Clinton Is Trying to be Big Brother

August 8, 1996 by Phyllis Schlafly

We hope the appropriate government agencies will soon solve the recent terrorist crimes and punish the criminals. But all Americans who care about civil liberties should vigorously resist President Clinton's attempt to use the terrorist attacks as an excuse to carry on his all-out war against the personal privacy of law-abiding Americans.

This mind-set was first revealed in the Clinton health care bill, which would have given the government computer access to the medical records of all Americans. Fortunately, that totalitarian takeover of the health care industry was rejected.

The Clinton Administration's education legislation now pending in Congress would put personal information about all schoolchildren -- academic, medical, attitudinal, behavioral, and family -- into an expanded Labor Market Information database available to the government, as well as to prospective employers.

Now the Clinton Administration is trying to make it illegal for individual Americans to have private conversations with one another. That's the real meaning of its effort to control encryption technology, and it's a direct assault on the First Amendment.

It would be downright ridiculous to assert that the First Amendment guarantees our right to speak in public but not in private. It would be just as ridiculous to say that we have freedom to speak in words that the government can understand, but not in words the government can't decipher.

Americans have the right to speak to one another in private, behind closed doors, and we should likewise have the right to speak to one another in code and to put our coded messages on computer in a

process called encryption. Americans would not tolerate the government ope0ing and reading the letters we send through the mails, and we shou0d not tolerate the government opening and reading our encrypted, or coded, messages sent via computer.

Yet, Attorney General Janet Reno, FBI Director Louis Freeh, and Vice President Al Gore are all demanding the authority to read our encrypted messages. In a speech to the Commonwealth Club of California, Reno bluntly stated her demand for "ensuring law enforcement access to encrypted data."

Reno boasted that there is "a consensus" that the government should create a system known as "Key Escrow" (i.e., a supposedly "neutral third party"), to which all Americans should be forced to "entrust" the keys to their encrypted messages, and to which the government would have access. On the contrary, there is no such consensus.

Do you trust Janet Reno with access to your private messages? Do you trust the FBI to keep your files confidential?

The Clinton Administration is already doing 30 to 40 percent more federal telephone wiretaps and other electronic surveillance than the last year of the Bush Administration. Those figures don't even include national security wiretaps or the hundreds of extensions granting more time for wiretap orders already issued.

FBI Director Freeh wrote the New York Times last November that "There is no intention to expand the number of wiretaps or the extent of wiretapping." Four months later, FBI documents revealed that the FBI does, in fact, plan to increase electronic surveillance 54 percent by 1998 and 130 percent by 2004.

On July 12, Al Gore announced that the Administration will continue to push for the adoption of a massive public key infrastructure to give the government access to all encrypted communications. In a blatant bid for a police-state surveillance society, Gore warned about "the dangers of unregulated encryption technology."

A neutral panel of the National Research Council was set up to make policy recommendations about encryption. The panel called on the government to abandon its efforts to restrict encryption.

The NSC panel concluded that increased use of encryption would enhance our national security, not diminish it. Thirteen out of its 16 members had security clearances with access to secret information, and they saw no national security reason to justify the Clinton policy.

The Clinton Administration bases its campaign to control private encryption on the alleged need to fight crime through wiretapping. However, the NSC panel concluded that the ability of the private sector to transfer confidential financial and other data over the information highway without interception is far more important.

New technologies have given government awesome power to spy on individuals. The Filegate investigation accidentally uncovered the shocking news that, as soon as Bill Clinton entered the White House in 1993, he secretly spent $400,000 on software to create a highly sophisticated computer database to track detailed political, financial, attitudinal, and personal biographical information on 200,000 people, including members of Congress and the media. Known as WHODB for White House Office Data Base, the system was nicknamed Big Brother.

Encryption is a First Amendment issue, not a crime issue. If the Clinton Administration is allowed to control encryption, it would be the biggest expansion of federal power since the passage of the Income Tax Amendment in 1913.