

Devices on U.S. Agency Phones

mation to many of the nation's largest insurance companies," that one employe of SSA was finding out from SSA records who had died, then issuing new cards in their names to illegal aliens, that another fed his own address through the computer onto the records of people who had died and collected their checks, that another sold addresses obtained from SSA records to a company in the business of locating missing persons and that others fabricated 14 different beneficiary records and processed them for \$55,000 in benefit payments.

The GAO said that after earlier warnings by GAO to SSA, the latter had bought 200 doors and 480 door locks and taken some other steps to improve security. Acting SSA Commissioner Don Wortman, in a statement yesterday, said many of the lax practices are being corrected, security training was being given, doorlocks and keylocks for computer terminals which can be used only by authorized personnel were being installed, and

SSA was giving "high priority to safeguarding personal information against unauthorized disclosure."

The enormous amount of information about individuals accumulated in Social Security files and made available to other agencies was revealed in a series of letters to Moss and Rose by government agencies.

The Railroad Retirement Board said it gave income and other information to Social Security about 1.1 million people through mid-1977. Social Security said it was receiving about 5.2 million reports each quarter on veterans from the Veterans' Administration, 7 million reports from other parts of the Department of Health, Education and Welfare on closed vocational rehabilitation cases, and thousands of others from various other agencies.

In turn, it made information available without the subject's consent on millions of people to the states, the Railroad Retirement Board, and, in a smaller number of cases, the Justice Department, VA, Office of Inspector General of HEW, Labor Department, Treasury and other agencies—usually for the purpose of determining whether coordinated benefits were payable, but sometimes for auditing and investigative purposes.

Although Social Security information on an individual is generally secret, special laws permit exchanges in a wide variety of cases—such as locating runaway fathers and coordinating welfare benefits.

The GSA move on telephone conversations arose from GSA's authority over use of listening devices in federal civilian agencies, and has been encouraged by Rep. Dale E. Kildee (D-Mich.).

Frank Carr, commissioner of automated data and telecommunications

service for GSA, said the use of surreptitious listening devices of various types to monitor phone calls from outside is already forbidden by GSA except where expressly permitted by law or court order.

However, nonsurreptitious devices have been permitted where the agency deemed them essential but would be barred in the future.

Carr said that under this nonsurreptitious rule, a supervisor normally notified an employe—a Social Security expert who advised the public on benefit claims, or a tax expert who gave advice on filling out returns over the phone—that the supervisor intended to listen in.

After this blanket notice, the supervisor simply went ahead and listened whenever he or she deemed fit, without telling the employe on each occasion.

Normally no notice at all was given to the citizen who called in, according to Social Security officials. Carr said the agencies claim the purpose was to see if employes were being considerate and helpful to the public.

HEW discontinued monitoring two years ago, when Moss and others criticized the practice, but recently it asked GSA for permission to start again (though with notice to the callers this time). IRS had already notified GSA on Nov. 4, 1975, that it would monitor calls at taxpayer collection offices and services offices, according to a GSA letter to Kildee dated June 29, 1978.

Kildee, Moss and Rose are said to be deeply concerned about potential invasions of privacy from listening devices, the liberal use of Social Security information banks to give data to other agencies and the alleged loose Social Security control over data terminals.

GSA Acts to Block Listening

By Spencer Rich

Washington Post Staff Writer

The General Services Administration, supported by key House members, has moved to block various federal agencies from using listening devices to monitor telephone calls from citizens seeking information.

GSA proposed regulations on June 29 to bar all such devices, whether surreptitious or nonsurreptitious, except where permitted expressly by law or court order, or installed for public safety purposes.

The Internal Revenue Service, in 1975, received permission to use such monitoring devices. The Social Security Administration, which abandoned monitoring devices after a political blowup four years ago, had sought permission from GSA to reinstall them. Officials there said the devices would be used by supervisors to monitor how their employees deal with citizens who seek information.

The proposed GSA regulations

would block the Social Security Administration from installing the devices and would force the IRS to abandon their use.

In another development, the General Accounting Office yesterday reported that Social Security computer records on about 50 million Social Security and welfare beneficiaries "are not being properly safeguarded from potential loss, destruction, abuse or misuse."

The GAO study, requested by Reps. John E. Moss (D-Calif.) and Charles Rose (D-N.C.) more than two years ago, said there are about 3,700 computer terminals in Social Security offices all over the country and in 180 state welfare offices and 40 private insurance companies which service Medicare. These terminals can feed in as well as take out information, though since 1975 the private companies are electronically barred from nonmedical records.

The report said that, in some cases,

the computer terminals were kept in unlocked rooms with little security, that the machines were left electronically unsealed and that access to the rooms during the day wasn't restricted adequately.

The report said that a dishonest employe or even an outsider knowing the proper codes could walk in and pull information out of the computer.

Officials said the same computers also have access to central Social Security payroll records on 110 million nonbeneficiaries who are working in jobs subject to the Social Security tax.

So it is theoretically possible sources said, for outsiders or dishonest employes to obtain earnings records, addresses, medical information and other crucial facts about 160 million to 170 million people.

The report said that a private company "built a flourishing business by gaining unauthorized access to federal medical records and selling the infor-