See also Wicker, 11 Feb 71.

THE NEW YORK TIMES, TU

Raw Material for the Snoopers

By TOM WICKER

WASHINGTON, Feb. 15 — Senator Sam J. Ervin Jr., the scourge of the snoopers, is about to open hearings on the proliferation of data banks, and it's none too soon. Every day, new disclosures make it more imperative that safeguards be imposed on computer storage and distribution of personal information.

Last week, for instance, Deputy Attorney General Richard Kleindienst told the American Bar Association that the Justice Department had made 253 applications to Federal Courts in 1969 and 1970 to make electronic "interceptions"—wiretaps and bugs. As a result, he said, there had been over 800 arrests and 72 convictions and all but twelve of the applications had been "productive."

These statistics show that more than 700 persons were arrested but have not yet been convicted of any crime. Unquestionably, a high proportion of these persons never will or should be convicted; yet, under present practices, their arrest records will go into Government files, which now means a computer data-processing center.

These records will then become instantly available to hundreds of state, local and private agencies—even in some cases to prospective employers —few of which are under any particular strictures about their privacy or as to how they may be used.

Moreover, 253 applications to bug and tap must have resulted in literally thousands of conversations being intercepted. And Mr. Kleindienst said

IN THE NATION

most of the applications had been "productive." This means that an untoward amount of unprocessed and unverified data on individuals, not all of it leading to arrests and not all of them necessarily criminals, also is finding its way to the waiting computers.

But that is just the beginning. New Jersey, which put an eavesdropping law into effect in 1969, has just reported that in the second year of operations, its agents tripled the number of wiretaps they conducted. In 1970, New Jersey officers alone recorded 24,192 conversations, of which 19,443 were reported to be incriminating: 287 arrests resulted, but no conviction data were given. New Jersey is one of only twelve states with eavesdrop laws but the American Bar Association is urging the other 38 to get cracking at the earphones. So the raw material to go into the data banks, for distribution to interested agencies and persons, is accumulating rapidly.

The police are not the only eager collectors. Senator Ervin already has disclosed that the Dragon Lady of the State Department, Director Frances Knight of the Passport Office, has at her disposal a computer bank of 243,135 names of persons considered—not necessarily proven—to be subversive or to fail to "reflect credit" on the United States. And how much do we know about the links, official or unacknowledged, between state and Federal agencies and private concerns —credit bureaus, for instance—that collect data on individuals for computer storage? Very little.

Mr. Kleindienst said the Justice Department interceptions were directed at organized crime, so it may seem quixotic to object to gathering, storing and distributing data on those engaged in that nefarious field. But the question is whether this is being done under rules that give maximum protection to innocent people.

An arrest, for example, is not proof of guilt; thousands of totally innocent people are arrested every year, but are never convicted. Yet the arrest record becomes a permanent liability that can hound an innocent person throughout his life. Even the F.B.I. tacitly concedes this by its policy of expunging arrest records from its files —but only when notified by the arresting agency that no conviction resulted, a notification local police seldom bother to make.

Dr. Alan F. Westin of Columbia University, the director of a study on data-bank implications, said in a speech at Dickinson College last week that computer technology itself made possible data-processing systems that would automatically wipe out certain obsolete records, record all requests for and distribution of data, notify the individual concerned of such transactions, and otherwise safeguard computer information and its use. This may well be the most potent suggestion Senator Ervin's subcommittee will hear.