Subject: Wiretap loophole concerns.
From: the tty of Geoffrey S. Goodfellow <Geoff @ SRI-CSL>

TAP 2takes (EXCLUSIVE: 10 p.m. EST Embargo) A
Loophole Raises Concern About Privacy in Computer Age By DAVID BURNHAM
c. N.Y. Times News Service

WASHINGTON - Telecommunications experts are expressing concern that the federal wiretap law does not make it a crime for anyone, whether private citizen, law enforcement officer or foreign spy, to intercept the millions of messages transmitted around the United States each day by computer.

The experts, who are in Congress, the American Telephone and Telegraph Co., and the American Civil Liberties Union, say the importance of the loophole in the 1968 law has been greatly magnified in recent years with the increasing use of computers for storing and transmitting personal, business, and government information.

Three congressional panels are considering whether the law should be rewritten to reflect the computer age. A major concern, both in Congress and among the experts, is whether the loophole gives local, state, and federal law enforcement officers an opportunity to conduct computerized electronic surveillance without the court approval required for wiretaps.

There is no evidence of widespread exploitation of the law by officers. But John Shattock, director of the national office of the civil liberties union, said: "The issue here is the privacy of communications against secret government surveillance. The threat here truly is Big Brother, not a group of little kids."

Some fear that any change in the current law, unless it is done carefully, could inadvertently increase or decrease the power of law enforcement officers.

The wiretap law forbids the monitoring of conversations except for law enforcement officers who have obtained a warrant from a judge. In the age of the computer, however, more and more messages, including those expressed by the human voice, are broken down into "digital bits" in their transmission.

But because of the way the 1968 law is written, the interception of these bits is not a crime and the police are free to intercept them without warrants.

Most electronic surveillance is passive, making it impossible to measure how much the loophole is being exploited, whether by the authorities, by industrial spies, by organized crime figures trying to make a killing in the stock market, by international spies seeking government data, or by curious individuals with a personal computer.

But in recent months a number of computerized data banks in government and industry have become the targets of long-distance

telephone attacks by amateur computer experts working from their home computers. In addition, indictments have charged foreign computer concerns with attempting to purchase sensitive details about the products of American companies.

More seriously, p 1 years ago the Carter administration announced that it believed the Soviet Union was using antennas believed to have been set up on its grounds in Washington, New York, and San Francisco to intercept digital information being transmitted in microwaves by businesses and government agencies.

The Carter administration took limited technical steps to prevent the Russians from obtaining sensitive government data and ordered the National Security Agency to help private corporations improve their security. But it never took any formal legal action against the Russians or formally asked Congress to amend the law.

H.W. William Caming oversees privacy and corporate security matters at AT&T. "As we enter the year made famous by George Orwell's book, 'Nineteen-Eighty-four,' computer crime is on the rise and may well constitute a major crime threat of the 1980s," he said in a recent interview. "We therefore are encouraged by and vigorously support current efforts in Congress and the states to enact suitable legislation concerning computer crime. We believe that such legislation should include provisions making it a crime to secretly intercept non-voice communications."

AT&T is not the only company concerned about the wiretap law. In response to an inquiry, Satellite Business Systems, a major new data communications company jointly owned by International Business Machines, the Aetna Life and Casualty Co., and Comsat, agreed that some experts believed there was a "potential loophole" in current law and that, to the extent this was so, "legislation to make clear that such unauthorized interception is prohibited would be useful."

The 1968 wiretap law makes it a federal felony for a third party to intercept the conversations of others by placing an electronic listening device, or a "bug," in a telephone or other place such as an office.

The only exception is that federal, state, and local law enforcement officers may use wiretaps in the investigation of certain crimes but only with the approval of the senior prosecutor of a particular jurisdiction and a special warrant from a judge.

The law does not apply to computer tapping