Who's Listening?

How NSA Tunes In on Americans' Overseas Phone Calls and Messages

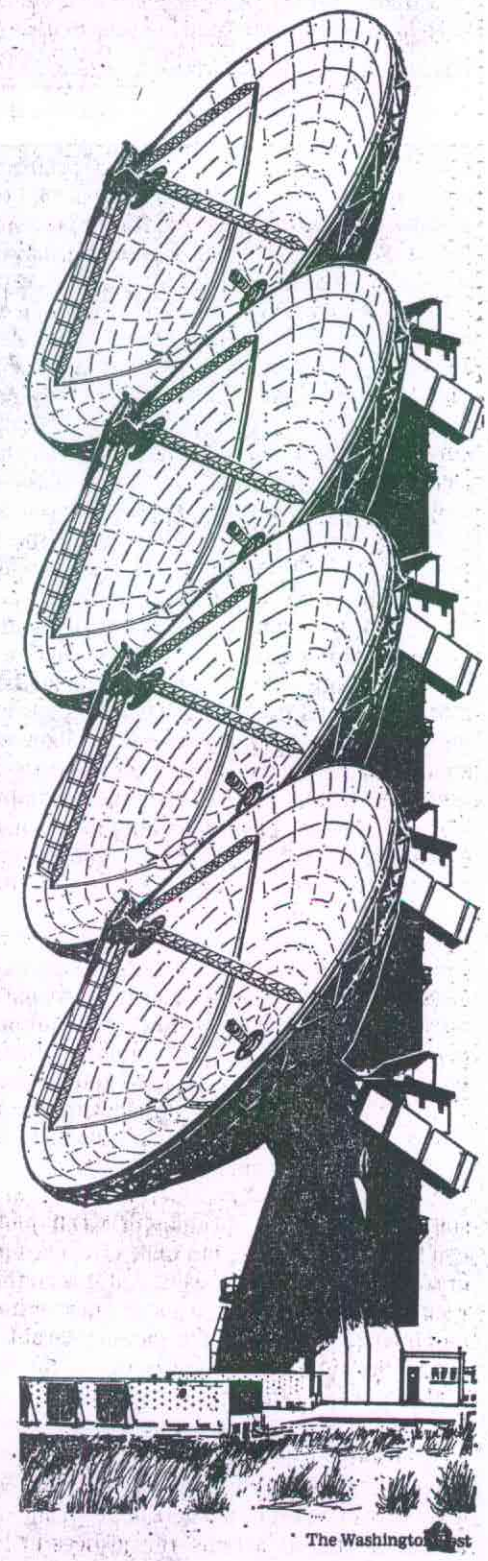
By Deborah Shapley

THE LITTLE-KNOWN but long-standing practice by the National Security Agency of scooping up the international telegrams, telex messages and some international phone calls of American citizens, keeping some of them and forwarding some for use by other government agencies, is coming under scrutiny on Capitol Hill as Congress tries to enact the first major updated wiretap law since 1968. NSA's capability for sweeping up hundreds of thousands of simultaneous communications is so vast that, in the words of one expert, it is "ripping open" legal protections of the privacy of American citizens.

Sen. Birch Bayh (D-Ind.), chairman of a Senate select intelligence subcommittee on the rights of Americans, calls the alleged NSA practice "intrusive, covert foreign intelligence surveillance that requires further safeguards to protect American citizens and domestic organizations." And Mark Lynch, an American Civil Liberties Union lawyer specializing in wiretap law, says: "NSA's alleged dragnet seizure of people's conversations and messages couldn't be more at odds with the Fourth Amendment, the historical origin of which was to prevent general searches and warrants."

The "dragnet seizure" of messages appears to be a much larger operation than that ascribed to the Soviets in recent press reports. According to these accounts, the Soviets are bugging domestic American communications from some Soviet-owned properties in Washington, San Francisco and other U.S. cities. The reports have not revealed what other bugging the Soviets may do, but the NSA operation involves sweeping up entire streams of overseas messages into receivers at several strategic points, many of them abroad.

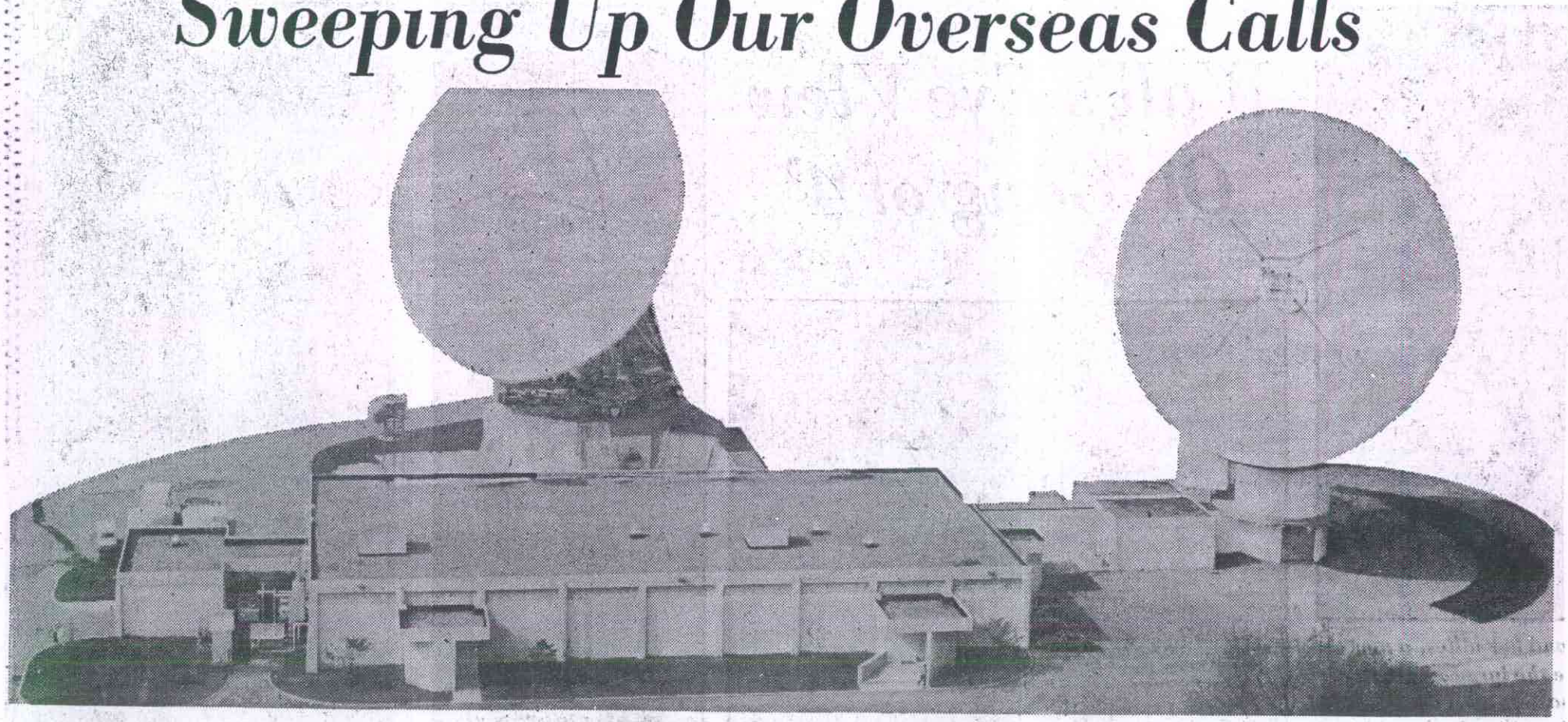
See NSA, Page C4



The Washington Post

Shapley is a reporter for Science magazine, from which this article is reprinted.

Sweeping Up Our Overseas Calls



Trans-Atlantic communications transmitted and received by satellite relay stations like this one in Etam, W.Va., are monitored by NSA facilities.

NSA, From Page C1

The NSA's collecting of messages of American citizens is attracting concern these days on Capitol Hill, and to a lesser extent within the administration, as both try to draw up new laws and charters governing intelligence activies in the wake of an investigation of past abuses by a Senate committee headed by Frank Church (D-Idaho) in 1975-1976. During that investigation, NSA gave its first public testimony, which alluded in a veiled way to its incidental gathering of the communications of American citizens.

Giant Vacuum Cleaner

VIRTUALLY ALL of the NSA's operations are classified. The following account of how the NSA collection program operates was pieced together by Science magazine from interviews with about two dozen people. About half of these sources have had knowledge of the NSA operation, but because of the secrecy barrier, they would discuss it only in general terms. Science also interviewed a number of experts, who, because of their technical knowledge, could advise on how the collection, storage and dissemination program must operate.

It is public knowledge that NSA devotes itself mostly to decoding the secret communications of foreign governments, and encoding important U.S. government communications. The supersecret agency also spends lots of time and money listening to military communications of potential U.S. enemies and worrying about activities of enemy submarines, tanks, radar and the like.

According to knowledgeable sources, about one-tenth of NSA's estimated $1.5 billion yearly budget, or some $150 million, goes for what he called "communications intelligence," or in the lingo of the trade, COMINT. COMINT, however, is what most people would call eavesdropping. One source estimates that half of NSA's COMINT budget goes for an advanced technology effort which, like a giant vacuum cleaner, can sweep up every communication traveling by satellite or microwave ground transmission between the United States and foreign countries. Even undersea cable traffic is vulnerable, apparently, after the cable comes ashore.

Some of this eavesdropping is for obvious national security reasons, such as listening to communications between foreign embassies located in the United States and their home governments. Or the NSA might seek the calls and telegrams of a known spy in Tokyo to learn who his contacts are in the United States. The Tokyo spy or the designated foreign embassy would be, in NSA jargon, "targets" of the surveillance.

But with modern telecommunications, these "target" messages travel not singly over individually tappable wires like those that connect the ordinary telephone, but as part of entire message streams, which can contain up to 970 individual message circuits, and have voice, telegram, telex and high-speed data bunched together. The modern eavesdropper must record all the messages in the stream, and later sort through this enormous haystack of signals to ferret out the "target" ones he seeks.

The Carter administration's new director of NSA, B. R. Inman, has stated recently: "There are no U.S. citizens now targeted by NSA in the United States or abroad. None." But this assertion says nothing about how many messages of U.S. citizens the NSA sweeps up incidentally and then keeps in its files. Certainly the volume NSA could choose from is huge: In 1976, exclusive of leased line traffic, 13.6 million telegrams were sent between the United States and points overseas, as well as 52.3 million telex messages and 74 million telephone calls lasting 10.9 million hours. No source could be found who would estimate the volume of all this that winds up in NSA files, or that is forwarded to other agencies.

Automatic Sorting

THREE TECHNOLOGIES have brought about the era of mass-scale "dragnet" eavesdropping. First is the capability for putting more and more messages onto a single stream and for automatically sorting them out at the receiving end. A second element has been the growth in computer storage capacity during the 1960s. The third development has been the accompanying ability to retrieve, with great precision, selected information from the growing files.

All three technologies continue to develop; communications research promises future mini-revolutions in packaging thousands of messages in a single stream — for instance, a hollow 2-inch-wide cable that would carry 280,000 separate messages. And, of course micro-miniaturization is swelling the storage capability of computerized data banks.

Telegram and telex messages are in written form initially, and so can be easily reprocessed into digital form for radio transmission. NSA or some other eavesdropper can simply set up its own receiver and decode these streams of messages back into written language for computer scanning and filing. Because of the ease with which this can be done, sources say, NSA for years has made a practice of collecting this traffic and sorting it out only after it has been stored in the computers. "They take all that stuff and dump it into their computers. It would be totally impractical to sort it out before it enters the files," says one source.

Telephone conversations, however, cannot be monitored as easily and automatically. Experts agree that spoken language, with its continuously variable sounds, is now decipherable as coherent language only by the human ear. IBM researchers say no one can get their machines to take naturally occurring continuous speech and accurately

transcribe it to written language. Thus, sources assume the NSA must use people — probably military recruits from the Army Security Agency and the Naval Security Group — to listen to recorded conversations, decide which are "of intelligence interest" and make transcripts of them for the files.

The problem of computerized speech recognition, which received a lot of Defense Department support in the early 1970s, has proved enormously difficult to solve. At IBM, researchers use the company's most advanced commercial machine, the 370/168, and an artifically quiet room, to recognize and transcribe artificially constructed spoken language.

Raj Reddy, a professor of computer science at Carnegie-Mellon University, says he works with a fairly sophisticated computer that can recognize 1,000 acoustically distinct words. Reddy is convinced that NSA can't do much better, either, at the moment. He adds, however, "I have no doubt that the technology will be available in 15 to 25 years for NSA to monitor phone conversations on a mass scale."

Reddy and others have speculated, however, that the NSA might use other speech recognition devices to sift through masses of recorded telephone conversations and select out ones in which key words appear.

Reddy cautions, however, that such recognition devices could be foiled. "You can speak with a Chinese accent. Or you can cough or whistle in the middle of a key word, and the machine will miss the word and the entire conversation. Or if you know the machine is searching for 'assassination,' you could plant large numbers of conversations containing the words 'a fascination.' "

The extent of NSA's listening to international telephone traffic is not known, but one knowledgeable source said that NSA is "disillusioned" with searching through ordinary telephone traffic because "people assume the phones are bugged and when they have something important to communicate, they don't say it over the phone."

The source went on to offer a glimpse of the bizarre mental logic of the professional eavesdropper: "But NSA doesn't want it known that they're giving up listening to phone calls because they think it will encourage people to say important things that the NSA then won't be able to pick up." According to this reasoning, then, the NSA is actually afraid that people might use the international phone system for their private communications.

Search and Retrieval

GIANT COMPUTERIZED files, accessible by key words, are widely said to be the other main element of NSA's vacuum cleaner operation.

Large data banks are currently in commercial use; law firms, for example, have automated files that, in minutes, can scan all federal court decisions for the last quarter-century. One source says of these systems, "You should assume that NSA is light years ahead of what is found in the commercial marketplace."

In fact, without discussing computers as such, NSA director Gen. Lew Allen Jr. testified in 1975 that these search and retrieval methods are used. "The use of lists of words, including individual names, subjects, locations, etc., has long been one of the methods used to sort out information of foreign intelligence interest value from that which is not of interest," Allen said.

Several sources confirmed that NSA continues to forward some number of telegrams, telex messages and transcripts of telephone communications — sometimes with proper names deleted — to other agencies when so requested. The requests can be for vague economic information, such as Soviet grain prices or Arab petrodollar flow, as well as for information obviously concerned with national security.

Sometimes, apparently, NSA has resisted attempts by other people in the executive branch to invade the privacy of U.S. citizens or corporations. In one case, a cabinet-level official in the Nixon administration is reported to have demanded that NSA identify an American corporation whose name had been blotted out from a cable he was reading. NSA refused. Angered, the cabinet officer appealed to the director of central intelligence, who has oversight of the NSA, to hand over the name anyway, but the director of central intelligence also refused. One NSA critic warns: "This was a case in which NSA looked good. But given another director of NSA, or a differently inclined director of central intelligence, the outcome might have been different."

IBM's Richard Garwin, in a paper on technology and intelligence, has proposed several ingenious technical means for making large data banks less vulnerable to abuse. Among other measures, Garwin suggested that the computer be programmed to keep "an indelible record of who has queried the file and what questions were asked, so the failures of access limitations will not go undetected."

Besides all this recording, storage and retrieval capability, the modern eavesdropper has at his disposal today's international communications network, which offers many tempting points at which he can intercept thousands of messages at a time.

Communications system experts agree that interception of the undersea cables that carry about half of the U.S.-overseas traffic would be difficult and expensive. But once out of the water, the cable messages are often transferred to microwave towers, which repeat them and send them along to other towers. "All you need would be a receiving station, placed correctly on high ground between towers, to pick up the entire transmission traveling along that route."

Satellite-transmitted messages also offer many possible intercept locations. Ground stations, such as that located at Etam, W.Va., have large antennas capable of directing the signals to the satellite with great accuracy. However, the antennas on the satellite are smaller, and they direct the signals back to earth with less precision; they can fall over an area perhaps thousands of miles square.

Thus, while much of the U.S.-to-Britain traffic is received in England at a station at Goonhilly Downs, Cornwall, which is operated by the British Post Office, the signals could also be picked up in their entirety by another receiving station on a ship offshore, or by a landbased receiver in England or Northern Europe.

Officials of the major communications companies admitted that such interceptions could take place without their knowledge. The executive vice president of Western Union International, Thomas Greenish, asked whether he knew of any recording by the NSA of international telegram traffic, said, "I have no knowledge of it. I doubt it. But it could be happening."

Secret Guidelines

THE TECHNOLOGY by which NSA allegedly "scoops up" the international communications to and from the United States has raised a number of controversial legal questions. Some of these may come to a head during discussion of the new wiretap bill before Congress later this fall.

The only restraint on NSA's current retention and forwarding of the massive amount of data in its files are secret executive branch guidelines, promulgated by former Attorney General Edward H. Levi in 1976. Officials with knowledge of the secret guidelines refused to discuss them, even in general terms. However, several officials said they are "very rigorous" and "carefully enforced."

But the secret nature of the guidelines, as well as the fact that they exist at the whim of the Attorney General, has provoked calls for other rules governing NSA eavesdropping, laid down by the courts or the Congress. The proposed wiretap law, which was drafted by the Carter administration (although NSA fought it in administration circles), requires a court-ordered warrant before any Americans in the United States can become "targets" of intelligence community surveillance. At that time, a judge would also approve procedures for minimizing the collection, retention and dissemination of unwanted messages. But Sen. Bayh is among the members of Congress who think that the "minimization" procedures in the current proposed bill have too many loopholes and could allow NSA's alleged "covert, intrusive surveillance" of Americans to continue.

Both the wiretap bill and executive guidelines may let NSA keep the telegrams, telex messages and other communications buried in their computers. In this sense, they are poor guards against later possible official abuse.

The feasibility of NSA's sorting of such quantities of material is also questioned. "Suppose they said they would not forward any communication to or from an American citizen," says one critic of the system. "Does that mean they run every message against a list of more than 220 million names before pulling it from the files?"

The ACLU's Lynch argues that NSA's dragnet search itself — a result of modern communications technology — may be illegal, since it may violate the Fourth Amendment's ban on general searches. He says, "If there's absolutely no way that NSA can target the messages for which it may have national security cause to collect without the dragnet, then other restraints must serve. But the NSA has to prove that — the burden is on them. And they haven't because they won't talk about their technology.

"But under no circumstances should they be allowed to maintain the stuff they've picked up in their dragnet after they've used their key words, or whatever, to select out the stuff they had cause to seize," Lynch adds.

Economic Intelligence

ONE OTHER aspect of the NSA's alleged vacuum cleaner technology for sweeping up communications to and from the United States also has come under fire. Much of the incidental telegrams, telex and telephone communications material it scoops up has turned out to be potentially useful economic and business intelligence that NSA has sent, on request, to other agencies. The issue was very much on the minds of the Church committee. Asked Church at one point: "What are we to do about communications that fall outside the realm of traditional intelligence concerns, such as the vague category of economic or business intelligence? Are we to allow communications to or from U.S. citizens regarding economic matters to be intercepted, analyzed and disseminated by NSA?

"In an era of economic crisis, are the international phone calls and cables of American businessmen fair game for government computers?"

But so far, these sweeping questions have barely received a public hearing, let alone any clear answers. Prof. Philip B. Heyman the Harvard Law School says that these are some of many areas in which "technology has ripped open all the law about the Fourth Amendment, and what constitutes a search and an invasion or privacy. And technology is still ripping it open."

Heyman explains that, for decades, the law, and the courts' interpretation of it, has lagged behind technology's growing ability to put people under surveillance. The NSA's alleged practice, Heyman says, is an example of the trend. "What happens is that technology outstrips the law, and then the law catches up to the technology bit by bit."