ARTICLE APPEARED
ON PAGE A13

WASHINGTON POST
15 May 1986

House Panel Votes to Modernize Curbs on Electronic Eavesdropping

Computerized Transactions, Cellular Phone Conversations Covered

By Mary Thornton
Washington Post Staff Writer

After more than two years of study, a House subcommittee yesterday unanimously approved a bill that would make it illegal to eavesdrop on electronic communications, including cellular telephone conversations, electronic fund transfers, and computer messages and data transmissions.

The bill would also extend to such communications Fourth Amendment protection against unreasonable search and seizure.

The "Electronic Communications Privacy Act of 1986" was approved by a unanimous voice vote of the House Judiciary subcommittee on civil liberties after it received the strong backing of the Justice Department, the American Civil Liberties Union and the computer and communications industries.

Jerry Berman of the ACLU called the vote "a significant victory for citizen privacy. It demonstrates that new coalitions can be formed to enhance privacy rights."

The legislation is designed to fill the void created as technology raced ahead of the laws prohibiting improper wiretapping of telephone calls or searches of mail.

A report by the congressional Office of Technology Assessment last October warned that "many innovations in electronic surveillance technology" available to law enforcement agencies "have outstripped constitutional and statutory protections, leaving areas in which there is currently no legal protection against . . . new surveillance devices."

The report included a survey of federal agencies, including six that said they planned to intercept or monitor electronic mail as part of their investigative work.

At stake in one area is the privacy of about 250 million electronic messages in the United States each year. Industry sources estimate that 5 million Americans use electronic mail, either through commercial networks operated by companies like MCI and GTE Telenet or through corporate networks linked by computer terminals and telephone lines.

The bill would require a court-approved search warrant for law enforcement agencies to obtain a computer message within six months of its generation and a subpoena after that. Most companies eliminate their messages from the system after three months.

Another major concern is the new cellular telephone technology. Under the legislation, law enforcement agencies would have to meet the strict standards of the federal wiretap statute to eavesdrop on cellular telephone conversations, transmitted by high-frequency radio signal to base stations connecting them to telephone systems in cities where the service is available.

The bill, introduced by subcommittee Chairman Robert W. Kastenmeier (D-Wis.) in the House and Patrick J. Leahy (D-Vt.) in the Senate, does not deal with the more difficult issue of "cordless" telephones, which use a lower-frequency radio signal.

Since those conversations are often picked up unintentionally on FM radio receivers, it was decided that cordless telephone users should assume that their conversations may be overheard.

The bill contains several provisions to make it easier for federal law enforcement agencies to obtain court-approved wiretaps. It would expand the categories of crimes for which a wiretap may be approved, as well as the number of officials in the Justice Department who can approve such a request to the court.

It would also allow for court approval of a new type of wiretap when a suspect uses pay telephones. In such a case, the agent could obtain approval to follow the suspect, then call the telephone company and have a wiretap activated for that conversation.

The bill would also make it a misdemeanor to use a satellite dish to intercept subscription television signals, but only if the information is then used commercially.