

PREPARED STATEMENT OF PHYLLIS SCHLAFLY, PRESIDENT, EAGLE FORUM

Security and Freedom Through Encryption (SAFE) Act

March 20, 1997 - House Judiciary Subcommittee on Courts and Intellectual Property

My name is Phyllis Schlafly. I'm president of Eagle Forum, a national volunteer organization concerned with public policymaking on many issues, including constitutional issues. Thank you for inviting me to present our views on H.R. 695 and cryptography. Our home page on the Internet is at www.eagleforum.org.

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, medical histories, and purchases. With everything connected to the Internet, the only way to keep our information private is to avoid computers (which is impossible), or to encrypt it.

Encryption should be recognized as a fundamental right. I believe that our right to speak in private (whether in English, a foreign language, or in code) is protected by the First Amendment to the U.S. Constitution, and that the government cannot regulate or limit that right without seriously eroding our fundamental civil liberties.

I thank Congressman Goodlatte and the other sponsors of this bill for recognizing that our rights of free speech are endangered by the Justice Department. It is a sad day to think that Americans might need permission from Congress to have a private conversation! It should not be necessary for Congress to pass a law declaring that encryption is lawful.

The problem is that Attorney General Janet Reno and FBI Director Louis Freeh are giving speeches advocating the regulation of cryptography and giving the government access to our computer messages. They repeatedly demand that the government be able to get a key to our telephones and computer systems.

Mr. Freeh even says that encryption poses a "threat to public safety." On the

contrary, the threat to public safety comes from the lack of encryption and the demands of Justice Department officials to have a key so they can read our private messages.

Are we worried about the Justice Department abusing 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 to Americans who like to support law-and-order. The FBI abuses are such that, to give the FBI access to our computer messages would be a long, dangerous step toward making America a totalitarian state.

We are also very concerned that a ban on "mandatory key escrow" might not preclude the government from other coercive key escrow plans, deceptively called "voluntary." The Federal Government is notorious for using all sorts of weapons, including intimidation and funding incentives, to make something mandatory while they are loudly proclaiming it to be "voluntary." The right of the individual to privacy would be meaningless if the telephone companies "voluntarily" agree to key escrow.

I believe it is not only important to recognize that encryption is a right of free speech, but also that encryption is a good thing, not a bad thing or a criminal thing. We are very opposed to the criminal penalties in this bill. It is doubtful that Congress even has the constitutional authority to criminalize encryption.

Let's take an example. It is, of course, lawful to use opaque envelopes. Would it make sense to legislate five years in federal prison for using opaque envelopes in connection with a crime? Would it stop the problem of bad checks if we were all forced to mail our checks in transparent envelopes? 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.

We object strenuously to the current trend toward federalizing crimes. This is offensive to our constitutional system of federalism. Considering the present status of judicial activism, Congress should be removing jurisdiction from the federal courts,

not adding to their jurisdiction.

We object to the implication that encryption is somehow suspect. Strong encryption is one of the greatest achievements of the information age. It means we will be able to talk on the telephone with assurance that no one is eavesdropping. It means we can 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.

It should be the policy of the United States to encourage wide dissemination of strong encryption technology. I thank the sponsors of H.R. 695 for recognizing the vital importance to individuals of unrestricted cryptography, and I hope the bill will be amended to remove criminal deterrents to using cryptography.

**NATIONAL
SECURITY
ARCHIVE**

This document is from the holdings of:

The National Security Archive

Suite 701, Gelman Library, The George Washington University

2130 H Street, NW, Washington, D.C., 20037

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu