Electronic Surveillance: Scope of Wiretapping

By NICHOLAS M. HORROCK
Special to The New York Times

WASHINGTON, Feb. 19 — From the advent of Watergate nearly three years ago, national attention has been drawn again and again to the question of electronic surveillance; the issue of exactly how much wiretapping and bugging really goes on in the United States. Recent disclosures that the Central Intelligence Agency engaged in domestic operations and that the Bell Telephone System monitored calls have served only to increase interest in the issue. Indeed, the problem has caused enough concern in Washington that a Federal commission has been appointed to investigate wiretapping and it is the subject directly or indirectly of studies by four Congressional committees.

News Analysis

Today, Senators Edward M. Kennedy, Democrat of Massachusetts, and Gaylord Nelson, Democrat of Wisconsin, introduced a bill to limit Government use of only one facet of electronic surveillance, the "national security" wiretaps and buggings. The bill would require court orders in this type of electronic surveillance.

Nobody knows how widespread unauthorized Government electronic surveillance is. Virtually every Federal investigating agency—the F.B.I., the C.I.A., the Drug Enforcement Administration, the Defense Intelligence Agency, the Secret Service, the Internal Revenue Service, the Bureau of Alcohol, Tobacco and Firearms, to mention only the large ones—has the capability for wiretapping or bugging.

With the help of Federal funds from the Law Enforcement Assistance Administration, every police department of any significant size probably has some equipment or training for electronic snooping.

Under present law, the American Telephone and Telegraph Company and the other companies of the Bell System have complete freedom to intrude on telephone conversations to check the quality of service and the performance of employes and to stop fraudulent use of telephones. Earlier this week a telephone company aide told a House subcommittee that in fighting toll fraud alone the company listened to 1.5 million to 1.8 million calls between 1965 and 1970.

Legislation Seeks Curb

Congress began to get concerned about bugging and wiretapping in the mid-nineteen sixties and the first framework of legislation to control its use was included in the Omnibus Crime Control Act of 1968.

The 1968 law, in turn, has been molded by amendments and by a Supreme Court ruling to the following legal shape: In order for any Federal or state police agency to use a bug or a wiretap in a domestic criminal or domestic intelligence case it must obtain a court order. That simply means the agency must convince a judge that there is probable cause to believe a crime is being committed and the police would be best aided in solving it by electronic intrusion.

Department of Justice officials report that in most Federal cases this is not an offhand matter, and some judges demand to know such precise details as where the bug would be placed and the chances that innocent persons might be overheard.

In the case of court-ordered wiretaps or buggings requested by a Federal agency, the agency must get the approval of the Attorney General before it goes to court.

Moreover, if the suspect under electronic surveillance is not prosecuted within 90 days and the tap or bug is thus unproductive, the Government must inform the person that he or she was listened to.

National Security Area

Current law is far more vague, however, in the area of national security wiretaps and buggings. First, no court order is required. A Federal agency has only to get the written authorization of the Attorney General in order to install a device. There is no time limit on its use and there are no criteria for determining whether it is really needed and no requirement to inform the persons under surveillance.

Present law virtually prohibits wiretapping or bugging by private individuals and strictly controls the manufacture of devices for these purposes. Indeed, it makes private electronic snooping a crime, but there are enough loopholes and exceptions in the law to allow private electronic surveillance to exist still.

In 1973, the year for which the most recent figures have been computed, courts approved a total of 864 applications for electronic surveillance from Federal, State and local police agencies. The Government does not have to make public the number of national security wiretaps or bugs it installs.

In hearings last spring before a Senate Judiciary Subcommittee studying wiretapping, former Attorney General Elliot L. Richardson estimated that the number of national security electronic surveillances being conducted at any one time was about 100. He said that the total started in the course of a year might be 150.

Mr. Richardson also pointed out that the Government conducted far more wiretaps than bugging, which brings up anplacing of an electronic listenplacing of an electroniclistening device in a room or other premises, often requires what Government agents call a "surreptitious entry," that is, a break-in or trespass to place the bug.

Wiretapping, on the other hand, can be accomplished at a distance from the target telephone.

What concerns many in Congress and in the courts is the degree to which unreported electronic surveillance is conducted by Federal and local police agencies. When J. Edgar Hoover was director of the F.B.I., high-ranking former aides have confirmed, he ordered taps removed when he

FEBRUARY 20, 1975

and Bugging an Issue of Rising Concern

testified before Congress so he could attest to a low number.

Moreover, many sources in Federal and local agencies say, there has been substantial "wildcatting"—that is the placing of surreptitious taps by the police or Federal agents for which they fail to obtain court orders.

These taps and bugs produce raw intelligence, which the police use to make arrests, and not evidence. "It's like having your own, very best informer," one Federal narcotics agent said.

Why do law enforcement officials engage in illegal wiretapping? Why do they jeopardize the prosecution of criminal cases and their own jobs? These questions go to the heart of the main issue of whether electronic surveillance is valuable at all.

Former Attorney General William B. Saxbe testified at Senate Judiciary subcommittee hearings last spring that a ban on national security taps would "put us at some disadvantage, but we would live with it."

But other law enforcement officials publicly and privately disagree. They argue that the threats to the United States, both foreign and domestic, are so sophisticated and make such great use of modern technology that police agencies without some ability to monitor telephones and to bug rooms are disarmed.

"In counterintelligence work," a former Army agent said, "you're trying to prevent a crime that hasn't happened. You need the wiretap to know where your adversary is going and what his plan is."

But electronic surveillance has had ominous side effects when used against American citizens. No matter how radical their politics, it is with this type of snooping that the Government has intruded most often into political matters.

The wiretapping of the late Rev. Dr. Martin Luther King Jr. was an example. Even if eavesdropping on Dr. King could be justified because of his own political activities, which many critics question, the eavesdroppers also overheard numerous private conversations between Dr. King and every major political leader in this country. What they said to him and he to them may well have been valuable political intelligence for then-President Johnson. Whether Mr. JJohnson learned of th material or not has never been confirmed, but the potential for political misuse was clear.

No responsible Government official now advocates a total ban on electronic surveillance. But many in the executive branch and Congress agree that there have to be far more rigid controls over electronic intrusion into the private lives of citizens. Concern is not only with wiretapping and bugging as it is now known, but also with conditions as they will be as 1984 approaches.

For instance, most major cities are now linked by computers that transmit their data, much of it private, from one city to another. There is no clear legislation against tapping computer talk. New developments in telephone technology make it possible to intrude on a large number of lines with little mechanical effort and less manpower, and these are not anticipated in current law.

Though the Government now prosecutes illelgal wiretapping in the private sector, many in Congress believe the laws should be clarified and prosecutions more aggressive. Another proposal that appears to have growing support would require court approval for all legal Government electronic surveillances, whether involving criminal cases or national security.