Big Brother Is on the Prowl

March 25, 1998

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

Do you worry that Big Brother (a.k.a. the Federal Government) wants to monitor your e-mail, your phone calls, your health and financial records, and your business? You should, and that's why Sen. John Ashcroft's Subcommittee on the Constitution is holding a hearing this week.

The Fourth Amendment to the Constitution, "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated," was written at a time when unreasonable searches and seizures were carried out principally by armed troops. This language is just as applicable and vital today to protect us against unreasonable searches carried out by modern mechanisms.

Encryption is the marvelous technology that can enable American citizens to protect their Fourth Amendment right "to be secure in their persons, houses, papers, and effects." Encryption is the technology that can encode, or scramble, your computer files and messages and your telephone calls so they can only be read or understood by you and by persons of your choice.

Americans now have the right to encrypt our files and messages, but Janet Reno and the FBI want to take it away. They believe that, to be sure you are not breaking the law, the Federal Government should have access to all your private files and messages at any time and without your knowledge.

When you put messages in code, whether it's an old-fashioned code written on paper or a newfangled code concocted on a computer, there must be a "key" to enable you and the recipients of your communications to read them. Big Brother wants you to give him your key.

The FBI is asking Congress to pass a law requiring all Americans to deposit the key to all our software files and communications with a "third party" so that the government will be able to use those keys to read our files whenever it wishes. This is called "key recovery."

This is tantamount to giving the FBI the power to steam open all the letters we deposit at the post office. That's only done in totalitarian countries.

Rep. Bob Goodlatte (R-VA) says that "encryption is to digital communications what deadbolt locks are to doors." Giving the FBI access to our encryption keys would be like giving our door keys to the local police, leaving our doors unlocked, and relying on the police to catch burglars after they break and enter.

Strong encryption for individual use is the number-one privacy issue in the information age. There are all kinds of reasons why we want to encrypt our own computer files and e-mail and telephone calls, and also want the people with whom we do business to use strong encryption so that the personal records they have on us will not fall into unauthorized hands.

Whether you use a computer or not, enormous amounts of your personal information are already collected and stored "on line" on somebody else's computer. Doctors and hospitals store and transfer sensitive medical records.

The Internal Revenue Service, the Social Security Administration, your bank, and credit card companies hold and transfer information about your finances. Your employer and the stores where you shop collect and transfer information about your income and purchases.

The telephone company has a complete listing of every phone call you make or receive, including the phone numbers, the time, and how long you talked. Encryption will not prevent the government from getting that list, but it will protect you against anyone eavesdropping on your conversations.

The public schools are starting to participate in a national data collection system that will collect and transfer private information about all students, not only their academic records, but also medical, attitudinal, behavioral, and family information that is none of the schools' business. The plan is to have these electronic portfolios available to the government and to the students' future employers.

The new "deadbeat dads" law has initiated a massive federal database called the New Hires Directory. The law requires every employer to report to the Federal Government the name, address, Social Security number, and wages of every new worker, regardless of whether they are deadbeats or even dads.

Businesses have their proprietary information, trade secrets, and inventory data on computers and would be ruined if that information leaked to their competitors. Businesses use the Internet to buy and sell materials, to offer and receive bids, and to invoice customers.

The FBI argues that it needs "key recovery" power to crack down on drug lords and terrorists, but the bad guys can buy top-quality encryption from dozens of other countries. The danger from these criminals should NOT require Americans to submit to police-state surveillance of their daily lives and activities.

Can we trust the FBI with the awesome power of key recovery? No. The FBI has already betrayed our trust in so many areas, including turning over nearly a thousand "raw" personnel files to political operatives at the Clinton White House, the multiple outrages at Waco and Ruby Ridge, and the abuse of Richard Jewell, the falsely accused Atlanta security guard.