Telecommunications Eavesdropping by NSA on Private Messages Alleged

The little-known but long-standing practice of the National Security Agency (NSA), 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.

Senator Birch Bayh (D–Ind.), chairman of a subcommittee on the rights of Americans of the Senate Select Committee on Intelligence, 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, as described to *Science*, 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.

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 activities 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.

Virtually all of the NSA's operations are classified. The following account of how the NSA collection program operates was pieced together by *Science* 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 the activities of enemy submarines, tanks, radars, 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 is 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, or some $75 million, 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, that 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.

Vacuum Cleaner Technology

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 1960's. 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 microminiaturization 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. Researchers at IBM cannot get their machines to take 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 1970's, has proved enormously difficult to solve. At the IBM Corporation, researchers use the company's most advanced commercial machine, the 370/168, and an artificially quiet room, to try to achieve some recognition of continuous speech.

Raj Reddy, a professor of computer science at Carnegie-Mellon University, says he works with a fairly sophisticated computer that can recognize 1000 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 transcribe phone conversations on a mass scale."

Reddy and others have speculated, however, that the NSA might use other speech recognition devices to weed 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 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 told *Science* 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!

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 Lieutenant General 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 to *Science* that NSA continues to forward some number of telegrams, telex messages, and transcripts of telephone communications—sometimes with proper names de-

Briefing

Future Doctors Balk at the Bill

One day early last March students at the Northwestern University Medical School were startled—and outraged—to learn from the Chicago newspapers that in the fall their tuition would go up from $4350 a year to $6855, or a cool 57 percent.

A tuition increase was expected but the students had assumed that it would be in keeping with the increases previously imposed, which since 1970 had been running at about 10 percent a year. After this bolt from the blue, student representatives—encouraged by a sympathetic resolution by the Medical Faculty Senate—tried repeatedly to persuade the university to reconsider its action.

But, finally convinced that they were getting nowhere, the students anted up $12,000 for a legal action fund and, on 2 August, 260 of them—or more than 80 percent of the members of the rising sophomore and junior classes—brought suit against the university in the Cook County Circuit Court. They asked the court to order that the tuition increase be rolled back to one of no greater than about 10 percent. The university has until early September to reply. A similar suit that was brought against George Washington University 2 years ago was subsequently dismissed.

The students' argument is that the Medical School, by enrolling the students under certain terms and conditions, entered into an implied contract with them that is subject to only "reasonable" changes. They contend that the 57 percent increase cannot be justified as in keeping either with the tuition charged by other private medical schools or with changes in the university's own financial needs and circumstances.

It is true, according to a recent survey made by the Association of American Medical Colleges of the 48 private medical schools in the United States, that only three—those at the Rush Medical Center in Chicago and at Georgetown and George Washington universities in Washington—now charge higher tuition than Northwestern (the Georgetown tuition of $12,500 a year is $3000 higher than any other school's). Tuition at Northwestern is now $1500 above the national average. It is also true that the big increase there was not dictated by loss of revenues.

Why, then, has Northwestern jacked up the tuition so high? The day after the students filed suit, Raymond W. Mack, the university provost, explained: "In recent years, the medical school has been too dependent on capitation grants from the federal and state governments. These grants are subject to change; and there is a growing propensity for the federal government to impose conditions [see related article on page 1066]. . . . Northwestern does not want to make drastic operational changes because of any drastic changes in the level of capita-

leted—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 provide him with the name of 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."

The IBM Corporation'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, West Virginia, 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 land-based receiver in England or Northern Europe. "You'd just call it a radio astronomy observatory or something," says one expert.

Officials of the major communications companies admitted that such interceptions could take place without their knowledge. AT&T's counsel for security, H. W. William Caming, asked whether the company had knowledge of such interception, replied, "We refer all queries regarding national security to the Department of Defense." The executive vice president of Western Union International, Thomas Greenish, asked by *Science* 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."

Law Limps Behind

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

Briefing

tion grants; and it wants to remain in a position to refuse the grants if attached conditions are unacceptable."

The provost also repeated earlier assurances given by the university that no medical student would be forced by financial reasons either to drop out or to incur an indebtedness of greater than $22,500. Northwestern claims that its aid program is exceptionally good. To keep it that way, the university has promised that $1.1 million of the federal and state capitation money which it receives this year will go into the student aid fund. Also, the terms of interest and the payback and forgiveness provisions that apply to student loans are said to be generous enough that no student's career options will be effectively limited to ministering to the rich.

Yet the fact that better than three-fourths of the medical school's sophomores and juniors are suing the university shows that the students are distrustful or unimpressed by such assurances. Jack O'Dowd, Northwestern's director of university relations, has an explanation for this too, however.

"The administration of the medical school botched this," he says. "The increase should have been explained to the students before it was imposed. The lawsuit is, I think, a direct result of our bungling the original announcement."

Sandwiches and Beer for the Press at ACDA?

Thomas A. Halsted, who as executive director for the Arms Control Association (ACA) for the past 5 years has been pretty effective at getting press attention for his group's views on SALT negotiations and arms policies generally, has now gone to the Arms Control and Disarmament Agency (ACDA). There he will be public affairs adviser to the director, Paul Warnke. Part of Halsted's success at ACA in cultivating the press was due to his frequent scheduling of noon luncheons at which arms control specialists such as Warnke and Herbert Scoville (a former ACDA and CIA official) would meet with a select group of Washington reporters over sandwiches and beer.

Still very new at ACDA, Halsted may be looking back over his shoulder since the conservative columnists Evans and Novak blasted Warnke recently for bringing him in to replace Pedro Sanjuan, whom they credit with enjoying the confidence of "defense minded congressmen." Sanjuan has been reassigned to the White House staff, where he will reportedly help lobby for Senate ratification of any new SALT agreements.

Halsted has promised Warnke that he will help build a climate of opinion for arms control. He observes that it is too early yet for him to say whether the sandwich and beer press luncheon will be appropriate in his new job.

Luther J. Carter

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, with *Science*. However several officials declared that 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 Senator 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 the 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.

Legality of Economic Intelligence

One other aspect of the NSA's alleged vacuum cleaner technology for sweeping up communications to and from the United States has also 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?

Church's question is not yet answered.

But so far, these sweeping questions have barely received a public hearing, let alone any clear answers. Philip B. Heyman, professor of law at 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 of 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."—DEBORAH SHAPLEY

Seveso: The Questions Persist Where Dioxin Created a Wasteland

Few people outside the region of Milan in northern Italy had any reason to know of the town of Seveso until a year ago, when an industrial accident put Seveso on the map. On 10 July 1976, a batch reactor in a chemical plant there overheated and discharged downwind a noxious vapor laced with perhaps the most toxic of man-made substances—TCDD (2,3,7,8-tetrachlordibenzo-*p*-dioxin). Subsequent press reports almost invariably referred, with ominous double meaning, to the cloud over Seveso. Now, more than a year later, that overworked journalistic metaphor still describes the persisting uncertainties at Seveso.

Debate continues over how or, in fact, whether the most seriously affected area near the factory can be decontaminated so that the rougly 700 inhabitants evacuated can soon return to live there. Also left hanging are questions of the long-term effects on the health of those exposed to the dioxin contained in the cloud from the explosion. While there have so far been relatively few signs of serious illness among those exposed, so little is known about the effects on humans of dioxin that the casualty list at Seveso must be regarded as open-ended.

And now there seems to be a general sense of disappointment that a major opportunity has been missed to advance the scientific understanding of the behavior and effects of dioxin under such conditions.

Certainly, concern among those directly involved has not subsided. The confusion which followed the accident soon gave way to bitter recrimination. The Italian government has been criticized for indecision and inadequate action. Reports continue of conflict between central and regional authorities and of rivalries between individuals and institutions. And the operators of the ICMESA (for Industrie Chimice Meda Societa Anonyma) plant, where the accident occurred, have been pilloried in the press and parliament, particularly for a delay in identifying the presence of significant levels of dioxin, a delay which is said to have resulted in prolonging human exposure and making decontamina-