Civil liberties in the US threatened on two electronic fronts

James Brookfield
31 August 1999

Two US government initiatives made public over the past two weeks pose dramatic threats to civil liberties. First, the Justice Department has drafted proposed legislation to allow police to break into homes and businesses in order to "wiretap" computers, capture passwords and install devices to override security and encryption programs. Second, the Federal Communications Commission has adopted new standards for cellular telephones that will allow police to gather more information about callers, including their approximate location and the nature of their discussions.

Word leaked out about the Justice Department legislation, the "Cyberspace Electronic Security Act," in a news report in the *Washington Post* of August 20. The report indicates that the proposed legislation will allow police to obtain a warrant and enter a home or business unbeknownst to the those living or working there. (Presently, most search warrants require notification to be given before police enter.) Once the tapping device is installed and court approval obtained, computer data files may be captured. According to the article, the plan has already been reviewed by several government agencies and is ready to be introduced for consideration by Congress.

The proposed law is intended to circumvent popular encryption programs that are used to keep electronic communications private. These programs use "keys" to scramble and unscramble messages sent over the Internet. At present, the government is not able to crack the code used by the keys, so that even if it intercepted a message, it could not read it. By installing a device on a computer, government agents will be able to compromise this method of encryption.

Earlier, the Clinton administration wanted to find an electronic means to facilitate the interception and decryption of messages. But various proposals under consideration involved measures that clearly undermined the security of nearly all computer users (e.g., only allowing companies to distribute encryption keys that could be cracked by the government, requiring computers to use chips that could be accessed by the police, etc.). A new approach was needed. Because the latest proposal (physical break-ins) requires a judge's approval of a warrant, it will be presented as an "anti-crime" initiative that will affect only those under investigation.

The proposal has already been condemned by civil liberties and electronic privacy groups. The Center for Democracy and Technology said in a statement on its web site: "The proposal is intended to eliminate a core element of our civil liberties." A senior staff counsel at the CDT, James Dempsey, told the *Post*, "They have taken the cyberspace issue and are using it as justification for invading the home."

The cellular telephone decision came as part of a Federal Communications (FCC) ruling on August 27. The FCC was empowered by a 1994 law, the Communications Assistance for Law Enforcement Act (CALEA), to set down technical standards that all cell phone companies must obey. The intent of the law was to facilitate monitoring of cellular telephone calls by the Federal Bureau of Investigations.

Prior to the new FCC decision, federal agents had already been able to monitor calls, but the new rules give them additional wide-ranging powers. These include: the ability to identify all participants in a conference call in which a cell phone user is participating, the ability to listen in on such conversations even after the cell phone user has hung up, and the ability to track the physical location of the transmitter nearest the cell phone at the beginning and

end of a call, thereby turning the phone into a rough tracking device. The ruling was seen as a clear victory for the FBI.

These two developments follow similar efforts in other countries and a new US plan to eavesdrop on computer use by government employees (see links below).