 F. Supp. 430 (S.D. Fla. 1966), aff'd upon reh., 404 F. 2d 405 (5th Cir. 1968), cert. denied 394 U.S. 1015 (1969)
Brandon v. *United States*, 382 F. 2d 607 (10th Cir. 1967)
United States v. *Kane*, 450 F. 2d 77 (5th Cir. 1971), cert. denied, 405 U.S. 934 (1972)
Nolan v. *United States*, 423 F. 2d 1031 (10th Cir. 1970), cert. denied, 400 U.S. 848 (1970)
Bubis v. *United States*, 384 F. 2d 643 (9th Cir. 1967)
United States v. *McDaniel*, unreported Memorandum Decision (9th Cir. 1974), copy of which is attached, distinguishing *Bubis* supra.
United States v. *Baxter*, 492 F. 2d 150, 166–67 (9th Cir. 1973)
Katz v. *United States*, 389 U.S. 347, 352 (1967)
Burdeau v. *McDowell*, 256 U.S. 465 (1921)
United States v. *Shah*, 371 F. Supp. 1170 (W.D. Pa. 1974)
United States v. *Freeman*, 373 F. Supp. 50 (S. D.Ind. 1974)
United States v. *DeLeeuw*, 368 F. Supp. 426 (E.D. Wisc. 1974)
United States v. *Jaworski*, 343 F. Supp. 406 (D. Minn. 1972)
People v. *Garber*, 275 Cal. App. 2d 119, 80 Cal. Rptr. 214 (Ct. App. 1st Dist. 1969), cert. denied, 402 U.S. 981 (1971)

THE LIBRARY OF CONGRESS,
CONGRESSIONAL RESEARCH SERVICE,
Washington, D.C., March 3, 1975.

To: House Judiciary Committee, Attention: Bruce Lehman.
From: American Law Division.
Subject: The Legality of Telephone Company Monitoring for Anti-Fraud Purposes Under 18 U.S.C. § 2511(2)(a)(i).

This memorandum is in response to your request and our subsequent telephone conversation wherein you requested a legal memorandum discussing the legality of telephone company monitoring for anti-fraud purposes as disclosed by a St. Louis Post-Dispatch article of February 2, 1975.

A. THE TELEPHONE COMPANY'S MONITORING

According to the newspaper article and testimony of Mr. H. W. William Caming, attorney for American Telephone and Telegraph Company, before the Subcommittee on Courts, Civil Liberties and the Administration of Justice on February 18, 1975, the telephone company monitored nearly thirty million long-distance phone calls during the six year period from 1964 to 1970. During this period of time the phone company monitored only outgoing, direct distance dialed calls in five cities. In each of these locations several trunk lines were selected out of a large number. Scanners would then pick up a call and look at it with logic equipment in order to determine if the call had the proper direct current supervisory signals.

This supervisory signal goes to and activates the company's billing equipment, and if there is a voice conversation without this signal there is a strong indication of a possible fraudulent long-distance call. The phone company attorney stated that these calls were selected by the equipment randomly. The scanning was done at random, "but it was specific selection on designated logic principles of the particular call." When there was a preliminary indication to the mechanical equipment that there was an illegally placed call, the call would be transferred to a tape-recorder.

As reported in the newspaper, the recorder would record a segment or the entire content of the call. Approximately 1.5 million of these calls were recorded and sent to a central location to be analyzed by listening to the conversation. However, fewer than 25,000 of these calls were considered to be indicative of fraud, and during the first four years of this activity about 500 calls were confirmed as fraudulent. Thus it seems that a large number of nonfraudulent calls were monitored and recorded over a long period of time by the phone company.

B. THE LAW

During the period that the phone company was conducting its monitoring operation, two federal statutes governed wiretapping and electronic surveillance. Section 605 of title 47 was passed by Congress in 1934 and read as follows prior to June, 1968:

"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 agent, 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 communication 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."

In June, 1968, Congress passed the Omnibus Crime Control and Safe Streets Act of 1968, 82 Stat. 197 (1968). Title III of that Act, 18 U.S.C. §§ 2510–2520, generally made it a federal crime to intercept or attempt to intercept any wire or oral communication or to disclose or attempt to disclose or use information obtained by an unlawful interception. Several exceptions to this prohibition were given in the statute including one that allows law enforcement officials to secure a court order approving interceptions. Another exception is found in 18 U.S.C. § 2511(2)(a) which states:

"It shall not be unlawful under this chapter for an operator or a switchboard, or an officer, employee, or agent of any communication common carrier, whose facilities are used in the transmission of a wire communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the carrier of such communication: *Provided*, That said communication common carriers shall not utilize service observing a random monitoring except for mechanical or service quality control checks."

Title III also amended Section 605 so that the prohibition of that section became subject to 18 U.S.C. §§ 2510–2520.

The statutory language in section 605 does not grant an exception for communication carriers or their employees. However, such an exception has been created by judicial interpretation. One of the most significant cases on this point is *United States* v. *Sugden*, 226 2d 281 (9th Cir. 1955), aff'd per curiam, 351 U.S. 916 (1956). In *Sugden*, the defendant was indicted for conspiracy to violate the immigration laws. Part of the evidence was obtained by a Federal Communications Commission employee, who intercepted radio communications broadcast over a licensed radio station by unlicensed operators. The defendant moved to suppress the evidence, and the trial court was of the opinion that the evidence was obtained in violation of Section 605 and granted the motion to suppress.

On appeal the United States Court of Appeals reversed. The appellate opinion starts by making an interesting distinction:

"The government must concede that if the facts were the same save that [the government agent] had tapped the Sugden's telephone line and obtained the same information without the Sugden's consent as he did by monitoring the air waves, then the trial court's rulings were correct. 226 F. 2d at 284."

The court went on to say that the purpose of Section 605 was to protect the means of communication, and the court held that this purpose would not support an application of that section to an unlicensed operator. It seemed implicit in the Act, the court said, that agents of the F.C.C. could make interceptions in order to enforce the Federal Communication Act.

"Therefore, we hold that as to private radio communications, . . . the voice must be legally on the air; otherwise one who hears, . . . may make full disclosure. Giving the one who broadcasts without authority any protection under Section 605 could not tend to protect the means of communications. 226 F. 2d at 285."

The *Sugden* case was affirmed per curiam by the United States Supreme Court with 3 Justices dissenting. However, the distinction made by the Ninth Circuit between the protection given to a licensed operator and the protection given to an unlicensed operator by Section 605 has been criticized. Note, 44 California L. Rev. 603, 606 (1956); Note, 42 Virginia L. Rev. 400, 401 (1956). Also, the *Sugden* court seemed to ignore the language in *Nardone* v. *United States*, 302 U.S. 379, 382 (1937), that

". . . the plain words of § 605 forbid anyone, unless authorized by the sender, to intercept a telephone message, and direct in equally clear language that 'no person' shall divulge or publish the message . . . to 'any person.'"

The Supreme Court in *Nardone* interpreted the phrase "no person" to include federal officers, and the Court went on to say that "Congress may have thought it less important that some offenders should go unwhipped of justice than that officers should resort to methods . . . destructive of personal liberty." 379 U.S. at 383. If Section 605 applies to federal law enforcement officers it would also seem to apply to communications carriers, although the *Nardome* court did not discuss this point. Since the Supreme Court did not issue an opinion when it affirmed *Sugden* the law is not clear.

Three federal courts of appeal have given the telephone company an exception to Section 605, however. *Nolan* v. *United States*, 423 F. 2d 1031 (7th Cir. 1969), cert, denied, 400 U.S. 848 (1970); *Hanna* v. *United States*, 404 F. 2d 405 (5th Cir. 1968), *cert. denied*, 394 U.S. 1015 (1969); *Brandon* v. *United States*, 382 F. 2d 607 (10th Cir. 1967); *Bubis* v. *United States*, 384 F. 2d 643 (9th Cir. 1967).

In *Bubis*, the telephone company was investigating a situation in which a device was being used to enable the caller to circumvent the company's record-keeping equipment so as to avoid long distance charges. As a result of information obtained by keeping a record of the member and duration of telephone calls made, the phone company connected automatic monitoring equipment to Bubis' telephone line. This equipment monitored all of his incoming and outgoing telephone calls over a three month period and tape-recorded the conversations of all such calls. The company notified the government that some of the recorded conversations revealed gambling information and the tapes were subpoenaed. Bubis was convicted and appealed on the grounds that the district court erred in denying his motion to suppress the evidence obtained through the recordings.

The Ninth Circuit Court of Appeals said that:

"To apply the literal language [of § 605] to the foregoing circumstances, would, in our view, reach an absurd result, contrary to common sense and reasonable business practices. . . . It would mean that communications systems are powerless to take reasonable measures to protect themselves and their properties

against the improper and illegal use of their facilities. We do not believe that in the enacement of Section 605, or in any of the provisions of Title 47, Congress intended to deprive communications systems of their fundamental right to take reasonable measures to protect themselves and their properties against the illegal acts of a trespasser.

"When a subscriber of a telephone system uses the system's facilities in a manner which reasonably justifies the telephone company's belief that he is violating his subscription rights, then he must be deemed to have consented to the company's monitoring of his calls to an extent reasonably necessary for the company's investigation. 384 F. 2d at 647."

A similar interpretation of Section 605 is found in *Brandon* v. *United States*, supra, and *United States* v. *Beckley*, 259 F. Supp. 567 (N.D. Ga. 1965). The *Bubis* court went on to hold that the monitoring and tape-recording in the instant case had continued for such a length of time, after ample evidence of illegal use had been secured, that it was unreasonable and unnecessary. "To sanction such practices on the part of the telephone company would tend to emasculate the protection of privacy Section 605 was intended to protect." 384 F. 2d at 648.

The *Hanna* decision is a curious one. Hanna was charged with violation of the federal wire fraud statute and the interstate gambling laws. Most of the evidence consisted of tape recordings which resulted from the monitoring of Hanna's telephone lines by the telephone company. The company had detected an unusual condition on a certain telephone line in Miami, and this condition was such as to indicate that a device was used to circumvent the company's toll equipment. The suspected telephone number was subscribed to by Hanna. A phone company engineer confirmed the use of a "blue box" on Hanna's line, and a company employee attached a tape recorder to the line in order to record the electronic signals emanating from the "blue box." The recorder operated only during the first 35–45 seconds of all telephone calls placed with the "blue box" during a 3 week period.

The defendant asked the trial court to suppress the evidence. This court refused, reading into Section 605 "an implied right to monitor under certain conditions." 260 F. Supp. 430, 433 (S.D. Fla. 1966). On appeal, the United States Court of Appeals for the Fifth Circuit reversed the lower court in its first opinion published at 393 F. 2d 700. The majority relied primarily on *Nardone*, supra, and *Bubis*, supra, for the proposition that Section 605 did not imply a right to monitor by the phone company. The court also rejected the suggestion that, by his illegal use of the telephone company facilities, Hanna impliedly authorized the interception of any communication.

After rehearing the case, the Fifth Circuit issud its second opinion reported at 404 F. 2d 405. This later opinion affirmed the lower court and was necessary, the court explained, because the original opinion was in error as to the facts and the law. In its second opinion, the court found that recording limited parts of telephone conversations was necessary for the telephone company to comply with the duties imposed by 47 U.S.C. § 220 and 26 U.S.C. § 4251. The Fifth Circuit also felt bound by the *Sugden* case.

"It must, therefore, be conceded that when the use of the communication facility itself is illegal, section 605 has no application, at least insofar as concerns the person guilty of such illegal users [sic, uses]. Whatever we might otherwise think, this Court is bound by the *Sugden* decision. 404 F. 2d at 408" (emphasis added).

However, the court failed to distinguish *Nardone*, the case relied on by the court in the first *Hanna* opinion.

The *Hanna* decision was appealed to the United States Supreme Court, but certiorari was denied. 394 U.S. 1015 (1969). Justices Fortas and Douglas dissented. They would have granted certiorari to resolve the area of conflict between *Bubis* and *Hanna*. By this time Congress had passed Section 2511(2)(a) of Title 18, and Justice Fortas wrote that it ". . . is by no means clear that the new statute would authorize this kind of conduct if a similar case occurred today."

In *Nolan*, supra, the defendant attempted to suppress tape recordings obtained by the telephone company as part of an investigation of illegal use of its long distance lines. The Tenth Circuit held that the evidence was obtained legally under Section 605. As to the senders of illegal calls, the *Nolan* court said that Section 605 ". . . was not intended as a refuge for the wrongdoer who uses the telephone in a scheme to violate the wire fraud statute." 423 F. 2d at 1031 (citing *Brandon* and *Sugden*). With regard to the recipients of illegal calls, the court relied on

Hanna for the argument that the telephone company has the right to monitor its lines in order to fulfill its statutory duty to detect toll fraud. The court also pointed out an alternative theory that there was an implied exception to the second clause of Section 605. Of course, the fact that the Supreme Court denied the petition of certiorari in *Nolan* does not mean that the Court approved this decision.

It should be noted that in *Hanna, Brandon, Beckley,* and *Nolan* the defendants were using the telephone illegally, and the telephone company made tape recordings only of the illegal calls. None of these courts had to consider whether the taping of an innocent phone call would be legal under Section 605, although the *Bubis* opinion seems to say that it would not. In each of these cases the phone company had evidence that a specific phone line was the source of fraudulent calls prior to any tape-recordings. Also, none of these cases had to discuss the legality of random monitoring by the phone company. Thus it does not seem clear that under Section 605 the phone company had the legal right to randomly monitor all outgoing calls, tape-record all those calls that appeared to be fraudulent, including the entire conversation, and then listen to the conversations to determine if they were indeed fraudulent.

In 1968 Congress passed Section 2511(2)(a). This section declared that it would not be unlawful for a communication common carrier employee to intercept a communication in the normal course of his employment while engaged in an activity necessary for the protection of the rights or property of the carrier. However, the statute also provides that the carriers shall not utilize "service observing or random monitoring" except for mechanical or service control checks. The legislative history of this section does little to explain what is meant by random monitoring. There is no House Report and the Senate Report says:

"Paragraph (2)(a) provides that it shall not be unlawful for any operator of a switchboard or employees of a common carrier to intercept, disclose, or use wire communications in the normal course of their employment while engaged in any activity which is a necessary incident to the rendition of his service or the protection of the rights or property of the carrier. It is intended to reflect existing law (*United States* v. *Beckley*, 259 F. Supp. 567 (D.C. Ga. 1965)). Paragraph (2)(a) further provides that communication common carriers shall not utilize service observing or random monitoring except for mechanical or service quality control checks. Service observing is the principal quality control procedure used by these carriers for maintaining and improving the quality of telephone service. Such observing is done by employees known as service observers, and this provision was inserted to insure that service observing will not be used for any purpose other than mechanical and service quality control. S. Rept. No. 1097 at 93, 90th Cong. 2d Sess. (1968)."

Beckley was not a "blue box" or "black box" case. It involved a conspiracy to defraud the telephone company by an employee of the company and others. The court simply said, without citing any authority, that, "Section 605 does not prohibit the telephone company from monitoring its own lines." 259 F. Supp. at 571.

One author has interpreted Section 2511(2)(a) to mean that the monitoring must be random and it must be done to determine mechanical or service quality in the case of a communication common carrier. "No monitoring for criminal misuse as such would be acceptable under this provision." J. George, Constitutional Limitations on Evidence in Criminal Cases 158 (1973 ed.).

After diligent research no reported federal appellate court cases that interpret Section 2511(2)(a) could be found. Three federal district court cases involving this section have been reported. In *United States* v. *Deleeuw*, 368 F. Supp. 426 (E.D. Wisc. 1974), the telephone company connected a dialed number recorder to the defendant's telephone line. In addition, the company recorded a one minute conversation of the defendant whenever the mechanism was activated by a "blue box" frequency. The defendant was indicted for fraud, and on his motion to suppress the evidence the court held that ". . . the action taken by the . . . company in attaching a . . . detector to the defandant subscriber's line, which device recorded . . . the conversations had on such line in only those instances where a blue box' frequency was actually applied thereto, constituted the type of nonrandom monitoring for the protection of property which is sanctioned by 18 U.S.C. § 2511(a)(i)." 368 F. Supp. at 428.

On the basis of an analysis of a computer printout it was suspected the defendant Shah may have been using a "blue box." The phone company monitored Shah's line and recorded the beginning portion of any conversation when the "blue box" was used. Shah was charged with violating the wire fraud statute, and

on his motion to dismiss the court held that the phone company had done nothing that was not within the exception of 2511(2)(a). *United States* v. *Shah*, 371 F. Supp. 1170 (W.D. Pa. 1974).

In *United States* v. *Freeman*, 373 F. Supp. 50 (S.D. Ind. 1974), the phone company, after receiving information from another phone company, installed a tape-recorder on defendant's ex-wife's telephone line. The monitor recorded the use of a "blue box" on several occasions. The defendant made a motion to dismiss, but the court denied the motion. The trial judge said that the action taken by the phone company was "the type of non-random and non-service control monitoring for the protection of the utility's property which is contemplated by 18 U.S.C. § 2511(2)(a)(i), ..." 373 F. Supp. at 52.

Obviously, none of these cases have sanctioned the widespread use of random monitoring by the phone company. Like the cases decided under Section 605, each of these recent cases involved the monitoring of a specific telephone line. The question as to whether the random monitoring as reported in the newspaper was in violation of Section 2511 remains unanswered.

Section 2511(2)(a)(i) specifically states that the telephone company "shall not utilize . . . random monitoring except for mechanical or service quality control checks." It would seem that the random monitoring conducted by the company after the Omnibus Crime Control and Safe Streets Act took effect was within the proviso of Section 2511(2)(a)(i). The term random monitoring is not defined by the Act. Although the phone company has argued that "random monitoring" has a technical meaning, it is a general rule that a statute must be interpreted by its plain and common meaning. See, *Rathburn* v. *United States*, 355 U.S. 107, 109 (1957). As the Supreme Court has said, in speaking of Section 605, "distinctions designed to defeat the plain meaning of the statute will not be countenanced." *Benanti* v. *United States*, 355, U.S. 96, 100 (1957).

Even if the random monitoring is within the proviso of Section 2511(2)(a)(i) it would appear that no violation of that section has occurred. Section 2511 prohibits the willful interception of any wire or oral communication or the use of any device to intercept any oral communication. Section 2510(4) of Title 18 defines intercept to mean "the aural acquisition of the contents of any wire or oral communication through the use of any . . . device." The term device is defined so as to exclude any apparatus being used by a communications carrier in the ordinary course of its business. 18 U.S.C. § 2510(5). Only equipment being used by the carrier in the ordinary course of its business would be excluded. S. Rept. No. 1097, supra, at 90.

Arguably the random monitoring by the electronic scanner was not the aural acquisition of the contents of the communication and therefore not an interception of the conversation. The words "aural acquisition" as used in 18 U.S.C. § 2510(4) mean to come into possession through the sense of hearing. *Smith* v. *Wunker*, 356 F. Supp. 44 (S.D. Ohio 1972). The mechanical monitoring of telephone conversations to detect the use of a "blue box" a "black box" would not be an "aural acquisition" of the conversation.

The tape recording of the conversations would be an interception, but such an interception would seem to be legal by the exception given the phone company in Section 2511(2)(a)(i). However, if the company recorded the entire conversation or if the company recorded more calls than were necessary to prove illegality, then the company may have exceeded the authority given to it by Section 2511. See, *Bubis* v. *United States*, supra. If the scanning and the recording is viewed as a one-stage process, then what the phone company did was the aural acquisition of the contents of a communication. This one-stage process would only be illegal if the device was not being used in the ordinary course of the company's business.

One other possible argument that the phone company's monitoring was illegal is that it violated the Fourth Amendment rights of the company's subscribers. Generally there is no invasion of the security afforded by the Fourth Amendment against unreasonable search and seizure when evidence is acquired illegally by private parties. *Burdeau* v. *McDowell*, 256 U.S. 465 (1921). The argument has been made, however, that when the searcher has a strong interest in obtaining convictions and has committed searches and seizures regularly then the Fourth Amendment should apply even though the search was not done by a government official. Note, 19 Stanford L. Rev. 608, 615 (1967). Thus, there is the basis for any argument, albeit a weak one, that the phone company violated the Fourth Amendment by recording telephone conversations in order to prosecute illegal users.

C. CONCLUSION

It is not certain that the telephone company violated any federal laws by the random monitoring of telephone conversations during the period from 1964 to 1970. This uncertainty exists because the Congressional intent in passing Section 2511(2)(a)(i) is not clear, and case law has not clearly explained the permissible scope of monitoring by the company. Under the existing law it seems that the only way that the telephone company can violate Section 2511 is if it randomly monitors telephone conversation with a device not used in the ordinary course of its business so as to aurally acquire the conversation. One obvious remedy would be for Congress to amend Section 2511 so as to make clear the extent of the monitoring to be allowed.

IRWIN MANDELKERN, *Legislative Attorney.*

Mr. CAMING. The reason we terminated the program was because the second generation, which we were attempting to develop as fast as we could, did come along and permit us to get as broad or broader coverage without the necessity of having any voice recording whatsoever, and the whole program and the concept of being closely guarded, seen by only a few very trusted employees under constant supervision, and promptly erased thereafter, was designed for this purpose.

That's a long way around Mr. Kastenmeier.

Mr. KASTENMEIER. Leaving that particular question, Mr. Caming, are you aware of company practices that have involved surveillance of individual employees or union activities or conversations conducted on company property, other than on business phones, in the recent past?

Mr. CAMING. There have been a number of situations where there have been allegations over the years. Each one of those is carefully and fully investigated. How, if we are talking in terms of the normal supervisory observing, whether it is visual, whether it is from a desk across the room, or at an adjacent location, there is a possibility that this may have occurred, but that would certainly in no wise be designed to overhear union conversation.

For example, let us take a plant repair test room, or let us say a business office, which is very simple. A business office service representative may also be a union vice president, let us say. She is at the front desk, and she may receive a call on one of several telephones, which she handles for telephone contacts with the public, and usually they handle large volumes.

One of that large volume of business calls may be a call on union business. If so, it is possible that it would be subject to observation.

However, it is to be borne in mind that those particular telephones are to be used only for official business, and—and I think this is most important—there are other phones immediately available, such as in the employees' lounge next door, where any and all calls can be taken in complete privacy.

Now, that is a possibility. I can only conjecture when that might occur. Any specific allegation would be carefully investigated. Normally, if such a call was overheard, the supervision would drop off the call, the purposes of the observation being purely for determining the quality of service rendered by the individual, and also by the—I'm sorry—and also whether the individual employee might require further training and assistance.

I might say that I appeared before the Government Operations Subcommittee of this respected House and discussed this subject at considerable length on June 11, 1974, with respect to——

Mr. KASTENMEIER. Did you discuss with them the complaint of Local 2108 of the Communications Workers of America in a local case out here?

Mr. CAMING. I do not know, without knowing the date. It does not ring a bell, but Mr. Glen Watts, president of CWA, was next to me at a very pleasant hearing which we had, and we did discuss this subject matter, and whether it is one case or another, I think the same would apply.

There was an allegation, which we have been unable to run down, that somewhere in the distant past, about 15 years ago or more—no, about 12 years ago—that there was a specific instance of that at one location. I might say it is wholly against company policy to engage in any such conduct. It is also to be borne in mind that these employees using official business lines for official business are aware of the fact that their calls are subject to periodic supervisory observing.

Mr. KASTENMEIER. Let me recite to you the incident I have in mind.

Mr. CAMING. Sure.

Mr. KASTENMEIER. It is alleged by officers of Local 2108 in the Silver Spring area, that on or about April 4, 1974, they discovered electronic devices in a company garage wherein they had held, I gather, union meetings from time to time, and after investigating, they discovered that a craftsman had in fact put the equipment in under the direct supervision of the foreman.

Accordingly, they concluded that management was responsible. At that time they were apparently involved in grievances with the company, and they then reasonably concluded that there was a direct relationship.

Mr. CAMING. May I respond? I am familiar with that, highly familiar.

As you can appreciate, I was trying to give you an overview of the problem, and not recognizing the name of the particular local union—but this was a case not at all what it appeared to be on its face at first blush. This is a case, perhaps best described as consideration at a low level of supervision, of the use of audiovisual alarms.

Now, we do provide, under tariff, in a number of our places, audiovisual alarms to subscribers and others. The question was, a particular Maryland garage, the one at Silver Spring, as I understand it, was subject to a series of thefts, and various methods to protect the property of the company against losses, which ultimately our ratepayers bear, were used without success.

And the question arose then, see what else is on the market in the way of burglary alarms that might assist in apprehending the perpetrators. One of the subordinates installed an instrusion alarm, which was a perimeter alarm that when anyone broke into the garage during certain hours when employees were normally not there, it would sound a nonaudible-to-the-intruder alarm, and then this would permit activation of an audiosurveillance burglar alarm to overhear unusual noises and the like to see if a burglar was breaking in or perhaps an animal or the like triggered the alarm.

This was installed by a craftsman, as you mentioned. There was nothing covert about it, and at the time no notices had yet been posted, but it had been the intention to post notices because we use, for example, such audio alarms in Pacific Northwest Bell at remote loca-

tions high in the Rockies, at which there are unattended locations, and there are notices posted to that effect, that an audiovisual alarm is there, because it is some miles from the nearest human habitation.

Now, this was in for only 4 to 5 days on an experimental basis. It had not been approved by management yet, and it was only at this one location on an experimental basis. The question was raised by the union. That brought the matter to the attention, you might say, of middle management there, and on learning of it, they pulled it out immediately, and it was never used, except for this very brief period.

It was not permanently installed. It was determined first, that it did not appear to be a sound method for a burglary alarm system, and thus certainly would have not been approved under any circumstances. It was to operate after hours, and I believe that was all there was to it, and that was not for the purposes of overhearing, and if there were within that very short period, union officials there, that—as I understood the grievance, however, although those allegations were made, in fact it was known to the craftsman who put it in. He put it in himself. It was not put in covertly at night for some cynical purpose.

Mr. KASTENMEIER. Do you know who the company official was who was responsible for the installation of this particular device?

Mr. CAMING. I don't. I know he was rather low level. I know the commercial manager, I believe, Mr. Landon, was the one who removed it.

Mr. KASTENMEIER. Mr. Connor, would you know?

Mr. CONNOR. No, sir; I would not know.

Mr. CAMING. But I believe—I had talked, and I know personally of this incident, and it did occur over a year ago because I have these notes in connection with——

Mr. KASTENMEIER. Almost a year ago, according to the record I have. I will read you the first line of the letter, which I will offer for the record, from the president of the union, James E. Mazzi, April 24, 1974, and one line is: "Members of Local 2108 became aware of surveillance equipment in the Tech Road Garage on or about April 9, 1974."

[The letter referred to follows:]

COMMUNICATIONS WORKERS OF AMERICA,
Silver Spring, Md., April 11, 1974.

To: Chief Stewards.
Subject: Grievance Meetings—Surveillance.

This is to advise that as of today, April 11, 1974, grievance meetings should not be conducted in telephone company garages. I am aware of eavesdropping equipment in at least one Company location, the Tech Road garage. All anyone need do is dial the appropriate access code, and they are immediately connected to amplification equipment strategically mounted in the garage. Conversations in the garage are easily overheard by the calling party. The conversations could then be documented or recorded. For obvious reasons, we cannot run the risk of subjecting the problems of our members to this Big Brother surveillance system.

Ed Lewinski, our CWA Representative, is aware of the situation and has taken immediate action at his end. We will be discussing the problem in greater detail in the near future. In the meantime, protect your conversations. Don't meet in telephone company garages. You should advise all employees who work in garage locations of the possibility of any conversation being monitored.

Sincerely and fraternally,

JAMES E. MAZZI, *President.*

Mr. CAMING. I referred, Mr. Kastenmeier, when I said a year, I meant since I testified with respect to this on June 11. Mr. Watts was right next to me, you see. This is the second time around on this.

Mr. KASTENMEIER. This particular question was not raised at Government Operations.

Mr. CAMING. I said I knew about it fully at the time. That's why I had these notes. It had happened before June 11, is what I meant.

Mr. KASTENMEIER. Thank you, Mr. Caming.

Mr. Connor, are you supervisor for security with Chesapeake and Potomac Telephone Company?

Mr. CONNOR. Yes, sir, that's right.

Mr. KASTENMEIER. How long have you been employed in that capacity?

Mr. CONNOR. About 10 years, Mr. Kastenmeier.

Mr. KASTENMEIER. Last April, when Mr. Caming then appeared before the committee, he stated:

In cooperating in court-ordered national security cases, we endeavor to provide the very minimum assistance necessary as required by law to effectuate a particular wiretap. Under no circumstances do we do the wiretapping itself. That is the exclusive province of the appropriate law enforcement officers.

Is that correct? Do you agree with Mr. Caming's statement?

Mr. CONNOR. That's right.

Mr. KASTENMEIER. So that, in fact, is the practice followed here in this area in C. & P.?

Mr. CONNOR. That is—yes, sir, that is correct.

Mr. KASTENMEIER. Evidence obtained by the Judiciary Committee during its recent impeachment inquiry includes a May 12, 1973, memorandum written by Inspector O. T. Jacobsen of the FBI. This memorandum states that during the summer of 1969, FBI Supervisor James Gaffney received instructions to place wiretaps on certain telephones in an attempt to locate the source of unknown press leaks at the White House. The memo further states:

Gaffney, when he received the oral instructions to institute these wiretaps, would in turn orally request the telephone companies to effect the requested wiretap.

Now, we interpret this to mean that the phone company takes over in that case. What sort of assistance was Inspector Jacobsen referring to in terms of the company at that time?

Mr. CAMING. May I interrupt, Mr. Kastenmeier, respectfully?

Mr. KASTENMEIER. Yes.

Mr. CAMING. Mr. Connor did not—or were you involved at that time, Mr. Connor?

Mr. CONNOR. No, not in 1971.

Mr. CAMING. Are you referring to the *Halperin* case? I happen to be very familiar with it because I am one of the counsels in the *Halperin* case, and the 17 leaks in the House Judiciary Subcommittee——

Mr. KASTENMEIER. I am not necessarily referring to the *Halperin* case.

Mr. CAMING. But what I mean is, it's the incident where 17, according to the House Judiciary Subcommittee's evidence—17 individuals,

I think, 13 who were members of the Government, and 4 who were newspapermen, is that correct, Mr. Lehman, were in May 1969, subjected to so-called national security wiretaps, as designated by the Government in that terminology.

Now, Mr. Connor was not in that area, but I am very familiar with this incident, if I may. He did not take over.

Mr. KASTENMEIER. Who was, then, the——

Mr. CAMING. I believe then the Director of Government Communications at that time, Mr. Horace Hampton, handled those questions.

Mr. KASTENMEIER. Mr. Hampton, I see. Mr. Hampton has been retired.

Mr. CAMING. Yes; he has been retired for some years.

Mr. KASTENMEIER. But he was still active at that time?

Mr. CAMING. Yes; but I am personally familiar with the facts, if I may address myself to them.

Mr. KASTENMEIER. Yes; please do.

Mr. CAMING. You may recall—or you may not recall because it has been some time ago—that in my last appearance, I discussed at length the history of our involvement in national security wiretapping and mentioned that until July of 1969, there was no adoption of the so-called reduction to writing of the national security requests that we had theretofore received on infrequent occasions between 1941, when President Roosevelt, and every President since then followed it up until then.

It was at three regional conferences in July 1969, that we introduced the Hoover letter, as it was then described. That is one personally executed by the Director, or by the Attorney General.

Now before that, in May—and I might say the C. & P. Co., as I adverted to in my earlier testimony, did not adopt that letter until sometime later, in August of 1971. Up until then it had been our practice to provide assistance in connection with this, by receipt of an oral request from the properly authorized member of the Federal bureau.

Now, in that case, we did provide—we did receive a national security request orally, which was the practice, from the Federal Bureau of Investigation, and we provided equipment that went to the locations designated by the Federal bureau. The assistance was in providing the interconnecting channel terminal to terminal.

You may recall I testified—in my statement, you will find description of it on the April 26 date, and that we have appended hereto.

Now, in that case, one of those involved—and why we know it, one of the 17 happened to be Dr. Halperin, and I have just given a deposition of some 3 hours on this subject, and I am very familiar with the area. Now, we did not, as I stressed before the committee last, do more than provide the channel as required, and any cable and pair access information that would have been necessary in conjunction with it.

The actual wiretapping, the actual placing of the terminal equipment on the end, whatever it was, was done by the Government, and in that sense, as I have previously explained, we do not do the actual wiretapping. We have categorically refused to. We will not train them. We will not design wiretap equipment. We will not send our employees along, generally, to the site where it is being done.

And we've had repeated requests in this area for further assistance, not only at the Federal level, but at the local level, and we have said, as I have previously testified, that we do provide limited assistance, and we are to date in connection with national security investigations.

Mr. KASTENMEIER. In other words, the language, "to effect the requested wiretap," that Mr. Jacobsen refers to, in your view meant to provide access, and if you make some sort of connection for them. Is that——

Mr. CAMING. Well, generally, just to——

Mr. KASTENMEIER. To what extent is it installation as apart from conducting the actual auditing? I assume you do not conduct the wiretapping, but to what extent do you install the equipment?

Mr. CAMING. All right, if I may, both in court-ordered and in national security situations, court-ordered, when we receive a directive from the court to provide information facilities and technical assistance as required by section 2518(4)(e) of title III of the Crime Control Act, we do provide the assistance necessary, the minimum assistance necessary to effectuate the particular wiretap. That would normally consist of line access information in the form of cable and pair, and would also consist of a private line so that there is a connection running from the terminal of the suspect to the terminal designated by the Government, which presumably serves as their listening post. But we provide the channel of communication and the actual equipment, whether it is a tape recorder, whether a pen register or not, would be put on in that connection, made by the Government, and when a private line is provided terminal to terminal, the actual connection at the other end also is done by the Government.

Mr. KASTENMEIER. Thank you, Mr. Caming.

I am going to yield for my colleagues who have waited very patiently here, and I realize that they want the opportunity to ask some questions, too. So I am going to recognize the gentleman from Massachusetts, Mr. Drinan.

Mr. DRINAN. Thank you, Mr. Caming, for your testimony. I went back over what you told us about 1 year ago here, and you gave us the same information. I must say that it is a rather thin distinction between what assistance you provide and with what the Government actually does in the final act of wiretapping. But I think that you said last time, and you have said now, initially that the A.T. & T. collaborates and cooperates.

However, to come back to the question of the 1.5 million or the 1.8 million, just to make simple analogy that the supermarket has problems with monitoring people who like to shoplift, but at a moment in time they turn this whole thing over to the law enforcement agencies. I guess what we are arguing about is at what moment should A.T. & T. say now this is beyond our purview and turn a hard case over to the Department of Justice.

How would you feel about a decision that would say that you would have to do that? Why should you yourself, why should A.T. & T. make a decision to tap at a moment in time? Why not go and get a warrant? Why not turn over law enforcement to an outside agency? Why is A.T. & T. the police officer?

The supermarket proprietor at a moment in time has to call the law enforcement people and say we think that this particular person did

something. I am sure that you have thought about this, but I did not get a satisfactory answer. You people say that we are in charge, that this is our property and we can place our property under surveillance. How would you feel about a Federal statute saying that at a certain moment in time you too have to get a warant like the FBI and like other agencies.

Mr. CAMING. I am very pleased to address myself to this question if I may because I have thought of it very carefully and fully and we have conferred about it.

Mr. DRINAN. With the Department of Justice? Have you checked with the Department of Justice?

Mr. CAMING. Not as such, although we have, for the reasons I say, independently gathered our evidence. But if I can just start out by saying unlike a supermarket, we are a regulated public utility, subject to regulation not only by the Congress in general, but also by specific regulatory bodies, both at the Federal and State and at times local level.

Mr. DRINAN. And we have specifically withheld from you the right to do what you are alleging you can do. That you are regulated makes it more apposite. You do not have the right to tap a telephone wire just simply because you think this man is stealing, or keeping money. I mean, the statute does not really support your position, but go on.

Mr. CAMING. Well, for the reasons I have previously stated, I respectfully retain our belief, and the courts have sustained it uniformly, that we can protect our rights and property, and the *Beckley* case, which I personally handled, did just what we have recited here, and we did go up to the U.S. Supreme Court in *Hanna* and *Modell*, and the very strong opinion of the fifth circuit court of appeals was affirmed. The *Brandon* case was affirmed, the *Nolan* case went to the Supreme Court and cert. was denied.

We are not talking first—the reason I mentioned it was a public utility, Father Drinan, is——

Mr. DRINAN. Excuse me; *Hanna* was before the change in the law, was it not?

Mr. CAMING. That's right.

Mr. DRINAN. Well, that weakens your case.

Go ahead.

Mr. CAMING. Well, not necessarily, because *Hanna* has served as the landmark for a long number of cases that have followed, and the *Hanna* case is one of the cases that followed the *Beckley* theory and that was recognized in title III, which says we have the right to protect——

Mr. DRINAN. OK, sir, but tell me your policy reasons for why you do not want to get a warrant. Why do you not turn these matters over to law enforcement? You would save a lot of money, and the public would be assured that an outside agency, a Federal agency is in fact pursuing these obvious thieves who use the blue box and the black box.

Mr. CAMING. I wish it were that simple because it would certainly be saving us a great deal of trouble and difficulty.

First: We are not talking, as I adverted to earlier, about wiretapping. As I said in my statement, we are not seeking to obtain the contents of conversations of lawful calls, of lawful calls to obtain evidence of some other crimes than the theft of the call itself.

Now, if the call is legally placed, and let us say it is a call between two narcotics pushers, the telephone company does not have the right nor access to its contents. That is the law and we adhere to it.

Second: That is to access its contents for purposes of proving narcotics trafficking.

We are talking about monitoring selected, particular lines in specific cases to detect the fraudulent use of the service through electronic toll fraud devices in placing the call, where it circumvents the automatic billing equipment. We are not interested, I submit, interested in the contents of the conversation as such. Rather, we are discharging a statutory duty which is imposed upon us by the Communications Act and by our regulatory bodies to not permit people to knowingly make in volume calls which are illegal. To identify the person—and it may be a little long-winded——

Mr. DRINAN. We all read that. We have read your testimony. We read your testimony a year ago, and other Government Operations Committee material that is furnished us, but you keep saying the same thing, that you have a statutory authority to protect the company property, but that is begging the question.

Mr. CAMING. I agree with you. I am just merely reciting.

Mr. DRINAN. I know, I have heard this before. I want you to answer the question. Why doesn't A.T. & T. say it would be a beautiful thing if we could have Federal officials do all of this work for us and train them so that they are the law enforcement people, just like any other business. Granted, your business is uniqne, but in a moment in time, it seems to me that when you have clear evidence of wrongful acts, illegal conduct, you have to turn it over to somebody else.

Mr. CAMING. I agree with you 100 percent, and that is just the whole point. Now, that is what I have been trying to say and I know I am slow in getting to my points at times, and I hope you will indulge me, but I work in that way. That is why I was stressing the contents of the calls illegally placed, requires certain evidentiary minimal gathering of evidence before you have anything, because if you do not identify the criminal, you cannot have a crime.

Now, the monitoring and recording we do is done solely by us and I think this is important, and we do not make wholesale incursions. We do it in a limited number of calls.

Secondly, to have court orders would virtually eliminate prosecutions.

Mr. DRINAN. Why? Why? This is the key point now.

Go ahead.

Mr. CAMING. What I wanted to point out is that we must have a certain minimal probable cause in order to get search warrants, to have grand juries return indictments and the like. Now, when we selectively gather the very minimum evidence, very limited recording—and remember, this is not to get the contents of the conversation as such, but rather to establish that the call is being illegally placed—we must record, and as I say, it is usually 60 seconds or less, and we then can identify, A, who is calling, because through these portable devices, for example, you could use——

Mr. DRINAN. OK, Mr. Caming. I want to yield to Mr. Pattison. I have only 5 minutes, but would you explain this.

You said, "getting court orders would virtually eliminate prosecution," and that is why you are against them. Why?

Mr. CAMING. Because we would not be able to have the probable cause until we were in the stage, as we are now; when we do this minimal recording we get not only enough to establish probable cause, but we immediately are ready for prosecution, and every case we have is prosecuted to the extent we can get it accepted.

Mr. DRINAN. Well, now, you do not go to the courts because it is to your convenience.

Mr. CAMING. It is because it's in the public interest.

Mr. DRINAN. Well, in the interest of A.T. & T. to save a little money, but the public interest says, and the fourth amendment says, that the FBI, if they want to do an electronic eavesdrop, must get a written court order, and then within 90 days they have to inform the subject of the wiretap. You know all the things that are in the law.

Well, I see your point. I see the property point, but what would be so calamitous if we said that the telephone company must also go through this procedure or something comparable?

You have given one reason—that it would virtually eliminate prosecution. Now, the fourth amendment makes things very complicated because it does cut down maybe on prosecution because you have got to prove to a judge first that yes, there is probable cause, and we think we have got to tap this guy. He is using the blue box.

Well, what is so terrible about that? Why do you not prove it to a court before A.T. & T. itself goes in.

Mr. CAMING. OK, for two reasons, if I may. First, we are saying why don't we show the court there is probable cause that this guy is using a blue box and therefore get it—because we cannot show that unless we have enough evidence to show that minimal amount, and once we have that minimal amount, we prosecute. We do not need any more evidence than that minimal amount. We do not go in on a series of calls over 6 months. We take 1 or 2 or 6 days of calls, perhaps 10 calls. We go in, we prosecute, and remember, every one of those cases are subject to exhaustive judicial scrutiny, and not once has there been any abuse shown. Unless we have that minimal evidence necessary to turn it over to law enforcement, what I am saying is——

Mr. DRINAN. Well, Mr. Caming, it still comes out to me that it is very convenient for you and very convenient for everybody to finesse the fourth amendment and the regulations that apply to implement it.

And then let me ask one question and then I will yield to Mr. Pattison.

A year ago, before the Government Operations Committee, you said, "Customer to customer conversations have never been recorded in the Bell System." I am not suggesting an open inconsistency, but why has A.T. & T. been so secretive about all of this going on?

If you want to make any explanation of that, it would be helpful, I think.

Mr. CAMING. Very well.

May I just make one remark with your indulgence? You mentioned the fourth amendment, and you see, I think you and I are on the same side, Mr. Drinan. It is just that apparently I am not articulate enough to get across to you what I'm trying to say.

We gather, and I say this in tactful terms, but I think the nuance is, we gather our evidence independent of law enforcement, first. Second, we gather only enough to establish the minimal probable cause. When we have that we have enough to convict. Third, we are subject to judicial scrutiny, full judicial scrutiny on each case, because unless we can prosecute each case there is no deterrent. Fourth, with respect to the fourth amendment, sir, I respectfully refer you to a number of cases, including *Katz* v. *United States*, where I am sure you are familiar with the case which states in part that one who encloses himself in a telephone booth, and I quote, "and pays the toll that permits him to place a call" is within the protection of the fourth amendment. This is apart from the consideration of *Burdeau* v. *McDowell*.

Now, to address myself to your other question, if I may, on customer-to-customer conversations not being observed, I believe your references may have been to statements such as the following, and I read from page 179 of the hearings before the Subcommittee of the Committee on Government Operations of June 11 and 13. We were then addressing ourselves to questions, what do you do in service observing. That is all we were talking about, and I give you the question.

To what——

Mr. DRINAN. All right, so that is an adequate explanation, but it was very broad, and frankly I was surprised doing my homework to find that broad statement, and it just goes to demonstrate the point that you have not told anybody, including the law enforcement officials, of the 1½ million bugs or intercepts. I just raise the question of why did you not go to the law enforcement officials and say to the Department of Justice, we need you. It is a very complicated case.

In any event, thank you, and I yield to Mr. Pattison.

Mr. CAMING. May I, with the indulgence of Mr. Pattison and the Chair, may I respectfully address that question just to give you background. You said we did not go to the Department of Justice. That is not true.

Mr. DRINAN. Well, you just a little while ago said you had not consulted with Justice.

Mr. CAMING. I though you were asking me about the wisdom of having them work with us to gather evidence of toll fraud. If you are addressing yourself to the question of whether we informed the Department of Justice, we did. I did personally. I informed Mr.—I don't know whether you want to go into it, but in 1966——

Mr. DRINAN. Well, this contradicts what you just told me.

Mr. CAMING. It was just that I misunderstood your question.

Mr. DRINAN. The question was crystal clear: Did you consult with the Department of Justice? And you said "No."

I have it right down here, but go ahead.

Mr. CAMING. It was my understanding that your question was addressed to whether I consulted with respect to your suggestion about court-ordered wiretapping, but as far as the monitoring—and I respectfully want to just call it to your attention, we did in 1966 and again in 1967, in the discussions of the Hanna case, I informed the Department of Justice attorneys involved in the Criminal Division, of the scanning equipment, and on one or two occasions and again in 1967 when I met with them on a general survey, some of the leads from

that equipment could possibly, we thought, have come from—I'm sorry, some of the leads in that case which involved some gamblers in Miami, could have come from either some of our computer printouts, some of our informant sources, some of our plant testing gear, or possibly this equipment at the time. There were a number of leads, and I accordingly did inform the Department of Justice.

Now, that does not say they cleared it or gave me their imprimatur. We did not feel we needed it. And the law has clearly held, at that time, that there was no violation of 605, but we did inform them, and if I misstated my understanding of your question, I respectfuly apologize.

Mr. DRINAN. All right. Thank you, sir.

Mr. KASTENMEIER. The gentleman from New York, Mr. Pattison.

Mr. PATTISON. I just have a couple of questions.

Suppose that the law was that it was illegal for you to engage in this kind of monitoring, and that it was very clear that it was the Federal Government's responsibility only to detect this kind of theft of telephone services. What would be the result of that in terms of the amount of recorded conversations that might be turned over to other people?

In other words, in your judgment, would it be more likely that the actual conversations that are recorded, that deal perhaps incidentally with illegal activities or private matters, to get out if the Federal Government were doing it as opposed to the telephone company doing it?

Mr. CAMING. I honestly think it is a question of judgment, of course, and I can only give you my opinion. Unquestionably, first, we only take the minimum amount, so that normally we cut off at the start of conversation. Second, if we find evidence of other crimes than toll fraud during our toll fraud investigations, we do not—and I repeat, we do not disclose that to the Government. The only way it could be disclosed is as part of that minimal number of calls.

Mr. PATTISON. Whereas, presumably, if the Government had that information, it would be more likely to use that information in the prosecution of those crimes.

Mr. CAMING. I think that is a conclusion that I respectfully would have to bow to the wisdom of this subcommittee on. I think it speaks for itself, that no one could do less recording than we could. When we get this minimal amount of recording, if we don't have this much you could not even get a search warrant. When we have this very limited amount—and most of ours is not recording—we have computer tests, plant testing. We are working on further developments to attempt to eliminate more and more of the recording. We immediately go, make proper disclosure, and go before a grand jury and get a search warrant. We do not have any further recording. As I say, this one incident that I gave you where there has been lots of illegal calling known and admittedly for several years, we went in on six calls. That is all we stood on.

Second, each of these cases is thoroughly examined by the court to see whether there is an abuse.

And third, it is not A.T. & T., I respectfully say, but our honest ratepayers that would ultimately have to bear the losses, you and me.

Mr. PATTISON. Just one other question.

I take it that it is your position that the words in the proviso to section 2511 random monitoring, are unfortunate words in the sense that

the random monitoring which is referred to there, is not what a layman would think of as random monitoring, but is a term of art which means service observing.

Mr. CAMING. That is quite correct. I could cite you in the cases in my testimony and testimony of our prior witnesses; for example, Mr. Kertz, who appeared before the Congress prior to this Act being enacted, who constantly used the term random monitoring. We have given information to the Jackson committee, for example, and others the Government Operations Committee that uses this term continuously. You look at the answers to our questions that I adverted to, full of random monitoring.

Now, it states, and I just would like to repeat, this provision was inserted to assure that service observing will not be used for any purpose other than mechanical and quality control. That is one point. The legislative history, too, that it would in effect—this is specific monitoring, not random monitoring, as Mr. Kastenmeier pointed out. Third, you must have a human ear to violate title III, aural acquisition, and so those are our positions.

Mr. PATTISON. But the normal meaning of the term random monitoring, and as applied to the activity of the 30 million calls, it would seem to be the same to the——

Mr. CAMING. I would agree, and we would say that was random monitoring, but without human ear, and without it meaning the type of random monitoring——

Mr. PATTISON. But not random monitoring without the meaning of the proviso.

Mr. CAMING. Exactly.

Mr. PATTISON. All right. I just wanted to make it clear.

I have no further questions.

Mr. KASTENMEIER. I have several concluding questions.

Just to return to a point so we can put it to rest, do I understand your testimony to say categorically that the listening device of which local 2108 was complaining, was not installed in the Tech Road garage for the purpose of overhearing union personnel?

Mr. CAMING. Categorically, sir.

It was done for only a period of 4 or 5 days until it came to light. It was done to serve as an audiovisual alarm, or an audio alarm for burglary purposes in a garage that had been subjected to a great many thefts. It was done, too, by a craftsman, which is self-evident that we are publicizing it, since he as a member of the bargaining unit, may well have been a member of the union.

Mr. KASTENMEIER. Another area which we have not really discussed, which I would only refer to briefly, and that is to the extent that toll billing records are made available either to law enforcement or private parties. I refer to this because a week ago Thursday some records were introduced into the testimony before this subcommittee which indicated that toll records in Madison, Wis., and presumably elsewhere throughout the country, were made available to the Secret Service, on mere oral request. That is in 1972.

Now, since February of last year, at this time, Bell System has a policy, as I understand it, that the toll billing records of a subscriber will be released only upon receipt of a valid civil or criminal subpena,

or administrative summons. Is that correct? This is part of the Bell System policy, and this is about a year old; it did not exist prior to February of last year?

Mr. CAMING. That is correct in this sense.

Mr. KASTENMEIER. I have given a very superficial statement of what your policy is.

Mr. CAMING. In March 1, 1974, we initiated a change of policy in which lawful demands of authorities in form other than administrative subpena, summons, or court order, were no longer acceptable, and that thereafter we would only disclose—and this is part of the warp and woof of our policy of not unduly cooperating and our refusal to cooperate except at arm's length with law enforcement, and of which there are many other illustrations. We now only disclose under a subpena or a summons.

However, prior thereto, it was our practice in a number of our companies to disclose under subpena or summons or other demand of lawful authority. Now, in this respect the courts had held and the Federal Communications staff had so agreed that toll billing records were subject to demand by proper law enforcement authorities. That was and I believe is still the law, and there is a host of cases, and I would be glad to even furnish the committee with a memorandum I wrote on October 29 before our change in policy which addressed itself to that.

So what we did before, such as with the Secret Service, was wholly lawful, was wholly consonant with our understanding. We on our own, however, felt it was advisable in the change of climate, further strengthening of privacy and expressing our concern for it, to on our own introduce a policy not only of subpena, but of automatic notification to the customer when the subpena or service is provided, absent the certification by law enforcement that it will impede a criminal investigation or by a legislative committee.

Mr. KASTENMEIER. Following up on that, then, normally you state to the law enforcement authority requesting the information and armed with a valid subpena that you will notify the subscriber within 24 hours unless that law enforcement authority indicates that such disclosure would impede the investigation being conducted, in which case the existence of this disclosure of this information would be deferred for 90 days.

Mr. CAMING. Mr. Kastenmeier, as you know, I always make as full a disclosure as possible. May I give it to you?

First of all, we will only accept a request for nondisclosure because it would interfere with an investigation, if it is an official investigation of a suspected felony. We do not do it in cases of misdemeanors. Then we will do it for a period of 90 days, withhold notification, and such notification is subject to renewal, just so that you are not in any sense——

Mr. KASTENMEIER. Subject to what?

Mr. CAMING. Subject to renewal, just so you are not misled.

Mr. KASTENMEIER. Well, that is one of the points.

Mr. CAMING. This would require a new certification in each instance by law enforcement. It would be equivalent to the extension of a court order in the title III proceedings. Bearing in mind, too, that the whole

question of notification is one that we strongly have endorsed, but we do recognize that there are the countervailing considerations when a certification is present.

Mr. KASTENMEIER. The reason I ask this is, while this has been Bell System policy since last year, we must decide whether something of this sort should be imbedded in the statutes. We are considering a bill which covers disclosure of private records such as bank records and phone company records

Mr. CAMING. Well, I would say first that over the long history of the Bell System, when we take a course like that we have never regressed. Anything that has furthered privacy has remained. I would submit respectfully that it is a question of national policy for the subcommittee to determine on really balancing on the one hand the individual considerations and the individual right to privacy which we think is so important, and the very important countervailing considerations from a social standpoint of law enforcement authorities acting under the strictest terms.

We personally have found within the last, almost a year now, that this has been uniformly adopted and enforced throughout the Bell System. It is working very well. I see no reason that we would ever consider changing this policy, and whether it should be imbedded in a statute is something that I would respectfully defer to the committee on.

Mr. KASTENMEIER. OK, fine.

The last question I have is the size and cost of the security force maintained by the Bell System, and to what extent it is, regional or local. That is to say, does the Chesapeake and Potomac or Southwestern Bell have its own security force. Is it independent of the national Bell System?

Mr. CAMING. Very well.

To address myself to the first question, I would say that since each of our 23 operating companies and the long lines department, which would be 24, plus Bell Laboratories and Western Electric, we have 26 independent operating entities. They are truly operating independent companies with presidents, boards of directors, responsible to local, State regulatory bodies, as New York Telephone Co. and the like. They are employees of and under the direction and control of their respective companies, so these are separate forces. We consider them that we treat them—it is just like with our various presidents. When we introduced this policy on toll billing record, we sent it to the security men. We also have security counsel in each company, legal counsel, especially trained and able. Mr. Kelleher, for example, who is with me today, is the general attorney and security counsel of C. & P. Co., and in the toll billing problem, when we forged the policy at A.T. & T., and I played a principal role with others in the operating end of the business, we then submitted it to the presidents, to the security managers, and security counsel through them, and the vice presidents and general counsel for consideration. We then got their comments. We adopted the policy. When there is a policy evolved, it is a system policy, and it is enforced by the system in the sense that if it is a policy that is violated, the system is concerned as well as the individual company.

Now, with respect to the numbers in the companies, in the 28 operating entities, if you take the A.T. & T. and include that in it, there are only in the 28, 644 employees out of over a million total employees by these companies. We have assets in the order of probably close to $70 billion plus revenues, which I have the statistics on, revenues for 1973 were $23.5 billion, in addition to $70 billion worth of property, or close to it.

The securities department's function, I might say, in areas like wiretapping and electronic toll fraud is a very minimal part of their overall responsibility. These 644 employees cover all of the companies. Now, of that, the number, because I have seen it bruited about in the press of our having a great many members of the Federal Bureau, we only have 42, 6½ percent of our total force, are former members of the Bureau who are in security positions, and most of them are people of relatively short Bureau experience and such long telephone experience that although we don't think—and I don't mean to say it washes out their sins, because I am sure they are without sin, to be facetious for a moment—still, they are of long telephone experience.

And let me give you a figure that may interest you. We have the heads of our 28 groups, only two of the operating heads—the New England Co. and the Northwestern Bell Co. at the present time—have had any FBI background. The head in security and one in Western Electric, which is a non-Bell—I'm sorry, in A.T. & T. security, and the one in Western Electric, which is a nonoperating company, also are members of the FBI.

Now, let us look at their experience just to give you an illustration. New England Tel, 6 with the FBI, 20 with the telephone company; Northwestern Bell, it was 12 and 5. In the case of A.T. & T. it was 21 and 5. We have in addition—and of that, less than 1 percent of the force are retired FBI personnel of that 6½ percent. The others are very short term.

We also have some 50 others, which would be 7.8 percent of the force, who have some law enforcement background, non-CIA. We only have one or two others who were in the Federal group, not that there is anything wrong, with reference to members of the CIA. I am sure they make very attractive security people. They don't seem to seek telephone company work.

Mr. KASTENMEIER. There is nothing wrong with that, or being a former member of the FBI. As a matter of fact, several members of the Judiciary Committee are former members of the Federal Bureau of Investigation.

One of the reasons, to interrupt, however——

Mr. CAMING. I'm sorry.

Mr. KASTENMEIER. And there is a numerical inconsistency here. There was a column in a news release, an AP release covered in the Washington Post last month on January 1, which indicates that the Bell System, the legal eavesdropping in the Bell System is done by the small, tightly organized group of not 644 employees, but 665 security agents. They control when, according to this article, when, where, and how it is done.

At least 76 members of that force are former FBI agents. You indicated 42. And then it refers to a spokesman for A.T. & T., and

then the next paragraph, the spokesman, Attorney H. W. William Caming, and so forth. So, I am wondering, how do you explain the difference?

Mr. CAMING. Well, understandably with the vast press of problems that the newspapers have in meeting the deadlines, and the various sources they gather from, some of whom are not necessarily thinking of the best interest of the public or the Bell System, these figures may have arisen. I know not the source. These are figures which I have had taken and prepared in great depth, effective January 1975, of the Bell System. These were responded to by each of the companies. This is fact, not allegation.

Mr. KASTENMEIER. I take it that the reporter obtained his information from what he thought was reliable sources, but not from you. I would only note that there is not a great deal of discrepancy.

Mr. CAMING. I will respectfully defer when you say from reliable sources. I cannot comment on that whether they were, but I do know that there is no question about this, Mr. Kastenmeier, this is fact. I can produce every name, and there are no others except this group that I know of that handle any function.

Now, if it appeared in the newspaper, I am sure that the reporter did think he had a reliable source, and it is a very highly regarded newspaper, but in fact, this is the statistical situation and I am powerless to say anything else, except express the facts.

Mr. KASTENMEIER. Actually the deviation is minor, although 665, or 644, one referring to agents, and the other to employees, whether the 644 could not be referring to all as agents, I take it.

Mr. CAMING. May I say, as there are members of the Judiciary Subcommittee with an FBI background, there are members of the telephone industry with an FBI background who are not in any way connected with security. There are 20 to 25 of those.

Mr. KASTENMEIER. Well, no, the story says at least 76 members of that force are FBI agents.

Mr. CAMING. Well, all I'm saying is the facts are, so that you can rest assured what they, and we will be glad to, if you wish, produce every one of the 665 names, or whatever, 644.

Mr. KASTENMEIER. That will be fine. Yes, we would request that for the purpose in following this matter up. That would be useful.

In the nature of what annual expense is incurred by the Bell System, by A.T. & T. in maintaining this security force and in its operations?

Mr. CAMING. I would have to have those figures assembled. I am not prepared. I think we would have to poll the individual companies. As you can recognize, we operate nationwide. The amount that we expend for this security force, in view of the major responsibilities in the area of prevention, in areas of indoctrination of employees, as well as detection of crime, make this a very small proportion of our total revenues of $23 billion a year.

Mr. KASTENMEIER. I appreciate that. One of the reasons I asked this, to give you fair warning, but I am sure you are able to assess it anyway, is because of the allegation made that while the company suggests that the blue-box problem is the major reason to maintain a security force of this size, that as a matter of fact, the cost of the force, even as imputed to the little blue-box problem, exceeds the losses that are attributed to it.

Now, without arguing that point——

Mr. CAMING. May I respectfully address myself to that because I think that that statement is understandable, quite, Mr. Kastenmeier, but it has nothing to do with the facts, which I am sure you are most interested in. First, there was no imputation that the speaker is not at fault, nor that the major use of our security force is in electronic toll fraud. What I said was that if electronic toll fraud is not scotched like a snake wherever it appears, the losses could be of staggering proportions and you could see if one-half of the population had a blue box it would clog the facilities and destroy our ability to serve effectively.

But our security forces' functions overall are in the area of prevention, protection of property, protection of assets, there are many other types, coinbox larceny, credit card fraud, third billing fraud, the actual physical safeguarding, instruction of personnel, deciding how the property is to be supervised and protected. These are the functions of the security. The 644 do not devote themselves to electronic toll fraud. I repeat, they do not. It is a very small, select group in each company, and we are only talking of 644 in 28 companies which, due to my very poor mathematics, I hesitate to speculate on proportionately, but I think it's only about 25 to a company. We cover 48 States, and we are engaged in innumerable activities, court ordered wiretapping, for example, takes some personnel. Treatment of personnel. So that 644 in nowise reflects within each company those who engage in electronic toll fraud. It is a very small segment of that group. Most of this is done mechanically by computers, by testing gear. It is done by accounting departments, and it is done by receiving aid from informants.

We just did with reference to a gentleman who is well known for a bevy of beauties, and one of his beauties was using a blue box which got a great deal of publicity in the Los Angeles area. But the number of personnel of the 644 devoted to electronic toll fraud is a very small proportion, and the amount of savings in proportion to that is very substantial. The potential savings are beyond compare.

Mr. KASTENMEIER. Therefore, the company official of Southwestern Bell Telephone who was quoted in the press as saying that the security force of Southwestern Bell Telephone was essentially devoted to matters such as the little blue-box problem is probably incorrect and inaccurate.

Mr. CAMING. Yes; I think you have reference, without mentioning his name, to the ex-Southwestern Bell employee who is suing for some $29 million, and who has made many newspaper allegations.

We will respectfully respond to them. We are very carefully——

Mr. KASTENMEIER. I was not referring to him. I was referring to the defensive explanation on the part of a company official. His allegation was not that. The defensive response on the part of a company official in Southwestern Bell Telephone was that, well, we need all these security personnel for the little bue-box problem. But you are indicating basically your personnel are not used for that problem.

Mr. CAMING. I would say that certainly they are used for that problem, but from a Bell System-wide standpoint, and I think, for example, in the C. & P. company, we have Mr. Connor with us, it would be a good illustration that a very small fraction of their time, an important fraction; just as it is with credit card fraud, coinbox larceny, a very small fraction of that time is devoted to blue-box fraud, and that is the system practice.

Now, in a particular area, or in a particular set of circumstances, the problem could be more acute than others, as in some cases we have areas where we have a great deal of coinbox larceny, and in other areas, like Madison, Wis., we have very little, is our experience, but this does not mean coinbox larceny is not a real problem in New York City.

Mr. KASTENMEIER. In conclusion, Mr. Caming, I would request, and, of course, it would require some time, I suppose, to accumulate the figure on the costs of the Bell System, and its subsidiaries in maintaining a security force, and the names, and at least superficially the background. I guess we are really interested in the Federal agency prior connection of certain of the security force people.

I gather Mr. Drinan still has some questions.

Mr. DRINAN. Yes; I do.

Mr. CAMING. May I, Mr. Drinan, just to clarify Mr. Kastenmeier's question, I would like to give the committee a full view. You have mentioned the Federal forces. If I may respectfully, I would like to also include any local or State officials. We have nothing to hide from this committee, and I would like to give the background on all of them.

Mr. KASTENMEIER. That would be very helpful. I do not wish to impose something terribly difficult.

Mr. CAMING. It will take awhile. I have the figures right now, by the way, but I do not have the names of the individuals. If you want just the figures and the breakdown completely without the names. I can give you those.

Mr. KASTENMEIER. We will wait for whatever you have as a composite.

Mr. CAMING. In other words, you would like the names of each individual.

Mr. KASTENMEIER. We would.

Mr. CAMING. It will be a pleasure.

Mr. KASTENMEIER. I would also like, and here I think generalities would be all right, more or less the breakdown of overall devotion to certain tasks. For example, if 15 percent of the time is devoted to toll fraud cases, and 15 percent of the time is devoted to cooperating with Federal authorities and installing wiretapping devices, or whatever.

Mr. CAMING. Zero in installing wiretapping devices.

Mr. KASTENMEIER. Well, whatever.

Mr. CAMING. I know, title III, court ordered, or the like, toll fraud or indoctrination of employees, and protection of plant.

Mr. KASTENMEIER. Yes.

Mr. CAMING. Certainly we'll give you the complete story of the entire overall.

Mr. KASTENMEIER. The mystique or the mystery of at least some of these so that we can determine to what extent some of the stories that have already appeared are correct or incorrect.

Mr. CAMING. It will be a pleasure, and if I may, I will work with Mr. Mooney and Mr. Lehman in providing the figures.

Mr. KASTENMEIER. Mr. Drinan?

Mr. DRINAN. Mr. Caming, I would think you would want a clear Federal statute to warn all people that the use of a blue box is a crime and that they can be prosecuted.

Have you people thought of seeking a Federal statute that would make it clear beyond a doubt that the use of a blue or black box is not merely a fraud on the phone company but it is a serious crime?

Mr. CAMING. Yes; we have. We have in a number of States statutes that say use, manufacture and possession, sale, advertising of blue boxes, et cetera, is a serious crime.

Mr. DRINAN. Would not a Federal crime——

Mr. CAMING. That would be very helpful. We do use fraud by wire, section 1343 of 18 United States Code.

Mr. DRINAN. Why do you not propose a law. Maybe it will be less murky than the one that turned up in 1968. We are here to help you and to prevent all of the misunderstandings that may arise.

Now, reading the two or three cases here since 1968 that support your position, I would feel, and I think that you would, that you are going to have a different result some day, that if you continue to litigate this in the court, some lawyer is going to turn up with some angle on this thing that it seems to me that will say that you may not monitor because monitor is a euphemism for intercept. There is just no doubt about it, that the random monitoring means random intercepting, that you listen. And in the case, for example of the gentleman from abroad—what is his name, Mr. Shaw, that you, the telephone company, listened until you found the name of Mr. Shaw, and then you called in the authorities. Well, this must have occurred to you that when you think that this is happening, why do you not ask the Federal or State authorities to get a search warrant and go and try to get the blue box. That is the way of circumventing all of this.

Mr. CAMING. We have, and I think this is well taken. I would like to thank you for the opportunity to present some legislation.

Second, we have employed that and we do wherever possible. However, because of its small size, portability, the fact that it is often used on a variety of telephones, it is very difficult to seize this in use, and unless you do that, possession is not illegal under Federal law.

Mr. DRINAN. Well, that is the whole point, you see, why do you not make possession—I take it that the blue and black boxes can be used for nothing else except to defraud A.T. & T.

Mr. CAMING. Exactly.

Mr. DRINAN. It seems to me that mere possession should be a crime, and then you can get a search warrant, and then the appropriate officials can go, and then this is destroyed.

Mr. CAMING. We still might require—and this would be very helpful—I am delighted, and I agree with you completely, it still may be necessary to have a very limited amount of recording in order to identify the criminal, in order to get the search warrant. In other words, we have to have a minimal probable cause, and that is our present philosophy. We do not stay on the conversation, and we do not record a large number of calls.

Mr. DRINAN. Well, one very technical point that perhaps you would want to submit something on this, but there is a device I understand, M220, by which you can preclude the necessity of actually intercepting or monitoring a call.

Would you explain the technical aspects of that or if you want——

Mr. KASTENMEIER. Well, actually, if the gentleman from Massachusetts would yield, we had asked Mr. Mack of Western Electric to come and explain something about the M220 observing system.

Mr. DRINAN. All right. I yield back to the chairman, and we welcome this gentleman.

Mr. KASTENMEIER. If very briefly you could explain that, Mr. Mack, it would justify your being here this morning.

Mr. MACK. Now the question——

Mr. CAMING. He has been very helpful, I might say, in preparing me for today's presentation.

Mr. MACK. The question is the need to record voice, essentially. Could you, Mr. Drinan, state the question again so I can make certain I——

Mr. DRINAN. Would you just tell us that the usefulness of the M220 and that if this is used would it preclude the necessity of actually monitoring the conversation until A.T. & T. finds out the name of the caller?

Mr. MACK. Right.

Mr. CAMING. There certainly, in the modes of operation of the MTTU—oh, is that the one you are referring to?

Mr. MACK. You said M220.

Mr. DRINAN. This was described in part on June 11, 1974, to the Government Operations Committee, and I have here a memo, which, frankly, is very specialized.

What I want to find out is whether or not there is some way of circumventing the problem of the possible violation of Federal law by using ultrasophisticated devices which in no way cut into the conversation of human beings.

Mr. KASTENMEIER. I believe Mr. Drinan is referring to the remote observing system which was explained during that hearing in part. That is an M220? Is that not what it is called?

Mr. CAMING. I know what the difficulty is because I was there, if I may interrupt, and I am afraid the designation is understandably confusing. That is probably the technical designation for Tel-Tone equipment. The minute you mentioned the committee hearing, I knew it.

Tel-Tone is equipment which permits us to remotely access for service observing purposes, plant repair bureaus, and service business offices to which calls are made, and instead of hard wiring, as we have in the past, the interconnection between the place being observed where the calls come in at random and the service observing bureau, is done remotely by dialing up first a security access telephone number of, say, 7 or 10 digits, and if you were in Washington, you could access a Baltimore plant repair bureau. Then a special tone comes back. Another security code must then be emitted within, say, 5 seconds. That then permits you to randomly monitor the plant repair calls to the telephone company or the business office calls at Baltimore.

That is the equipment to which reference was made at that hearing. And then they do actually overhear the contents of those business calls.

Mr. KASTENMEIER. May I just interrupt to ask one question in terms of the language? The term "observing" is employed both officially and

as a matter of testimony. I am wondering whether "observing" has a special meaning.

What does "observing" mean in terms of electronics?

Mr. CAMING. "Observing" is really used in the telephone industry as a word of art in two senses. One is the so-called service observing. That is, the official service observing whereby we statistically, for quality control purposes, monitor at random up to the start of conversation by a select group of people in service observing bureaus. That is what the statute referred to in the proviso when they say "known as service observers." These are at special locations. Mr. Lehman was to one with Mr. Mooney, I believe, and there they merely observed the quality of the calls, outgoing DDD calls, incoming calls, and the like.

Now there is the term "supervisory observing," which is done either by the telephone company or by certain business subscribers who sign prescribed agreements to comply with certain tariff preconditions for observing on the quality of service of individual employees who are apprised of that observing. And that is done for quality control of the individual employee.

The service observing is purely done by the telephone company to get the tone of the office. There is no identity of individuals or any specific unit of operation.

Mr. KASTENMEIER. There is no visual connotation whatsoever?

Mr. CAMING. There is observing done and we do use that term. Observing, for example, within a traffic room by our service assistant in the old days, or walking behind the operator, or by a group chief operator walking behind and watching girls today at TSPS boards and how they operate. We could usually call that observing or visual observing.

Mr. KASTENMEIER. Well, thank you. Going back to the question posed by Mr. Drinan, Mr. Mack, is not the remote service observing of the Tel-Tone system's M220 essentially for overhearing rather than for—well, let me ask you, for what purpose is such an instrument used for?

Mr. MACK. I think that—I believe that Mr. Caming really stated it. That purpose is to centralize the operation of the observing, and in this case we are talking about oral observation.

Mr. KASTENMEIER. It appears, if I understand your explanation, which, perhaps, you have not had an opportunity to give, this is a system which can be employed for wiretapping if you know the code, for wiretapping in a rather indiscriminate manner by unauthorized people, people other than phone company people or people authorized by law.

Built into the system is the susceptibility for such equipment being used for overhearing or substituted for wiretapping in a much more sophisticated sense.

Is that not true?

Mr. CAMING. May I respectfully answer that because that was the question I discussed at length and I refer you to the hearings of June 11 and our written answers thereto on Tel-Tone which appear, Mr. Lehman, on page 177 and before that—which describes this equipment. It cannot be used for wiretapping in any sense of the word, and also, it would be the most cumbersome way of doing it.

What this does—see, we do have bureaus—service bureaus, for official service observing for statistics which are presented to the FCC, the State regulatory body, and for us to determine the quality of our service. It is purely anonymous, random monitoring, as I adverted to in our earlier testimony before the Long committee.

Now, all you can do if you—first of all, you cannot access this from an ordinary Touch-Tone telephone. When we first used it on a trial basis in a couple of companies—and the equipment is made in the State of Washington by the Tel-Tone Corp.—it was accessible by—if you had stolen the codes which were closely guarded, it would then be accessible by the ordinary Touch-Tone telephone.

We immediately took measures of the following nature to insure against it. There are two security access codes which are changed with regularity. The first in 2-week periods; I think the second now at once a quarter.

In addition, these are very carefully held in a service observing location.

Third: You have to use special equipment now which is not the ordinary Touch-Tone telephone.

Fourth: Even if you access the line, what would you get? You would get random calls to the plant repair bureau or the business office. This equipment cannot be diverted to any other use. It is not. It has to be set up for this. And it is spelled out in detail in the answers both at 177 and the prior testimony which Mr. Lehman and Mr. Mooney might like to glance at.

Mr. KASTENMEIER. Yes, we can do that. Mr. Drinan, do you have any further questions?

Mr. DRINAN. Just one last question. I assume that the FBI is going after the people who make these blue boxes and the black boxes. They have a little organization somewhere to make this sophisticated equipment. Now, there must be one or more organizations. I assume that the men in blue are looking for the men with the blue boxes.

Mr. CAMING. I think that is very well stated. I don't really think that they are to any degree primarily with respect to blue boxes as such.

Mr. DRINAN. Maybe black boxes.

Mr. CAMING. Or any other type of such equipment, primarily because the telephone company wanting to insure the integrity of our evidentiary gathering proceedings and to confine the overhearing only to evidence of toll fraud and not other crime has always independently gathered this minimal amount of evidence, and we present the whole package to them—so at that time the fraud section would in the Department of Justice or U.S. attorney's office be prepared to prosecute, or in a State level, say, county prosecutor, and will, like the U.S. attorney in Milwaukee, who is a good friend of mine.

Mr. DRINAN. Well, what I meant is, how many of these things are out there, and there must be one or more persons manufacturing them, and what is the Department of Justice doing about just killing the production?

Mr. CAMING. Well, as I say, we ourselves are about the only body that can really—except if you get it through an informant—get the initial indications of use.

Now, we have had several big cases, and we have enjoyed the cooperation of the Department of Justice. We've had several big cases recently, and they are all being prosecuted for fraud by wire, where we have had manufacturing—we had one up in Minnesota which covered about six States with manufacturing and distributing. We had one recently in Montana, which involved as variegated a group as manufacturers, distributors, a druggist, a housewife, two members of the military.

We have recently had one in Oregon and Arizona. In each case, these have been prosecuted with the full cooperation of the U.S. attorney, and the FBI, and in the Bremson case, for example, in Minnesota, there were multistate raids coordinated to make the arrests, but we did gather the evidence, and we are extremely concerned about the proliferation of people who seem to find this a very lucrative way to make money.

For example, you can make one of these for $50, and in the right circles, whether it's organized crime or unscrupulous businessmen, get, as I mentioned, $3,500, and they are getting it.

Mr. DRINAN. Well, one last point. It would seem to me that it is so sophisticated, it would be very easy to catch and apprehend and deter the manufacture thereof, though maybe that is another case where the Department of Justice is not doing too well these days.

Thank you very much.

Mr. KASTENMEIER. Thank you, Mr. Caming, for your appearance here today, and your colleagues, Mr. Connor and Mr. Mack, both of whom we did not have to much access to, but perhaps at a later date, there will be additional reasons to ask for your help; also to others who may be here this morning from A.T. & T., I want to express the subcommittee's appreciation. It has been very helpful indeed.

Mr. CAMING. It has been a pleasure.

Mr. KASTENMEIER. The Chair would like to announce that Mr. Wiggins was to have been here this morning, but because of the death of our colleague, and very close friend from California, Congressman Pettis, Mr. Wiggins is attending the funeral in California and could not be here, so until we reconvene at a later date on this subject, the subcommittee stands adjourned.

[Whereupon, at 12:50 p.m., the subcommittee was adjourned, subject to the call of the Chair.]

SURVEILLANCE

TUESDAY, MARCH 4, 1975

U.S. HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON COURTS, CIVIL LIBERTIES,
AND THE ADMINISTRATION OF JUSTICE
OF THE COMMITTEE ON THE JUDICIARY,
Washington, D.C.

The subcommittee met, pursuant to notice, at 10:10 a.m., in room 2141, Rayburn House Office Building, Hon. Robert W. Kastenmeier [chairman of the subcommittee] presiding.

Present: Representatives Kastenmeier, Danielson, Drinan, Pattison, Railsback, and Wiggins.

Also present: Bruce A. Lehman, counsel; Timothy A. Boggs, professional staff member; and Thomas E. Mooney, associate counsel.

Mr. Kastenmeier. This morning the subcommittee will conduct another in its series of hearings on surveillance legislation.

We will be hearing this morning from three distinguished Members of Congress who are cosponsors of various antisurveillance bills pending in the subcommittee. They are Hon. Edward Biester of Pennsylvania, Hon. Barry Goldwater, Jr., of California, and Hon. Parren Mitchell of Maryland.

All three are among the 71 House cosponsors of the Bill of Rights Procedures Act. The subcommittee heard testimony from the chief House and Senate sponsors of this bill, Congressman Charles Mosher and Senator Charles Mathias, at its first hearing on February 6.

The Bill of Rights Procedures Act prohibits interception of any communication by electronic or other device, surreptitious entry, mail opening, or the inspection and procuring of bank, telephone, credit, medical, business, or other private records without a court order based on probable cause that a crime has been or is about to be committed.

In addition, two of our witnesses today have cosponsored legislation to limit military surveillance of civilians, and Congressman Mitchell has also cosponsored a bill to prohibit wiretapping performed with the consent of one party to a conversation unless accompanied by a court order.

At this time it is a great personal pleasure for me to welcome as our first witness not only a former colleague on the Judiciary Committee, but a colleague who served on this very subcommittee, and whose service was very deeply appreciated by this chairman for I guess about 4 years.

The Chair greets Congressman Ed Biester of Pennsylvania. Congressman Biester.

any purpose other than mechanical and service quality control." *S. Rept.* No. 1097 at 93, 90th Cong. 2d Sess. (1968) (emphasis added).

Beckley was not a "blue box" or "black box" case. It involved a conspiracy to defraud the telephone company by an employee of the company and others. The court simply said, without citing any authortiy, that, "Section 605 does not prohibit the telephone company from monitoring its own lines." 259 F. Supp. at 571.

One author has interpreted Section 2511(2)(a) to mean that the monitoring must be random and it must be done to determine mechanical or service quality in the case of a communication common carrier. "No monitoring for criminal misuse as such would be acceptable under this provision." J. George, *Constitutional Limitations on Evidence in Criminal Cases* 158 (1973 ed.).

After diligent research no reported federal appellate court cases that interpret Section 2511(2)(a) could be found. Three federal district court cases involving this section have been reported. In *United States* v. *Deleeuw*, 368 F. Supp. 426 (E.D. Wisc. 1974), the telephone company connected a dialed number recorder to the defendant's telephone line. In addition, the company recorded a one minute conversation of the defendant whenever the mechanism was activated by a "blue box" frequency. The defendant was indicted for fraud, and on his motion to suppress the evidence the court held that ". . . the action taken by the . . . company in attaching a . . . detector to the defendant subscriber's line, which device recorded . . . the conversations had on such line in only those instances *where a blue box frequency was actually applied thereto*, constituted the type of nonrandom monitoring for the protection of property which is sanctioned by 18 U.S.C. § 2511(2)(a)(i)." 368 F. Supp. at 428 (emphasis added).

On the basis of an analysis of a computer printout it was suspected the defendant Shah may have been using a "blue box." The phone company monitored Shah's line and recorded the beginning portion of any conversation when the "blue box" was used. Shah was charged with violating the wire fraud statute, and on his motion to dismiss the court held that the phone company had done nothing that was not within the exception of 2511(2)(a). *United States* v. *Shah*, 371 F. Supp. 1170 (W.D. Pa. 1974).

In *United States* v. *Freeman*, 373 F. Supp. 50 (S.D. Ind. 1974), the phone company, after receiving information from another phone company, installed a tape-recorder on defendant's ex-wife's telephone line. The monitor recorded the use of a "blue box" on several occasions. The defendant made a motion to dismiss, but the court denied the motion. The trial judge said that the action taken by the phone company was "the type of non-random and non-service control monitoring for the protection of the utility's property which is contemplated by 18 U.S.C. § 2511(2)(a)(i), * * *" 373 F. Supp. at 52.

Obviously, none of these cases have sanctioned the widespread use of random monitoring by the phone company. Like the cases decided under Section 605, each of these recent cases involved the monitoring of a specific telephone line. The question as to whether the random monitoring as reported in the newspaper was in violation of Section 2511 remains unanswered.

Section 2511(2)(a)(i) specifically states that the telephone company shall not utilize . . . random monitoring except for mechanical or service quality control checks." It would seem that the random monitoring conducted by the company after the Omnibus Crime Control and Safe Streets Act took effect was within the proviso of Section 2511(2)(a)(i). The term random monitoring is not defined by the Act. Although the phone company has argued that "random monitoring" has a technical meaning, it is a general rule that a statute must be interpreted by is plain and common meaning. *See, Rathbun* v. *United States*, 355 U.S. 107, 109 (1957). As the Supreme Court has said, in speaking of Section 605, "distinctions designed to defeat the plain meaning of the statute will not be countenanced." *Benanti* v. *United States*, 355, U.S. 96, 100 (1957).

Even if the random monitoring is within the proviso of Section 2511(2)(a)(i) it would appear that no violation of that section has occurred. Section 2511 prohibits the willful interception of any wire or oral communication or the use of any device to intercept any oral communication. Section 2510(4) of Title 18 defines intercept to mean "the aural acquisition of the contents of any wire or oral communication through the use of any . . . device." The term device is defined so as to exclude any apparatus being used by a communications carrier in the ordinary course of its business. 18 U.S.C. § 2510(5). Only equipment being used by the carrier in the ordinary course of its business would be excluded. *S. Rept.* No. 1097, *supra*, at 90.

Arguably the random monitoring by the electronic scanner was not the aural acquisition of the contents of the

tion of the conversation. The words "aural acquisition" as used in 18 U.S.C. § 2510(4) mean to come into possession through the sense of hearing. *Smith* v. *Wunker*, 356 F. Supp. 44 (S.D. Ohio 1972). The mechanical monitoring of telephone conversations to detect the use of a "blue box" a "black box" would not be an "aural acquisition" of the conversation.

The tape recording of the conversations would be an interception, but such an interception would seem to be legal by the exception given the phone company in Section 2511(2)(a)(i). However, if the company recorded the entire conversation or if the company recorded more calls than were necessary to prove illegality, then the company may have exceeded the authority given to it by Section 2511. *See, Bubis* v. *United States, supra*. If the scanning and the recording is viewed as a one-stage process, then what the phone company did was the aural acquisition of the contents of a communication. This one-stage process would only be illegal if the device was not being used in the ordinary course of the company's business.

One other possible argument that the phone company's monitoring was illegal is that it violated the Fourth Amendment rights of the company's subscribers. Generally there is no invasion of the security afforded by the Fourth Amendment against unreasonable search and seizure when evidence is acquired illegally by private parties. *Burdeau* v. *McDowell*, 256 U.S. 465 (1921). The argument has been made, however, that when the searcher has a strong interest in obtaining convictions and has committed searches and seizures regularly then the Fourth Amendment should apply even though the search was not done by a government official. *Note*, 19 *Stanford L. Rev.* 608, 615 (1967). Thus, there is the basis for any argument, albeit a weak one, that the phone company violated the Fourth Amendment by recording telephone conversations in order to prosecute illegal users.

C. CONCLUSION

It is not certain that the telephone company violated any federal laws by the random monitoring of telephone conversations during the period from 1964 to 1970. This uncertainty exists because the Congressional intent in passing Section 2511(2)(a)(i) is not clear, and case law has not clearly explained the permissible scope of monitoring by the company. Under existing law it seems that the only way the telephone company can violate Section 2511 is if it randomly monitors telephone conversation with a device not used in the ordinary course of its business so as to aurally acquire the conversation. One obvious remedy would be for Congress to amend Section 2511 so as to make clear the extent of the monitoring to be allowed.

IRWIN MANDELKERN,
Legislative Attorney.

SPEECH BY ZANE E. BARNES, PRESIDENT, SOUTHWESTERN BELL TELEPHONE CO., DELIVERED TO THE KIWANIS CLUB OF SAN ANTONIO, TEX., ON DECEMBER, 19, 1974

TRUTH IS OUR DEFENSE

I want to thank the Kiwanis Club of San Antonio for allowing me to speak to you today. It is a real privilege to be here.

Just over 14 months ago, I spent one of the most enjoyable times of my life here in San Antonio.

It was during the week of October 16, 1973—my first week as an employee of Southwestern Bell.

I was the newly elected president of the company and had come to San Antonio for our Annual Conference of top management people.

I was delighted that such a beautiful and friendly city had been selected for our meetings.

I was enthusiastic about joining a company with a reputation as one of the very best in the telecommunications business.

I was greeted most cordially here and was honored to be the subject of some fine interviews with the San Antonio news media.

It was a genuinely pleasant experience.

If you will forgive me for the personal references, I find to my dismay a sharp contrast between that wonderful period and today. Just over a year later, everything seems to have changed.

Everything that yesterday was right seems today to be wrong.

Southwestern Bell in Texas seems to be operating under a cloud.

Employes of my company have been embarrassed and mistreated.

Almost every day new accusations come to the fore against my company.

I know—and I am confident many of you know—that there is not justification for any loss of confidence in Southwestern Bell.

Today, I want to show you that the charges leveled at us are false, that we still have fine employees, that we place our highest priorities on good service at reasonable rates. In other words, nothing really has changed.

Ma Bell has not turned into Ma Barker.

We take great pride in the job we do and the contribution we make—as a supplier of an essential service and as a responsible corporate citizen.

If we prize anything above all else, it is our integrity—and that integrity has been challenged in recent weeks in San Antonio and for that matter, throughout a great portion of Texas.

I submit that a company that has been a good citizen for over half a century will not become a blot on any community overnight. Chet Todd and his people have an outstanding record of good citizenship here in San Antonio. A recent example was the United Way Campaign in which the combined giving by Southwestern Bell and employees was $351,000 or $87.15 per employee. In addition to this, Chet did an outstanding job in heading up this year's U.S. Savings Bond drive. He is serving now in several leadership positions in the United Way, the Chamber of Commerce and others.

Our employees in San Antonio live up to the standards that the people of San Antonio set for themselves. Telephone people occupy the church pews on Sunday, they lead Scout troops, serve on school boards and committees, pay their bills and taxes and generally are models of respectability.

We are proud of our employees—and the damaging of their reputations is perhaps the greatest tragedy associated with this apparent campaign of vilification that is being waged against Southwestern Bell.

I am aware of cases where innocent Southwestern Bell employees have been publicly ridiculed, because they work for a company that has been falsely accused of wrongdoing.

I don't believe for a minute that this is typical of San Antonio, and I am not blaming the citizens of San Antonio. Their behavior is natural in the light of the controversies that have been stirred up.

One of my concerns is that the atmosphere in a community can affect the ability of people to perform at a high level. In our business, that is especially important.

In discussing what has happened here in an apparent effort to change Southwestern Bell's image, I will confine my remarks primarily to allegations that have been made publicly.

Our internal investigation actually got under way in our company because of reports received at general headquarters. We initiated this investigation without any urging, pressure or assistance from the outside to see if any house cleaning was needed.

During the investigation, our top executive in Texas died under circumstances which caused his death to be ruled a suicide.

Because a lawsuit has been brought against the company, I will not make any further comments here about that investigation. I am sure that all the facts will come out in the courtroom.

But there is something that concerns me now and should be of concern to every thinking person. Widespread attempts have been and are being made to bring into disrepute a number of our operations in Texas that have passed the test of time for effectiveness and for fairness to the public.

I would like to discuss three major charges made against us:

1. That we make excessive profits through maintaining two sets of books
2. That we engage in illegal wiretapping
3. That we make illegal political contributions

Nearly everyone has heard the charge that we maintain two sets of books—one for our own auditors and the other for rate making purposes.

The facts concerning this charge are these:

Our accounting records are maintained as prescribed by the Federal Communications Commission. All other materials—including those sometimes referred to as a so-called "second set of Books"—are simply derivatives of this one set of books.

Texas takes into account that inflation has decreased the value of the dollar, and thus, has increased the value of a piece of property in terms of current dollars.

Texas law states that utilities will be permitted to make a fair return on the fair value of their property. Texas is one of many so-called "Fair Value" states.

The use of fair value is not a matter of convenience, but a matter of compliance with the law.

The other principal approach to rate making is called "Net Book," which means the original cost of plant less the depreciation. Net book alone has no legal status in Texas, as far as rate making is concerned.

In addition, the net book approach can be badly misleading since, by its very nature, net book requires a much higher rate of return to achieve the same financial effect as the fair value approach.

You may have heard reports of a so-called secret memorandum by a Southwestern Bell rate expert in St. Louis. Boiled down to simple terms, this memorandum says just what I said: original cost requires a higher rate of return than fair value.

City officials are not fooled by the phony charges concerning our rate negotiations. The financial director of the City of Fort Worth was quoted in the Fort Worth Star-Telegram as saying that statements circulated about our rate making procedures are a "fabrication," and those about the St. Louis memorandum are a "complete misrepresentation of the intent of the document."

The problem for utilities and regulators alike is determining fair value. Most people would say that the value of property is what it is worth today. Unfortunately, this is rather difficult to establish in the case of utility properties which are seldom sold. Texas courts have ruled that the rate base should be a reasonable balance between what it would cost to replace the plant and equipment at today's prices (less an adjustment for deterioration) and the net book value.

The word reasonable causes the problem. Actually, there are about as many approaches to fair value as there are utility companies and "rate experts."

Recent public statements imply that the fact that rates of return can be computed in different ways was a secret withheld from the public. The average citizen, I submit, does not know the details of utility rate making any more than he knows the formulas by which professional men set their fees or retailers figure the markups that they must have. On the other hand, ratemakers and regulators have long known of Southwestern Bell's approach to rate making. So there is no secret about it.

We look at earnings several different ways, because we know that those who review our data for the cities will do the same. We furnish net book data as well as fair value information to city staffs so they can look at our proposed rates in any way they wish. Establishing the proper rate base and setting rates are judgment matters which are decided upon by honest and capable city officials.

Representatives of the cities can, and do, review our detailed records which are maintained for Texas in Dallas. These data, incidentally are examined by the Internal Revenue Service, Federal Communications Commission and outside accounting firms as well as our own internal auditors.

Finally, Southwestern Bell asks to be judged on performance—not unsubstantiated allegations made in the press and in lawsuits.

We are furnishing unsurpassed service at local rates that year-by-year are a smaller part of the average family's budget. If we thought only of maximizing our short term profits and had taken the irresponsible approach to rate making as alleged by some, we could have asked for many more rate increases than we have over the past decades.

Anything as complicated as rate making can be twisted and can be distorted to make it seem the company is trying to milk the citizens of their money. It sounds very sinister when someone says that Southwestern Bell uses a special set of "Blue Books" in presenting its rate cases to city official in Texas.

This audience is going to have the rare privilege of seeing one of these mysterious "Blue Books." Here is one of them.

These books show our investinent, revenues, expenses and rate of return for a particular exchange—in this case, San Antonio.

Some years ago, this information was presented just as sheets of typewritten material. Then, one day, one of our people wanted to get a little bit showy, I guess, so he put a blue cover on the sheets. Ever since, they have been called "Blue Books."

All right. After all these explanations, how is the Texas rate payer really faring at the hands of Southwestern Bell?

Several comparisons can give us that answer—straight and clear—with no gimmicks.

First, Texas local rates compare favorably with those in other states. Some cities have higher rates, some lower. Texas cities are certainly not the leaders.

A number of cities have higher residential rates than San Antonio, Dallas and Fort Worth—cities such as Cincinnati, Seattle, Columbus, Phoenix, Birmingham and others.

In Houston, the largest city in Texas, residential rates are lower than in several cities with similar numbers of telephones—Boston, Cleveland, Atlanta and Miami.

Furthermore, Houston rates are lower than those in cities with much smaller calling scopes, such as New Orleans, Indianapolis and Buffalo.

A second comparison involves Texas earnings, which have been erroneously described as the highest in the United States.

Here is a fact: Texas currently ranks 16th among the 48 states served by the Bell System in rate of return on net plant.

Texas ranks fifth among the six states presently served by Southwestern Bell.

There is a third comparison that points to the reasonableness of our rates in Texas. Between 1967 and September, 1974, the Consumer Price Index in this country increased 52 per cent. During the same period, residential telephone service increased in cost an average of only 22 per cent.

These are nationwide figures.

Comparable detailed figures are not available for all the major cities in Texas, but Consumer Price Index increases in Texas are in about the same range as national increases and so are the increases in Texas residential telephone rates.

Let me make a point, though, about two-party service, which we offer primarily for low income families or customers needing service for emergencies. Cost of this service increased only about 5 per cent during this period.

Somewhat related to the way we set our rates is the way we pay our property taxes. I can say without fear of contradiction that we pay our fair share of property taxes—on the same basis as other businesses and other taxpayers.

We believe the taxes we pay are at or above the average for businesses in Texas.

Recently, charges have been made that we show a high property value for rate purposes and a low property value for tax purposes.

One reason for this apparent discrepancy is—as I explained earlier—that Texas law specifies a rate base made up of a blending of original cost and reproduction cost.

Valuation for tax purposes is made on the basis of original cost, with consideration given to improvements, depreciation and obsolescence and general market value.

We make studies of sales and transfers of property and other indicators to help determine what our fair share of the tax burden should be.

There is another reason it is not easy to make comparisons between tax and rate bases. Our property records for rate purposes may or may not cover exactly the same geographic areas as the taxing jurisdiction. For the most part, they do not match.

Much significance has been attache dto a reassessment and an increase in the property taxes on our Houston holdings.

This charge has been presented as if we were caught cheating on our Houston taxes.

Such is not the case. Our 1974 city and school property tax bill in Houston was some $2 million higher than 1973. Here are the reasons:

Our investment increased.

The tax rate increased.

And, our property was reappraised as part of a 4-year reappraisal program.

I repeat. We have only one objective with regard to our property taxes: We want to pay our fair share. That isn't Page One news, but it is the truth.

To move on to another subject, Southwestern Bell has been accused of illegal wiretapping.

I submit that this allegation is preposterous. There is no more relentless opponent of wiretapping than the Bell System.

We strongly oppose any invasion of the privacy of communications by wiretapping and accordingly welcome Federal and State legislation which would strengthen such privacy.

We strive to provide telephone service that is as useful and pleasing as possible. Any wiretapping—or even false rumors of wiretapping—detract from the customer's ability to use his telephone without fear that his conversation will not be private.

Distorted statements about alleged wiretapping seem to have started a wave of near-hysteria in some parts of Texas.

Let me assure you that we have taken ample precautions to assure the privacy of communication our customers want and they deserve.

Our company regulations against violation of the customer's right to privacy are drilled into our employees beginning with their first day on the job.

We have a booklet containing our code of ethics and our code of conduct. Employees are required to read this booklet and sign it. Anyone caught violating the secrecy portion of this statement is subject to dismissal, and under the provisions of the Communications Act, is subject to a fine and jail sentence.

What, then, is all the fuss about?

Let me retrace some of the events.

Under existing statutes, federal law enforcement officials investigating certain specified major crimes may wiretap only under federal court or Presidential order.

These orders may require Southwestern Bell to furnish information and facilities to a properly authorized law enforcement agency making wiretap connections.

THE TELEPHONE COMPANY DOES NOT PLACE ANY WIRETAPS

Accusations about Southwestern Bell's wiretapping have been made by an employee we dismissed. These were followed by further unfair and untrue charges made by people with questionable motives who for one reason or another apparently wanted to undermine confidence in our company and the service we provide.

For example, a San Antonio police official, who has never revealed his name, was quoted by the Associated Press on November 16 as saying that "Federal, state and city law enforcement officers, working hand in glove with Southwestern Bell Telephone Company, have conducted illegal wiretaps on an almost routine basis for years."

If this man has any information about illegal wiretaps, he should come forward with it so that it can be dealt with and properly investigated.

The police chiefs in a number of our largest cities, including San Antonio, have said they have authorized no wiretaps.

Very recently, we have heard allegations that Southwestern Bell has a piece of equipment—called a "mini-frame"—which can be used to monitor calls illegally.

I am not sure what is meant by the term "mini-frame." However, we do have special equipment used only in connection with suspected electronic long distance fraud and obscene and harassing calls and only as authorized under both the Communications Act and the Omnibus Crime Control and Safe Streets Act.

Two years ago, we used this equipment to apprehend a ring of manufacturers and users of illegal devices called "Blue Boxes" which are used to make fraudulent long distance calls at the expense of the telephone company and its customers.

A few years ago we undertook to stop the upsurge in obscene and threatening telephone calls. Our electronic equipment played a major part in bringing this activity under control. As I said earlier, this equipment was used only as authorized under the law.

Our security people are responsible and they are ethical and they are the ones who use this equipment.

Our security force is not a large one but it has been very effective in investigating coin telephone robberies, various kinds of long distance fraud and obscene and threatening telephone calls. We have 44 investigative people in Southwestern Bell and about 20 in the state of Texas.

The losses we sustain through coin telephone larceny and long distance fraud are substantial. They are a business expense which ultimately become part of the price the customer pays for his service. So our security forces perform a real service for the customer by holding down these kinds of losses.

The third major charge against Southwestern Bell is that it makes contributions of corporate funds to political candidates and maintains a fund of company money for political contributions.

I believe some accounts have alleged that employees make contributions and recover the money through expense vouchers. This is clearly and directly contrary to company policy and anyone doing it would have to reimburse the company and be subject to discipline.

As a good corporate citizen, however, Southwestern Bell does encourage its top management employees to make personal contributions to candidates for political office.

We expect our management people to take the lead in local activities that will improve the community.

Our management people are paid salaries that are competitive with salaries for similar job responsibilities in comparable industries. We conduct periodic salary surveys in our territory to update our salary information.

We think the management salaries we pay should enable our people to assume responsible roles in the communities they live in. I certainly hope our people do participate with their time and their money in church, charities, civic clubs—and politics.

It's up to the individual to decide what his or her involvement will be and it is by no means a condition of employment.

And in supporting political candidates, I would expect their decisions as to whom to support would be as varied as the whole field of aspirants.

The charge that we try to influence government officials with these contributions is ridiculous. Reporters combed the records to find contributions by Southwestern Bell people and came up with the startling news that some of our executives had contributed such sums as $25, $50 and $100.

One reporter commented to some of our people that we wouldn't influence a dog catcher with these contributions.

I want to stress that no authorized corporate funds are involved in contributions by our management people. However, the way these contributions reach the candidates has been under suspicion in some quarters.

Many personal contributions are made directly to the candidates.

Because they are active in the community and interested in encouraging good candidates, our management people talk together about such matters and it is natural they should do so.

They also consult our public affairs people for background on such things as candidates' positions on issues.

Occasionally, our public affairs people are contacted by candidates in need of financial support. Some of our executives respond to these requests by sending a personal check to the candidate.

I see nothing wrong with this—either ethically or legally. In fact, I would suggest that it is only through support of this kind that our uniquely American form of political process will survive. For all the buffeting it has taken recently, our system is far superior to any other I know about, and I am not ashamed to stand here and say so—even if it sounds a bit of old-fashioned.

What disturbs me, however, is that irresponsible charges such as those leveled against Southwestern Bell may very well dry up these legitimate sources of contributions for political candidates.

In summary, we have been accused of maintaining two sets of books, of illegal wiretapping and of making illegal political contributions.

It would be unrealistic for me to stand here and tell you we have never done anything wrong. But the fact that we have dismissed a management employee for misconduct provides evidence that we will seek out and discipline wrongdoers.

What I can tell you is what our policies are:

We do not maintain two sets of books.

We do not engage in or condone illegal wiretapping.

We do not authorize or condone illegal political contributions.

When we find that an employee has violated one of our policies we discipline that person.

I have talked long, but there was much to be said.

Truly, I do want to return to the kind of atmosphere I experienced in my first visit here. I pledge to you that I will do everything in my power to prove—by our actions—that Southwestern Bell deserves the kind of confidence we once had here.

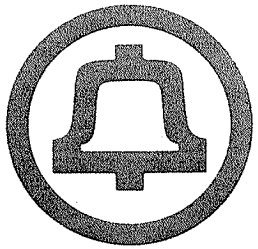
One bad apple—or a few, if that many are found—does not ruin the whole barrel. One man fired for misconduct should not reflect on the other 40,000 employees in Texas who have had exemplary conduct.

I am completely confident that the spirit of service that has been the trademark of Southwestern Bell employees is still intact, while it may be temporarily obscured by the reaction of some segments of the community to the false charges that have been made.

I am equally confident of the ultimate fairness of our customers, who, after all, are the final arbiters as to right and wrong. I am sure they will vindicate us in the end.

Thank you.

SECRECY OF COMMUNICATIONS AND PROTECTION OF COMPANY PROPERTY, RECORDS AND SERVICES



C&P Telephone

May, 1972

TO ALL EMPLOYEES:

OUR COMPANY'S GOOD REPUTATION has been built on the integrity of its employees, as well as their competence and efficiency. This good reputation is fundamental to the well-being of the business and to its future growth and progress. In an era when we are so often called upon to adapt to rapid change in our work together, this is one aspect of our jobs that never changes.

Every employee has a personal responsibility to maintain the Company's good name. We expect from each other the highest degree of honesty and integrity, and we require that our business be conducted in that manner. I'm sure you want it that way, too.

This booklet covers some of the rules, principles, and laws we must live by in maintaining secrecy of communications, in safeguarding Company property and funds, in preparing and handling Company records, and in carrying out certain related responsibilities. I ask and expect you to read this booklet carefully and to follow the rules and principles in any way they may apply to your job. It is your responsibility to know its contents. Violations can lead to disciplinary action, including dismissal, and also to arrest and conviction under Federal and State laws.

Naturally, no booklet can cover all the laws, detailed rules and practices, and specific Company policies that relate to honesty and integrity as they apply to every aspect of every job in the Company. The basic principle is personal integrity. This must be our standard in everything we do.

President

SECRECY OF COMMUNICATIONS

Maintaining the secrecy of communications is a fundamental policy and an absolute requirement of the Company. A telephone or teletypewriter connection between customers, or such a connection involving any other equipment is for the exclusive and confidential use of the parties to the connection. Should the contents or nature of any communication come to the attention of an employee, this information must not be divulged by the employee to anyone else except to a supervisor in those instances where it is absolutely necessary for handling emergencies, for preventing illegal use of service, or for other similar situations.

Federal law makes it a criminal offense to violate the secrecy of communications. An offense is severely punishable by fine or imprisonment, or both.

Some examples of your obligations to assure secrecy of communications, on or off the job, are:

You must not listen in to any call or any portion of a call between customers 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 there has been a call from one telephone, teletypewriter, or other station to another is not to be divulged except to properly authorized persons.**
- **You must never use any information regarding any communication for your own benefit or for the benefit of any other person not entitled to it.**
- **You must never permit any person, other than the parties to the communication, to hear, record or otherwise intercept any communication, except as required for proper handling of the call.**
- **You must not disclose information regarding the location of any equipment, including trunks, circuits or cables, or regarding records of calls, except to other employees as required in the operation of the business.**

- **You must not permit anyone to tamper with communication facilities of the Company or to have unauthorized access to Company premises.**

- **You must not discuss any communication arrangements provided for our customers except as required in the operation of the business or as specifically authorized by the customer.**

Such rules are, of course, not intended to prevent access to information and communications by Company employees whose duties require it or by law enforcement officials acting with proper authorization. An employee may, however, at some time be approached by someone who is not an authorized employee desiring access to our equipment or to information about communications or wishing to hear, record or otherwise intercept, or learn about a communication. Under no circumstances should you undertake to comply with any such request. This rule applies even if the request comes from someone claiming to exercise authority, such as a police officer or other government representative. You, as an individual, should not take the responsibility of complying with that request. Any such request must be referred immediately to your Staff Supervisor—Security through normal lines of organization. It is the responsibility of the Staff Supervisor—Security to obtain a decision, with the advice of the Company's Legal Department, as to what action shall be taken.

- **For example, a police officer might show you a court order authorizing interception of a particular telephone line, and he might ask you for information regarding that line. You should tell the officer that the proper person to handle the request is the Staff Supervisor—Security and you should tell him how to get in touch with him, but you should not give any other information. You should also immediately report any such request to your Staff Supervisor—Security through normal lines of organization.**

SAFEGUARDING COMPANY INFORMATION

Our records, plans and other data contain information of value to outside firms and individuals. This includes unlisted telephone numbers, nonpublished numbers, the daily information addendum, toll tickets, details of the physical telephone network, and information of or about cable pairs, terminals, line assignments, credit records, billing, payrolls, personnel records, correspondence and other similar data. Information of this type must not be used for any purpose other than in the conduct of Company business, even after it becomes obsolete for current Company use.

- **Treat all such information confidentially. Do not discuss it except with authorized Company employees. Do not use it except as authorized by the Company.**

* * *

SABOTAGE AND ESPIONAGE

Continuous vigilance is necessary to prevent the disclosure of Company information which could be of value to espionage agents or saboteurs. Such information includes security procedures, circuit layout information, emergency rerouting and restoration data and all classified defense information.

- **You must not divulge any such information to any unauthorized person. Report any attempt to obtain such information by unauthorized or suspected persons to your supervisor.**

The Federal Criminal Code specifically provides punishment for injuring, destroying, or interfering with communications facilities and for various acts of obtaining or communicating information about telecommunications, facilities related to national de-

fense, to be used to the injury of the United States or to the advantage of any foreign nation.

Access to classified defense information involving national security will be granted to employees who are properly cleared, but only on a "need-to-know" basis.

- **You must not discuss classified defense information with or in the presence or hearing of any person not authorized to have knowledge of it.**

Employees who either willfully or negligently fail to safeguard classified defense information are liable to severe penalties under the Espionage Act. Even the disclosure of certain unclassified technical information to foreign nationals, including disclosure by means of visual access to Company facilities, is regulated by law and prohibited by Company policy.

- **You must obtain approval through lines of authority from the Staff Supervisor—Security before disclosing any technical information to foreign nationals or before permitting them to view Company facilities.**

* * *

HANDLING COMPANY FUNDS

Any employee who handles or has access to Company money—whether it be coin telephone deposits, overflow coins from coin boxes, payments, cash advances, or funds in any other form—is expected to know and follow Company procedures and instructions in each case.

Toll or message tickets, AMA tapes, service orders, or similar material are sources of revenue. They are the same as money. Removing, destroying, or otherwise misappropriating them, or failing to prepare required tickets, service orders or similar records is as serious as misappropriating funds or property.

Employees who are required to make adjustments on bills, spend Company funds, or incur personal expenses that will be reimbursed by the

Company, have the responsibility to use good judgment on the Company's behalf and to see that the Company gets value received for the money expended.

- **You must not use Company advance funds for any purpose except in the conduct of the Company's business, and you must protect such funds at all times.**
- **When money is owed to the Company, as in refunds for transportation, you must take action to insure that remuneration is made to the Company.**

Certification as to the correctness of vouchers and bills never should be made without knowledge that the expenditures and amounts were made and have been listed correctly. Vouchers and bills should be approved by supervisors only when they are reasonably certain that the expenditures have been incurred and after determining that the amounts were appropriate to the circumstances.

* * *

SAFEGUARDING AND USING COMPANY PROPERTY AND FACILITIES

Each employee is responsible for all Company property entrusted to him. Even if it is not specifically entrusted to him, each employee has the responsibility to be alert to its possible theft or misuse.

- **Return all tools, supplies, or equipment to the proper supply area, truck, or desk when not in use. Store them in such a manner that they are protected against loss, damage, destruction, and theft.**
- **If you drive a Company vehicle, lock it and its material compartments every time you leave it in a public place.**
- **Be sure that only authorized persons have access to Company property and that unattended Company buildings or storage areas are locked before you leave.**
- **You must always advise your supervisor promptly**

of any theft or misuse of Company property or records, and also notify him promptly of any situations that come to your attention where you suspect possible theft or misuse.

All equipment, tools, materials, and supplies purchased with Company funds are Company property and must not be taken for the personal benefit of an employee. Employees shall not use Company property for personal purposes unless authorized. Telephone equipment must not be installed, rearranged, or removed unless it is covered by an authorized order, or is followed up immediately by a report of a change in the order or by a request that an order be issued. This rule also applies to equipment installed in connection with telephone service for employees.

- **Without specific authorization, you may not take, sell, lend, or give away Company property, regardless of its condition. Neither do you have the right to receive or give away service or use equipment or facilities without authorization.**

It is the Company's policy that service which is to be used for illegal purposes will not be furnished. Equipment which is used for illegal purposes will be removed.

- **If service appears to be used for illegal purposes, report it to your supervisor immediately.**

Coin telephone keys, both to coinbox compartments and to upper housing units, require most careful protection. They are not to be used to gain access to coin telephones except for legitimate business under an authorized collection order, either written or verbal, or for carrying out authorized maintenance or service order work.

- **If you have an upper housing key, you must protect it and use it in strict accordance with the receipt you signed upon receiving it.**

Unauthorized use of local and long distance service is not permitted. Employee discount telephone service privileges apply only to normal and authorized usage by the employee and his immediate family. Official telephones and other Company communications facilities may be used for personal purposes only as specifically authorized and, in no

case, may such usage be permitted to interfere in any way with the conduct of Company business.

- **Use only those office telephones as designated by your supervisor to make authorized personal calls from Company premises. It is strictly forbidden to make personal calls at any time from any other equipment provided for the business—such as testboards, switchboards, terminals, or similar equipment.**

* * *

PREPARING AND HANDLING COMPANY RECORDS

Accurate, reliable records of many kinds are necessary to meet our legal and financial obligations and to manage the affairs of the business.

Vouchers, bills, time reports, payroll and service records, equipment and supplies records, work measurements, performance data, and all other reports and necessary information must be factual and accurate. No excuse will be accepted for a deliberately false or misleading report or record. Willful falsification of data entered on any report, record or memorandum constitutes an act of dishonesty and also may be a violation of the Federal and State laws.

- **Be sure to account for time, materials, tools, vehicles, Company funds, expenses, and any other Company property in accordance with prescribed practices.**
- **Toll tickets, AMA tapes, and service orders are as important as money. You must always prepare such records of service when required, and you must never destroy or withdraw them except when properly authorized.**

Our accounts are maintained in accordance with the Uniform System of Accounts prescribed for telephone companies by the Federal Communications Commission. The rules contained in the Uniform System of Accounts must be followed.

- **If your work involves using accounting classifications and procedures, you must follow correct procedures. If in doubt, ask your supervisor.**

The FCC and other governmental agencies also require that many of our records and documents be

retained for specific periods of time. Such records are not to be destroyed or discarded except in accordance with instructions or with proper authorization.

* * *

CONFLICT OF INTEREST

Our Company buys many goods and services from others. A large number of C&P employees are involved in the selection of suppliers or in purchasing goods and services. Our policy is to award business solely on the basis of merit, without favoritism and, wherever practicable, on a competitive basis.

This policy requires that employees must have no relationship or engage in any activities that might impair their independence of judgment. They and their families must have no personal financial interest in suppliers of property, goods or services that might affect their decisions or actions. Employees must not accept gifts, benefits or unusual hospitality that might tend in any way to influence them in carrying out their responsibilities.

- **You must not accept, either directly or indirectly, tips or any other form of gratuity for services rendered as a telephone employee.**

Our Company interconnects its communications services and facilities with those owned and maintained by others. In many cases, these services are directly competitive with those provided by C&P. Any employee who is employed by or performs services for a competitor violates his duty of loyalty to C&P and is involved in a conflict of interest.

- **You must not engage in any activities which promote or assist in the design, sale, repair, construction or installation of communications equipment or systems competitive with services provided by C&P Telephone.**
- **If there is ever any question as to the possibility of a conflict of interest, you must disclose the facts to your supervisor who will determine whether a conflict exists and, if so, what course of action should be taken.**

EMPLOYEE BOND

Every employee is covered by a Bell System Fidelity Bond. While this bond protects the Company against losses of money or property due to fraud or dishonest acts, it does not free the employee from liability to the Company for any such losses, from Company discipline, and from punishment under the law for any dishonest act, including willful falsification of any Company record or report. An employee's bond coverage is automatically canceled upon discovery by the Company of a dishonest act committed by the employee either on or off the job. Cases of dishonesty must be reported to the bonding company even though no loss is involved or no claim is made.

* * *

REPRESENTING THE COMPANY TO THE PUBLIC

The public knows the Telephone Company through its employees. People reason, and rightly so, that a company is no better than the people who work for it. No matter where you find yourself—in a business office, in a manhole, at a switchboard—to customers, friends, neighbors and outside business acquaintances, you are the Telephone Company. The responsibility rests with all of us always to conduct ourselves with highest integrity. Nothing less is acceptable.

- **Never enter a customer's premises without authorization. Be prepared and willing to show your Company identification if there is the slightest indication that the customer has any doubt as to who you are.**
- **When you enter a customer's premises, you have a responsibility to respect his property and to do no harm or damage to it.**
- **Be sure that your personal conduct on customers' premises is beyond reproach.**
- **Be sure that your telephone contacts are always courteous and respectful.**

TO SUM UP . . .

Personal integrity is basic to the performance of our job.

- **You must always maintain the secrecy of communications and safeguard Company records, property, information and services.**
- **You must always behave with complete honesty in dealing with the Company's property, records, funds, and services and in your relationships with other employees, customers, and the general public.**
- **You must always act in strict observance of Company regulations in such matters, as well as Federal and State laws that apply to our business.**
- **Don't be influenced by a mistaken belief that deviations from Company policy are all right because they appear to be to the advantage of the Company.**
- **You should always keep in mind that violations of the rules and regulations referred to in this booklet can lead to disciplinary action, including dismissal, as well as to possible arrest and conviction.**

* * *

If you have any questions about any part of this booklet, please discuss them with your supervisor.

EXCERPTS FROM FEDERAL LAWS

Secrecy of Communications

47 U.S. Code § 605. Unauthorized Publication or Use of Communications.

Except as authorized by chapter 119, title 18, United States Code, no person receiving, assisting in receiving, 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, (1) to any person other than the addressee, his agent, or attorney, (2) to a person employed or authorized to forward such communication to its destination, (3) to proper accounting or distributing officers of the various communicating centers over which the communication may be passed, (4) to the master of a ship under whom he is serving, (5) in response to a subpena issued by a court of competent jurisdiction, or (6) on demand of other lawful authority. No person not being authorized by the sender shall intercept any radio communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person. No person not being entitled thereto shall receive or assist in receiving any interstate or foreign communication by radio and use such communication (or any information therein contained) for his own benefit or for the benefit of another not entitled thereto. No person having received any intercepted radio communication or having become acquainted with the contents, substance, purport, effect, or meaning of such communication (or any part thereof) knowing that such communication was intercepted, shall divulge or publish the existence, contents, substance, purport, effect, or meaning of such communication (or any part thereof) or use such communication (or any information therein contained) for his own benefit or for the benefit of another not entitled thereto. This section shall not apply to the receiving, divulging, publishing, or utilizing the contents of any radio communication which is broadcast or transmitted by amateurs or others for the use of the general public, or which relates to ships in distress.

47 U.S. Code § 501. General Penalty.

Any person who willfully and knowingly does or causes or suffers to be done any act, matter, or thing, in this chapter prohibited or declared to be unlawful, or who willfully and knowingly omits or fails to do any act, matter, or thing in this chapter 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 chapter, by a fine of not more than $10,000 or by imprisonment for a term not exceeding one 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 chapter punishable under this section, shall be punished by a fine of not more than $10,000 or by imprisonment for a term not exceeding two years, or both.

Sabotage

18 U.S. Code § 1362. Communication Lines, Stations or Systems.

Whoever willfully or maliciously injures or destroys any of the works, property, or material of any radio, telegraph, telephone or cable, line, station, or system, or other means of communication, operated or controlled by the United States, or used or intended to be used for military or civil defense functions of the United States, whether constructed or in process of construction, or willfully or maliciously interferes in any way with the working or use of any such line, or system, or willfully or maliciously obstructs, hinders, or delays the transmission of any communication over any such line, or system, shall be fined not more than $10,000 or imprisoned not more than ten years, or both.

In the case of any works, property, or material, not operated or controlled by the United States, this section shall not apply to any lawful strike activity, or other lawful concerted activities for the purposes of collective bargaining or other mutual aid and protection which do not injure or destroy any line or system used or intended to be used for the military or civil defense functions of the United States.

* * *

Espionage

18 U.S. Code § 793. Gathering, Transmitting, or Losing Defense Information.

(a) Whoever, for the purpose of obtaining information respecting the national defense with intent or reason to believe that the information is to be used to the injury of the United States, or to the advantage of any foreign nation, goes upon, enters, flies over, or otherwise obtains information concerning any vessel, aircraft, work of defense, navy yard, naval station, submarine base, fueling station, fort, battery, torpedo station, dockyard, canal, railroad, arsenal, camp, factory, mine, telegraph, telephone, wireless, or signal station, building, office, research laboratory or station or other place connected with the national defense owned or constructed, or in progress of construction by the United States or under the control of the United States, or of any of its officers, departments, or agencies, or within the exclusive jurisdiction of the United States, or any place in which any vessel, aircraft, arms, munitions, or other materials or instruments for use in time of war are being made, prepared, repaired, stored, or are the subject of research or development, under any contract or agreement with the United States, or any department or agency thereof, or with any person on behalf of the United States, or otherwise on behalf of the United States, or any prohibited place so designated by the President by proclamation in time of war or in case of national emergency in which anything for the use of the Army, Navy, or Air Force is being prepared or constructed or stored, information as to which prohibited place the President has determined would be prejudicial to the national defense; or

(b) Whoever, for the purpose aforesaid, and with like intent or reason to believe, copies, takes, makes, or obtains, or attempts to copy, take, make, or obtain, any sketch,

photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, document, writing, or note of anything connected with the national defense; or

(c) Whoever for the purpose aforesaid, receives or obtains or agrees or attempts to receive or obtain from any person, or from any source whatever, any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note, of anything connected with the national defense, knowing or having reason to believe, at the time he receives or obtains, or agrees or attempts to receive or obtain it, that it has been or will be obtained, taken, made, or disposed of by any person contrary to the provisions of this chapter; or

(d) Whoever, lawfully having possession of, access to, control over, or being entrusted with any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted or attempts to communicate, deliver, transmit or cause to be communicated, delivered or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it on demand to the officer or employee of the United States entitled to receive it; or

(e) Whoever having unauthorized possession of, access to, or control over any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it; or

(f) Whoever, being entrusted with or having lawful possession or control of any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, note, or information, relating to the national defense, (1) through gross negligence permits the same to be removed from its proper place of custody or delivered to anyone in violation of this trust, or to be lost, stolen, abstracted, or destroyed, or (2) having knowledge that the same has been illegally removed from its proper place of custody or delivered to anyone in violation of his trust, or lost, or stolen, abstracted, or destroyed, and fails to make prompt report of such loss, theft, abstraction, or destruction to his superior officer—

Shall be fined not more than $10,000 or imprisoned not more than ten years, or both.

(g) If two or more persons conspire to violate any of the foregoing provisions of this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be subject to the punishment provided for the offense which is the object of such conspiracy.

18 U.S. Code § 798. Disclosure of Classified Information.

(a) Whoever knowingly and willfully communicates, furnishes, transmits, or otherwise makes available to an unauthorized person, or publishes, or uses in any manner prejudicial to the safety or interest of the United States or for the benefit of any foreign government to the detriment of the United States any classified information—

(1) concerning the nature, preparation, or use of any code, cipher, or cryptographic system of the United States or any foreign government; or

(2) concerning the design, construction, use, maintenance, or repair of any device, apparatus, or appliance used or prepared or planned for use by the United States or any foreign government for cryptographic or communication intelligence purposes; or

(3) concerning the communication intelligence activities of the United States or any foreign government; or

(4) obtained by the processes of communication intelligence from the communications of any foreign government, knowing the same to have been obtained by such processes—

Shall be fined not more than $10,000 or imprisoned not more than ten years, or both.

(b) As used in subsection (a) of this section—

The term "classified information" means information which, at the time of a violation of this section, is, for reasons of national security, specifically designated by a United States Government Agency for limited or restricted dissemination or distribution;

The terms "code," "cipher," and "cryptographic system" include in their meanings, in addition to their usual meanings, any method of secret writing and any mechanical or electrical device or method used for the purpose of disguising or concealing the contents, significance, or meanings of communications;

The term "foreign government" includes in its meaning any person or persons acting or purporting to act for or on behalf of any faction, party, department, agency, bureau, or military force of or within a foreign country, or for or on behalf of any government or any person or persons purporting to act as a government within a foreign country, whether or not such government is recognized by the United States;

The term "communication intelligence" means all procedures and methods used in the interception of communications and the obtaining of information from such communications by other than the intended recipients;

The term "unauthorized person" means any person who, or agency which, is not authorized to receive information of the categories set forth in subsection (a) of this section, by the President, or by the head of a department or agency of the United States Government which is expressly designated by the President to engage in communication intelligence activities for the United States.

(c) Nothing in this section shall prohibit the furnishing, upon lawful demand, of information to any regularly constituted committee of the Senate or House of Representatives of the United States of America, or joint committee thereof.

NEWS MEDIA ACCOUNTS OF ALLEGED MONITORING PRACTICES OF AMERICAN TELEPHONE AND TELEGRAPH COMPANY

[From the St. Louis Post-Dispatch, Feb. 21, 1975]

BELL SECRETLY MONITORED MILLIONS OF TOLL CALLS

(By Louis J. Rose)

The Bell Telehone System monitored in random fashion millions of long-distance calls originating in six cities, including St. Louis, and secretly tape-recorded parts of at least 1,500,000 calls for analysis in New York.

The Post-Dispatch has learned that the highly secretive program was designed to help combat electronic toll call frauds, but only a tiny fraction of the calls listened to and recorded were ever confirmed by the company as being fraudulent.

Other cities besides St. Louis where calls were monitored were New York, Detroit, Miami, Los Angeles and Newark, N.J.

The monitoring program covered a six-year period and ended in the spring of 1970, when those Bell executives involved were warned to purge their files of any reference to the program and to destroy any materials relating to it.

A source with knowledge of the internal operations of the Bell system said that Bell executives who ran the monitoring program believed the company was within its legal rights, but were afraid Bell's image might be damaged if word leaked to the public.

"From the beginning they analyzed this very carefully," the source told the Post-Dispatch, "and decided that if it ever were necessary to reveal the existence of this equipment in order to prosecute a toll fraud case, they would simply decline to prosecute."

A good percentage of the tape recordings involved segments of from 30 seconds to 90 seconds from the time a call was first dialed, but in several hundred thousand instances entire conversations were recorded.

The monitoring equipment frequently misread calls as having indications of electronic toll fraud. Certain frequency components in human speech, for example, could have caused the equipment to be activated as if fraud were involved,with the result that the entire conversation might be taped, it was said.

The program was unknown to many high-ranking Bell executives even in areas where it was in effect.

More than 30,000,000 long-distance calls were monitored during the first four years of the program by sophisticated equipment that scanned trunk-line calls. The equipment looked for electronic indications that an attempt was being made to bypass the system's toll charge mechanism.

Of the more than 1,500,000 long-distance calls that were at least partly recorded during the first four years of the program, with the tapes being sent to New York for anaysis, fewer than 25,000 were considered by those doing the analysis to be indicative of fraud.

Fewer than 500 of the calls in this category during the first four years were confirmed as fraudulent.

Initially, the program went into effect in late 1964 with six units, each capable of monitoring 100 trunk lines. Each unit could handle about five calls at any given moment. The program began with two units each in New York and Los Angeles and single units in Miami and Detroit.

Early in 1967, the Detroit unit was transferred to St. Louis. It was installed here at the Southwestern Bell facility at 2651 Olive Street, remaining there until the spring of 1970. It was about then that the entire program was ended.

Several factors, including fear of public exposure, figures in the decision to end the program. Other factors, included concern over the condition of the monitoring units and whether the whole approach was efficient and comprehensive enough.

Joseph F. Doherty, who is now director of corporate security at the New York headquarters of American Telephone & Telegraph Co., played an important role in the program and was among those involved in the orders that files relating to it should be purged and destroyed.

Doherty, when asked for comment, suggested that a reporter channel his questions through public relations personnel at Southwestern Bell Telephone Co. here, one of 22 AT&T companies.

Later Friday, William Mullane, press relations director for AT&T confirmed most of the details known to the Post-Dispatch. Mullane said the program largely was an experimental or trial project and was ended May 1, 1970.

He said he did not know how many calls had been tape recorded, but said he believed the recordings ran between 60 and 90 seconds. The Bell system continues to crack down on electronic toll fraud, but its present approach does not involve voice recordings, he said.

The monitoring unit used during the old program were designed by Bell Laboratories to detect electronic toll cheaters, particularly those persons who utilized "blue box" and "black box" equipment.

(A blue box is a device intended to allow the user to place long-distance calls that dodge the Bell system's billing equipment. A black box is a device that enables persons to call the box's owner long distances without paying for the call.)

The monitoring units worked this way:

Once the unit locked onto a call, it would record on a temporary recorder the initial phase of each call. If it found nothing indicating electronic fraud, the temporary recording was erased and the equipment prepared to handle a new call.

But if the initial phase appeared to indicate, for example, that a blue box was being used, the equipment activated a master tape recorder that would record a segment or the entire content of the call. The master tape subsequently was snt to New York for analysis.

Mullane said that elaborate precautions were taken to assure that the tapes were studied only by a small group of trained security personnel in New York. "They could not be listened to locally," he said.

He conceded the program had been kept highly secretive.

"The fewer people that know anything you are doing to detect fraud, the better off you are," he commented.

[From the Washington Post, Jan. 15, 1975]

Telephone Police Wire In

No Limit to Taps They Make

Houston (AP)—They don't wear guns or badges and they can't make arrests, but the Bell Telephone Co. security force is one of the most powerful private police groups in the country.

Federal law allows Bell Telephone to conduct wiretaps for its own use under certain conditions. There is no limit to the number of taps provided the conditions are met. The company does not have to go through a court to run such taps nor report them to any government agency.

The Bell security organization conducts such taps in the 85 per cent of the nation where Bell is "the only phone company in town." The law permits Bell, or companies like it, to monitor any telephone conversation on lines where they have reason to believe telephone fraud against the company may be taking place.

This legal eavesdropping in the Bell System is done by the small, tightly organized group of 665 security agents. They control when, where and how it is done. At least 76 members of that force are former FBI agents.

A spokesman for American Telephone and Telegraph Co., parent company of the Bell system, said that company policy dictates that such wiretaps are only used to investigate cases of "electronic tool" fraud. The spokesman said this means use of a "little blue box" mechanical device to make free phone calls.

The spokesman, attorney H. W. William Caming, in charge of legal matters involving industrial security for AT&T, said in rare cases the wiretap law is used to investigate other kinds of fraud against the company.

The Bell security group is the key link for law enforcement agencies which want to establish a legal wiretap of their own. Under Bell company policy, the security agents verify all court orders which permit law enforcement officers to wiretap. Bell officials here said the security agents are usually the only ones who verify court orders.

Caming said in New York that company policy requires the agent to run the order through the phone company's legal department for verification. Caming said in rare cases the agent might skip the legal department procedure, but does so at the risk of his job.

Misuse of this system is prevented, according to one agent, only by "my integrity and the integrity of those with whom I work." Strength of that integrity is currently being questioned on two fronts.

A federal grand jury here is conducting an investigation into illegal wiretapping by police officers. Houston Police Chief Carrol M. Lynn says that "sophisticated wiretaps" have been used with the aid and support of Bell Telephone Co. employees.

Bell has denied the charges. Five telephone company agents have testified before the grand jury.

In San Antonio, a former Bell executive, James H. Ashley, and the family of a deceased phone official, T. O. Gravitt, have filed a $29.2 million lawsuit against Bell. Among the charges they make are that the company used illegal wiretaps.

The Gravitt family also claims that an investigation by the security force hounded Gravitt to his death.

Gravitt, who was a vice president in charge of the Bell system in Texas, died of carbon monoxide poisoning in the garage of his Dallas home in October. He left behind a suicide note and some memoranda charging misconduct by Bell in ratesetting, slush funding and influence-buying.

And Ashley has charged that the Bell security force serves an important role in these activities.

Houston, the largest city in the Southwestern Bell Telephone Co. area, has a security force typical of those throughout the Bell system.

Jerry Slaughter, a sharp, precise, clean-cut man who usually wears dark, conservative suits, is chief of Bell security here. He operates out of a sparsely decorated office atop the 12-story Bell building here. On his office wall is an autographed photo of J. Edgar Hoover, the late FBI director. Slaughter served five years with the FBI. Two of the five agents under him are also FBI veterans.

Former "bureau men" are prominent throughout the Southwestern Bell system. Of 44 security agents in the company, 15 are former FBI agents.

Down the hall from Slaughter's office, in a room not much bigger than a closet, is the major investigative tool of the security force.

The small room is equipped with devices for monitoring conversations on selected telephone lines. Agents can call a switching station and be plugged into any Houston telephone. Officials here described the procedure as a relatively simple one, but Caming of AT&T said it was an elaborate one which takes some time.

The equipment can record on paper tape the numbers called from the selected line. With the addition of a tape recorder, the instrument can also record conversations. And it's all legal.

"There's nothing clandestine about this," said Jim Russell, a security agent who gave a tour of the room to reporters after Bell officials earlier denied the room's existence.

According to James W. Shatto, a Bell attorney, the product of this monitoring is carefully guarded and surrendered to the FBI only by subpoena. This, says Shatto, is company policy.

Yet, one attorney said that "several scores" of persons have been tried and convicted on information Bell agents voluntarily surrendered to the FBI.

Several cases cited in federal court records show individuals were convicted of gambling, possession of weapons and other charges unrelated to fraud as the result of information from phone company wiretap volunteered by company security agents.

In Houston, Michael Clegg, a 32-year-old man from Marble Falls, Tex., was convicted last March of defrauding the phone company after his line was tapped by Bell agents for four months.

As a result of the Clegg wiretap, taps were established at several other towns around the country. In Memphis, for example, a listening post on the phone of one suspect was set up in the garage of a neighbor who happened to be a Bell employee.

After several months, the FBI arrested men in four cities in what one attorney called "a nationwide, coordinated bust."

The attorney said the FBI was given details gleaned from company wiretaps. The notes even included, in one case, names of stocks and bonds a suspect discussed on his phone.

Another attorney said that the Bell security force and law enforcement agencies have a very close "sweetheart" relationship in other areas.

Bell, for example, hires about 70 Houston policemen who work as security guards at telephone company buildings during off hours.

Additionally, eight Bell officials in Texas, including Slaughter and his counterparts in Dallas and San Antonio, hold special Texas Ranger commissions. By law, this gives them virtually the same powers as regular police, including the right to carry guns. In practice, the special ranger appointments are mostly honorary.

This close relationship has advantages for both Bell and for police.

It provides for Bell an avenue to get information that would not be available otherwise.

For the police, the relationship helps cut through red tape in establishing wiretaps which are legal with a court order. The Bell security force is the gate keeper for setting up these legal taps.

Slaughter, in an interview, said the mechanics of a government wiretap go like this: the police bring a court order to Slaughter. He, and usually he alone, judges the validity of the order. Then he calls a supervisor in the telephone exchange involved and gets the needed information to pinpoint the wiretap location. Exchange office supervisors, said Slaughter, give him the information essential to establish a wiretap solely upon his word that court order exists.

The supervisors, said Slaughter, never see the order. There is no system for double-checking.

The primary purpose of the security force, said Slaughter, is to catch persons defrauding the telephone company, by one means or another, through making unpaid long-distance calls. Such frauds in Houston, said Slaughter, costs Bell "in the neighborhood of $100,000 a year," a figure considerably lower than the salary paid the Bell security officers.

RADIO TV REPORTS, INC.,
Washington, D.C., February 4, 1975.

For: National Broadcasting Co.
Program: "The Today Show."

AN INTERVIEW WITH THE SPECIAL COUNSEL FOR A.T. & T.

JIM HARTZ. Over the weekend, the American Telephone & Telegraph Company, A.T. & T., admitted monitoring and recording millions of long distance telephone calls between 1965 and 1970 to catch people cheating on toll charges. The calls originated in six major cities—New York, Los Angeles, Detroit. St. Louis, Miami, and Newark, New Jersey. A.T. & T. said it had been plagued by people trying to make free long distance calls by using a device called the blue box to bypass the phone company's billing system. A spokesman justified the practice of monitoring the calls by referring to telephone calls as "our property."

With us this morning is Mr. H. W. William Caming (?), an attorney who has been with A.T. & T. for twenty years as special counsel in security matters.

First, Mr. Caming, could you tell us what that means, that A.T. & T. owns the calls?

H. W. WILLIAM CAMING. Good morning, Mr. Hartz.

HARTZ. Good morning.

CAMING. I think what was meant by that was that it is our property in the sense that telephone calls are the property of the people of our country, and losses that are incurred are incurred by our honest customers. And if there is thievery, stealing of calls, the losses must ultimately be borne by the honest rate payer.

HARTZ. Uh-huh.

CAMING. And I think that was the sense in which we speak of our property as we speak of our country.

HARTZ. Well, the spokesman wasn't misquoted. He did say that the calls were. . . .

CAMING. Yes.

HARTZ. . . . the telephone company's only [sic] property—is that correct?—and that we have a right to intercept them.

CAMING. That is. . . .

HARTZ. Is that a correct quote?

CAMING. That is correct, as far as I understand it. But knowing the gentleman quite well, I knew the context in which he meant it.

HARTZ. How did you decide which telephone calls to monitor?

CAMING. I think, Jim, if we look at the situation in perspective, starting in 1964 and 1965, we may get an insight into what required the institution of this project. In about 1964 or so, two electronic toll fraud devices burst upon the scene, the so-called blue box and the so-called black box, named after the original boxes in which they were contained.

The threat to the telephone industry as a whole from such devices was of staggering proportions. We were able to readily estimate that if unchecked, free calls could be made, that is if our service could be stolen at will, that the losses would aggregate in the hundreds of millions of dollars, which would directly affect our rates.

HARTZ. What were the actual losses? Do you know?

CAMING. The actual losses were difficult to ascertain because of clandestine nature. It was well in excess, at the inception, in our estimation, of a million dollars a year. But this was only the start.

To give one of the statistics we were able to obtain—and one of the major purposes of instituting this project was to determine the magnitude of the theft, because it would possibly require the expenditure of more than a billion dollars to modify the network unless this type of theft could be checked.

HARTZ. How many—how many did you catch?

CAMING. Well, we have, I believe, had over two hundred and fifty convictions, many of major proportions.

HARTZ. And how many telephone calls were monitored?

CAMING. There again . . .

[Confusion of voices.]

HARTZ. . . . said thirty million. . . .

CAMING. Yes. Well. . . .

HARTZ. Is that correct?

CAMING. No. The telephone calls that were recorded for analysis were in the neighborhood of a million five plus. What happened, if I may for a moment just give you some background and to advert to an earlier question, we had estimated in 1966 that there were over three hundred and fifty thousand cases of toll fraud of this nature, many involving innumerable calls. Therefore, some device to measure the extent of the fraud to determine whether the telephone system had to be modified and to attempt to find means of prosecuting those who were stealing had to be introduced. And we introduced, through Bell Laboratories, six experimental units in the cities that you named. These units were scanning devices which scanned calls at random. We put each unit on a hundred trunks.

Now, each trunk has a stream of calls flowing through it. And we would dip into the stream, you might say, and pull out a fish and examine it to see whether it was a lawful call. And if so, it was immediately put back in the stream.

HARTZ. How could you tell whether it was lawful or illegal?

CAMING. In our system, particularly since we're talking only of outgoing long distance calls, there are special signals—answering signals, supervisory signals—that permit us to know whether a call is completed. the duration of the call for billing and transmission purposes. So that the equipment was electronic equipment designed to identify the call.

HARTZ. Then why did you have to record the conversation?

CAMING. One of the necessities was to attempt to determine, if it was a preliminary indication of an illegal call, where the call was coming from or where it was going. A black box, I might say, is the device which is used at the receiving end. For example, if you were a well-known gambler and I wanted to place a bet from Tennessee with you, I would call you in New York. You would activate your device, and therefore my bet would be placed without any telephone charge to me.

HARTZ. When you recorded these conversations—and you say that there were at least a million five surveyed one way or another—did you put that little beep on the wire to let people know they were being recorded?

CAMING. No. The million five or so were recorded and placed on a recorder. And I might say that this recording was not done by human ear listening. And these were done in very safely guarded, locked cabinets, and automatically done. And . . . .

HARTZ. Don't your tolls require you to put that beep on there, your tariffs?

CAMING. No, they do not when the call is illegally placed. And we had—it would be like . . . .

HARTZ. But you were monitoring some calls that weren't illegally placed, were you not?

CAMING. No. None of the calls, Jim, at the time in question appeared lawful to the equipment. There were preliminary indications of illegality.

HARTZ. I'm out of time. We've got to stop for a station break. Mr. Caming, thank you very much.

CAMING. You're quite welcome.

APPENDIX 17

IMMUNITIES, RIGHTS, AND PRIVILEGES ACCORDED FOREIGN GOVERNMENTS AND THEIR REPRESENTATIVES IN THE UNITED STATES

(Prepared by the Office of the Chief of Protocol, Department of State, May 1970)

This memorandum gives a detailed account of some of the more important immunities, rights, privileges, and exemptions accorded foreign governments and foreign diplomatic and consular personnel in the United States. It is not intended to be an exhaustive treatment of the subject, and further information may be obtained by writing or telephoning the Office of the Chief of Protocol of the Department of State.

I. Immunity From Judicial Process; Offenses Against Foreign Diplomatic and Consular Offices, Officers, and Property

The following pertinent statutory provisions of the United States Code, 1964 Edition, are quoted verbatim:

§ 252, Title 22. *Suits against ministers and their domestics prohibited.*—Whenever any writ or process is sued out or prosecuted by any person in any court of the United States, or of a State, or by any judge or justice, whereby the person of any ambassador or public minister of any foreign prince or State, authorized and received as such by the President, or any domestic or domestic servant of any such minister, is arrested or imprisoned, or his goods or chattels are distrained, seized, or attached, such writ or process shall be deemed void.

§ 253, Title 22. *Penalty for wrongful suit.*—Whenever any writ or process is sued out in violation of section 252 of this title, every person by whom the same is obtained or prosecuted, whether as party or as attorney or solicitor, and every officer concerned in executing it, shall be deemed a violator of the laws of nations and a disturber of the public repose, and shall be imprisoned for not more than three years, and fined at the discretion of the court. (R.S. § 4064.)

§ 254, Title 22. *Exceptions as to suits against servants, etc., of minister; listing servants.*—Sections 252 and 253 of this title shall not apply to any case where the person against whom the process is issued is a citizen or inhabitant of the United States in the service of an ambassador or a public minister and the process is founded upon a debt contracted before he entered upon such service; nor shall section 253 of this title apply to any case where the person against whom the process is issued is a domestic servant of an ambassador or a public minister, unless the name of the servant has, before the issuing thereof, been registered in the Department of State and transmitted by the Secretary of State to the marshal of the District of Columbia, who shall upon receipt thereof post the same in some public place in his office. All persons shall have resort to the list of names so posted in the marshal's office and may take copies without fee. (R.S. §§ 4065, 4066.)

§ 112, Title 18. *Assaulting certain foreign diplomatic and other official personnel.*—Whoever assaults, strikes, wounds, imprisons, or offers violence to the person of a head of foreign state or foreign government, foreign minister, ambassador or other public minister, in violation of the law of nations, shall be fined not more than $5,000, or imprisoned not more than three years, or both.

Whoever, in the commission of any such acts, uses a deadly or dangerous weapon, shall be fined not more than $10,000, or imprisoned not more than ten years, or both. (June 25, 1948, Ch. 645, 62 Stat. 688; Aug. 27, 1964, Pub. L. 88–493, § 1, 78 Stat, 610.)

These provisions of statutes drawn from the District of Columbia Code, 1967, Edition, are also pertinent:

§ 22–1115. *Interference with foreign diplomatic and consular offices, officers, and property.*—It shall be unlawful to display any flag, banner, placard, or device designed or adapted to intimidate, coerce, or bring into public odium any foreign government, party, or organization, or any officer or officers thereof, or to bring into public disrepute political, social, or economic acts, views or purposes of any foreign government, party, or organization, or to intimidate, coerce, harass, or bring into public disrepute any officer or officers or diplomatic or consular representatives of any foreign government, or to interfere with the free and safe pursuit of the duties of any diplomatic or consular representatives of any foreign government, within five hundred feet of any building or premises within or its representative or representatives as an embassy, legation, consulate, or for other official purposes, except by, and in accordance with a permit issued by the superintendent of police of the said District; or to congregate within five hundred feet of any such building or premises, and refuse to disperse after having been ordered so to do by the police authorities of the said District. (Feb. 15, 1938. 52 Stat. 30, ch. 29, § 1.)

§ 22–1116. *Penalties for interference with foreign diplomatic and consular offices, officers, and property.*—The District of Columbia Court of General Sessions shall have jurisdiction of offenses committed in violation of section 22–1115, and any person convicted by a fine not exceeding $100 or by imprisonment not exceeding sixty days, or both: *Provided, however*, That nothing contained in said section shall be construed to prohibit picketing, as a result of bona fide labor disputes regarding the alteration, repair, or construction of either buildings or premises occupied, for business purposes, wholly or in part, by representatives of foreign governments. (Feb. 15, 1938, 52 Stat. 30, ch. 29, § 2; Apr. 1, 1942, 56 Stat. 190, ch. 207, § 1; July 8, 1963, 77 Stat. 77, Pub. L. 88–60, § 1.)

* * * * * * *

Members of households of administrative and technical staffs of diplomatic missions enjoy immunity in accordance with the provisions of Article 37 of the Vienna Convention on Diplomatic Relations.

II. Exemption From Customs Duties and Taxes Imposed Upon or by Reason of Imporation of Merchandise

The United States customs regulations provide for the extension of customs courtesies and free entry privileges to diplomatic and consular personnel of foreign countries and for the free entry of official government shipments and outline the procedure to be followed in requesting such courtesies and privileges. The pertinent portions of these regulations are set forth below:

DIPLOMATIO AND CONSULAR OFFICERS

10.29 Baggage

(a) Upon application to the Department of State and appropriate instructions from the Treausry Department in each instance, the privilege of admission free of duty without entry shall be extended to the baggage and effects of the following representatives of foreign governments and their families, suits, and servants, provided the governments which they represent grant reciprocal privileges to American officials of like grade accredited thereto or en route to or from other countries to which accredited.

(1) Ambassadors, ministers, and chargés d'affaires; secretaries, counselors and naval, military, and other attachés of embassies and legations; high commissioners, consular officers, and trade representatives; all the foregoing who are accredited to this Government or are en route to or from other countries to which accredited; and

(2) Other high officials of foreign governments and such distinguished foreign visitors as may be designated by the Department of State.

(b) In the absence of special authorization therefor from the Department prior to the arrival of representatives of foreign governments enumerated in paragraph (a)(1) of this section, the privilege may be extended to their baggage and effects upon presentation of their credentials or other proof of their identity.

(c) Foreign ambassadors, ministers, chargés d'affaires; secretaries, counselors, and naval, military and other attachés of foreign embassies and legations shall not be detained or inconvenienced, and their baggage and effects shall remain inviolate. Every proper means shall be afforded them to facilitate their passage through ports of the United States.

* * * * * * *