Don't Let Janet Reno Read Our E-mail

August 13, 1997

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

The personal privacy of individual American citizens is rapidly eroding on every front. Advancing technology has made it easier for government agencies, the police, credit bureaus, telemarketers, and all sorts of nosy people to monitor where we are, who we associate with, how we spend our money, who we talk to on the telephone, and what medical care we receive.

With business computers and government bureaucracies constantly compiling data about our comings and goings, encryption is a wonderful technology that can enable us to get back some of our privacy. Encryption locks up your messages so that only the intended recipients, each of whom has his own key, can unlock them, and you can carry on a cell-phone conversation without snooping from scanners.

Once encrypted, your phone conversations and E-mail will sound or look like gibberish to everyone except those who have the key to decrypt it. We look forward to the day when encryption technology will be just as common as sealing an envelope before you mail it.

Encryption has become a hot political issue. Most of us want control over our own encryption keys, just as we demand and expect control over the keys to our homes.

Civil liberties groups correctly assert that we have a First and Fourth Amendment right to speak in a manner of our own choosing and to be secure from government searches. Just as we have the right to speak in Spanish or Greek as well as in English, we have a right to speak in code on our computer or on our cell phone so that our messages and conversations will be private.

But Bill Clinton and Al Gore want to regulate encryption. The Clinton Administration has come up with plans to control encryption, variously called "clipper," "key escrow," "key recovery," or "key management infrastructure."

These plans have been rejected by consumers, industry, those who believe in civil liberties and the free market, and even the Europeans. Only the U.S. Senate takes the Clinton plan seriously.

Senators John McCain (R-AZ) and Bob Kerrey (D-NE) have introduced the Secure Public Networks Act, S.909, which is a direct attack on the Bill of Rights as well as on our right to privacy. To avoid coping with arguments against it, they rushed it through the Senate Commerce Committee without any publicity.

S. 909 gives the FBI and other government agencies the ability to seize your cryptographic keys. The bill's advocates assert that the government is merely trying to maintain the status quo, and that civil liberties are protected because court orders are required before the government can get your keys.

That's false. S. 909 overturns the status quo and gives government agencies the practical power to pervasively monitor electronic communications in a way they cannot now. As originally drafted by the Clinton Administration, S. 909 would have allowed government agents to seize private keys without a court order or search warrant, and even without notice to the individual whose privacy is violated.

Supporters of S. 909 added a fuzzy one-sentence amendment to the bill in committee and claim it now guarantees full protection of our constitutional rights. Critics of the bill believe it takes more than a single sentence to paper over the bill's enormous dangers to personal liberty.

Supporters of the bill say the government-mandated key escrow system would be "voluntary." That's also false. A panoply of federal regulations, federal purchasing policies, criminal penalties, and civil liability exposure would effectively force any business of any size to use the government system, and all the business's customers would have to follow suit.

The bill would also make a type of government regulated electronic ID code effectively mandatory for doing business. To get the ID, you would have to buy into the government system.

FBI Director Louis Freeh is passionately eager to have a law that lets his agents seize private keys without a court order. He speaks ominously about what he calls "the looming spectre of the widespread use of robust, virtually uncrackable encryption."

Freeh compares encryption to fast cars, saying, "Would we allow a car to be driven with features which would evade and outrun police cars?" Maybe he'll try to ban Corvettes when he finds out how fast they can go.

This is the same Louis Freeh who last year proposed that one percent of the telephone capacity in urban areas be reserved for wiretaps (that's 10,000 phones in a city of one million). Even the KGB and the Gestapo didn't reach that level of surveillance.

Sensible people are not persuaded by Freeh's alarmist speeches. Last year, the National Research Council Commission concluded that national security arguments for controlling encryption are increasingly outdated, and that the ability of the private sector to transfer confidential financial and other data over telecommunications pathways without interception is a higher priority than government wiretapping.

No free nation has ever tried to regulate or snoop on the content of private messages until the Clinton Administration. The crucial political question is whether law-abiding Americans will be able to secure their own keys, giving them only to persons of their own choosing, or whether we will be forced to surrender our keys to government surveillance agents.