



United States  
of America

# Congressional Record

PROCEEDINGS AND DEBATES OF THE 105<sup>th</sup> CONGRESS, SECOND SESSION

Vol. 144

WASHINGTON, MONDAY, MARCH 30, 1998

No. 38

## House of Representatives

The House met at 12:30 p.m. and was called to order by the Speaker pro tempore (Mr. PETRI).

### DESIGNATION OF SPEAKER PRO TEMPORE

The SPEAKER pro tempore laid before the House the following communication from the Speaker:

WASHINGTON, DC,  
March 30, 1998.

I hereby designate the Honorable THOMAS E. PETRI to act as Speaker pro tempore on this day.

NEWT GINGRICH,  
*Speaker of the House of Representatives.*

### MORNING HOUR DEBATES

The SPEAKER pro tempore. Pursuant to the order of the House of January 21, 1997, the Chair will now recognize Members from lists submitted by the majority and minority leaders for morning hour debates. The Chair will alternate recognition between the parties, with each party limited to 30 minutes, and each Member, except the majority leader, the minority leader, or the minority whip, limited to 5 minutes.

The Chair recognizes the gentleman from Virginia (Mr. GOODLATTE) for 5 minutes.

### THE SECURITY AND FREEDOM THROUGH ENCRYPTION ACT

Mr. GOODLATTE. Mr. Speaker, strong encryption products are the locks and keys of the digital age. To ensure that the computer files of American citizens are protected, I have introduced H.R. 695, the SAFE Act, Security and Freedom through Encryption, which has 250 bipartisan cosponsors. The SAFE Act is supported by organizations from across the political spectrum. It is not often that legislation brings together such a diverse array of Members and interest groups.

On one side of this debate are the United States Chamber of Commerce, the National Association of Manufacturers, the Law Enforcement Alliance of America, the American Civil Liberties Union, the National Rifle Association, Americans for Tax Reform, Eagle Forum, the Center for Democracy and Technology, and a whole host of business organizations concerned about the security of their computer communications.

Who is on the other side? The administration, which continues to pursue a policy that threatens the privacy of American citizens. If the Government can access your encrypted computer files, medical records, tax returns and personal financial information, then hackers can, too.

I am pleased to be the sponsor of this legislation with the gentlewoman from California (Ms. LOFGREN), the lead Democrat cosponsors. There are about 150 Republican cosponsors of this legislation, and over 100 Democrat cosponsors as well.

This is truly a bipartisan effort. This legislation is designed to do three things: First, protect the privacy of law-abiding American citizens. People know today that their e-mail, their credit card numbers, their medical records, their tax returns, if they are submitted electronically, their industrial trade secrets, their copyrighted material, are all subject to invasion by hackers, by criminals and others who will make their communications available to who knows who for what reason.

Privacy is important in the Information Age, and we need to protect it.

Secondly, this is an important anticrime measure. This legislation will help to make sure that people who do use the Internet for electronic commerce will have that credit card number protected from a hacker stealing it.

The New York Stock Exchange, which has to encrypt its financial com-

munications, which go all over the world, to make sure somebody does not break into that system and cause a financial crisis by changing the numbers in the computer system, or the same thing for a nuclear power plant, somebody breaking into its computer system and causing a meltdown. This is something that protects the infrastructure of our country and it protects individuals using the Internet, making sure their medical records are secure.

Industrial espionage is one of the largest problems we have in the criminal area in this country. The FBI has estimated more than \$24 billion and/or more a year in industrial espionage takes place, and what is the prime place of that? Breaking into somebody's computer to steal information. Encryption, the scrambling of information to make sure it cannot be decoded by somebody intercepting it, is the Number one way to make sure this is safe.

Finally, this is an issue about jobs, jobs of American citizens. We dominate the software industry in the world. Today, nearly 75 percent of all the software sold in the world is created in the United States. But our foreign competition is on to the fact that this administration is using our export control laws to limit access to strong encryption by our software companies, by our citizens, and by those overseas who would like to buy the quality software products American companies make and cannot do so because of the fact that we have these export laws that limit access to this valuable software.

So they are using that to gain a competitive advantage, and we will lose the advantage we have in the world as we move more and more into encrypted software, as we move into the next century.

So these three things, protecting the privacy of American citizens, fighting crime, and making sure that we protect and create new jobs in a growing

□ This symbol represents the time of day during the House proceedings, e.g., □ 1407 is 2:07 p.m.

Matter set in this typeface indicates words inserted or appended, rather than spoken, by a Member of the House on the floor.



Printed on recycled paper containing 100% post consumer waste

H1701