Encryption Is Essential to Freedom

April 2, 1997

Google Ads are provided by Google and are not selected or endorsed by Eagle Forum

The Clinton Administration sent three of its spokesmen to Capitol Hill last week to plead the case for "key escrow" before the House Subcommittee on Courts and Intellectual Property. They were testifying against H.R. 695, a bill that states: "It shall be lawful for any person . . . to use any encryption, regardless of the encryption algorithm selected, encryption key length chosen, or implementation technique or medium used."

It is a sad day to think that Americans might need permission from Congress to have a private conversation! Key escrow means depositing a key to your computer code with a third party and allowing the government to have access to it. It is tantamount to giving the government the keys to your house and, if that ever happens, freedom in America is gone.

Sending messages on computer without encryption is like putting all your thoughts on a postcard; anyone and everyone can read it. Privacy in the computer age requires putting our communications in code (encrypting them) so that only designated recipients can read them.

Advances in computer technology have been wonderful in so many ways, but they are also constantly eroding our personal privacy. Massive databases are now keeping track of our phone numbers, addresses, income, credit records, purchases, and medical history.

The right of Americans to speak in private (whether in English, a foreign language, or in code) is fundamental to our First Amendment rights. The freedom to send and receive coded messages cannot be limited without seriously eroding our civil liberties.

That right is endangered today by the U.S. Department of Justice. Attorney General Janet Reno and FBI Director Louis Freeh are giving speeches advocating the regulation of cryptography. They openly and brazenly assert the right of the Federal Government to read your computer E-mail messages and listen in on your telephone conversations.

Freeh really doesn't like the whole idea that Americans can have private conversations. Last July 25, he

told the Senate Committee on Commerce, Science and Transportation that encryption poses a "threat to public safety." He wants to forbid the use of encryption products unless they are "socially-responsible," i.e., have key escrow built into them.

Freeh asserted that there is now an "emerging opinion throughout much of the world" in favor of key escrow. Al Gore calls it a "consensus." But there is no such consensus; nobody is pushing it except the Clinton Administration.

Are we worried that the Justice Department might abuse its power to eavesdrop on our computer messages? You bet we are. The misbehavior of the FBI in so many areas, and the coverups that followed, have been shocking. Giving the FBI access to our computer messages would be a long, dangerous step toward making America a totalitarian state.

The Clinton Administration spokesmen tried to tell the House committee that they are not urging "mandatory" key escrow, they only want "voluntary" key escrow. But this difference is not significant to the individual computer user.

The Federal Government is notorious for using all sorts of coercive methods, including intimidation, tax funding incentives, and export controls to make something mandatory while loudly proclaiming it to be "voluntary." The right of the individual to privacy would be meaningless if the Clinton Administration browbeats the telephone and software companies into "voluntarily" building key escrow into all their products.

It is important to recognize that encryption is not only a right of free speech, but also that encryption is a good thing, not a bad thing, or a criminal thing. Strong encryption is one of the greatest achievements of the information age.

Encryption will enable us to talk on the telephone with assurance that no one is eavesdropping. It will enable us to exchange E-mail, make purchases, and invest our money in privacy, because snoops cannot decode data traffic even if they gain access to a network.

Telephone users are becoming increasingly annoyed with the fact that nosy people can easily listen in on our wireless (cellular and cordless phone) conversations. Even though improved digital technology, which makes listening in more difficult, is becoming available, millions of old-style, insecure wireless phones are expected to be sold this year.

It should be the policy of the United States to encourage wide dissemination of strong encryption technology. It is unfortunate that some pending bills in Congress impose criminal penalties for the use of encryption in connection with a crime, thus giving the impression that encryption is somehow suspect. We should punish criminals for actual crimes, not for auxiliary activities that are entirely lawful and proper.

We don't want to move toward a nation in which any state crime becomes a federal felony merely because a computer, telephone, or other electronic device is involved. Considering the present status of judicial activism, Congress should be removing jurisdiction from the federal courts, not adding to their jurisdiction.