

There is little question that continuing advances in technology are changing forever the way in which people live, the way they communicate with each other, and the manner in which they work and conduct commerce. In just a few years, the Internet has shown the world a glimpse of what is attainable in the information age. As a result, the demand for more and better access to information and electronic commerce continues to grow—among not just individuals and consumers, but also among financial, medical, and educational institutions, manufacturers and merchants, and State and local governments. This increased reliance on information and communications raises important privacy issues because Americans want assurance that their sensitive personal and business information is protected from unauthorized access as it resides on and traverses national and international communications networks. For Americans to trust this new electronic environment, and for the promise of electronic commerce and the global information infrastructure to be fully realized, information systems must provide methods to protect the data and communications of legitimate users. Encryption can address this need because encryption can be used to protect the confidentiality of both stored data and communications. Therefore, my Administration continues to support the development, adoption, and use of robust encryption by legitimate users.

At the same time, however, the same encryption products that help facilitate confidential communications between law-abiding citizens also pose a significant and undeniable public safety risk when used to facilitate and mask illegal and criminal activity. Although cryptography has many legitimate and important uses, it is also increasingly used as a means to promote criminal activity, such as drug trafficking, terrorism, white collar crime, and the distribution of child pornography.

The advent and eventual widespread use of encryption poses significant and heretofore unseen challenges to law enforcement and public safety. Under existing statutory and constitutional law, law enforcement is provided with different means to collect evidence of illegal activity in such forms as communications or stored data on computers. These means are rendered wholly insufficient when encryption is utilized to scramble the information in such a manner that law enforcement, acting pursuant to lawful authority, cannot decipher the evidence in a timely manner, if at all. In the context of law enforcement operations, time is of the essence and may mean the difference between success and catastrophic failure.

A sound and effective public policy must support the development and use of encryption for legitimate purposes but allow access to plain text by law

enforcement when encryption is utilized by criminals. This requires an approach that properly balances critical privacy interests with the need to preserve public safety. As is explained more fully in the sectional analysis that accompanies this proposed legislation, the CESA provides such a balance by simultaneously creating significant new privacy protections for lawful users of encryption, while assisting law enforcement's efforts to preserve existing and constitutionally supported means of responding to criminal activity.

The CESA establishes limitations on government use and disclosure of decryption keys obtained by court process and provides special protections for decryption keys stored with third party "recovery agents." CESA authorizes a recovery agent to disclose stored recovery information to the government, or to use stored recovery information on behalf of the government, in a narrow range of circumstances (e.g., pursuant to a search warrant or in accordance with a court order under the Act). In addition, CESA would authorize appropriations for the Technical Support Center in the Federal Bureau of Investigation, which will serve as a centralized technical resource for Federal, State, and local law enforcement in responding to the increasing use of encryption by criminals.

I look forward to working with the Congress on this important national issue.

WILLIAM J. CLINTON.

THE WHITE HOUSE, September 16, 1999.

SALUTE TO GERARD GAUTHIER, EDWIN KUHLMANN, AND ROBERT STUMPF UPON RECEIPT OF POW MEDALS AT NELLIS AIR FORCE BASE

(Mr. GIBBONS asked and was given permission to address the House for 1 minute and to revise and extend his remarks.)

Mr. GIBBONS. Mr. Speaker, today I rise in honor of three POWs, and I recall the words of President John F. Kennedy who once said, "In the long history of the world, only a few generations have been granted the role of defending freedom in its hour of maximum danger. I do not shrink from this responsibility. I welcome it."

Mr. Speaker, I can think of no better words to describe three former World War II POWs from Nevada who were honored with POW Medals at Nellis Air Force Base last Friday.

Gerard Gauthier, Edwin Kuhlmann, and Robert Stumpf did not shrink from their responsibilities, indeed they welcomed them, ultimately enduring the greatest test of fighting men and women, as captives of our enemies.

Just as the Soldiers' Code of Conduct now says, these men never forgot that they were American fighting men, responsible for their actions and dedicated to the principles which made our country free.

I stand here to honor these men, men of one of the greatest generations for providing the fighting men and women that followed in their footsteps the bedrock for returning with honor. As a veteran of two of our Nation's wars, I salute their sacrifices and services. They are our heroes. They are our Nation's heroes. I thank them for their patriotism, their courage, and their inspiration.

SPIES FROM RUSSIA

(Mr. TRAFICANT asked and was given permission to address the House for 1 minute and to revise and extend his remarks.)

Mr. TRAFICANT. Mr. Speaker, first it was China, and now it is Russia. The FBI said Russia is spying on America. If that is not enough to tax one's vodka.

The FBI says that 50 percent of all Russian diplomats in America are likely to be spies. Unbelievable. The White House gives billions of dollars to Boris. Boris uses our money to spy on us.

Now, Mr. Speaker, I thought we always gave billions of dollars to Russia because they were so poor they could not even afford toilet paper. I say it is time to put Boris on a cash diet. Maybe when he runs out of toilet paper, he will stop spying on us.

Mr. Speaker, I yield back the Charmin.

REPUBLICAN TAX CUT IS FAIR, PRUDENT AND BALANCED

(Mr. STEARNS asked and was given permission to address the House for 1 minute and to revise and extend his remarks.)

Mr. STEARNS. Mr. Speaker, let us set the record straight this afternoon about the Democrat accusations that the Republican tax relief package is huge, massive, gigantic, irresponsible.

It starts very slowly, as a matter of fact, and it only goes forward if we have surpluses.

Here are some figures that my colleagues will not hear from the Democrats: The tax cut for the first year, the fiscal year 2000, it is \$5.3 billion. Now, out of an \$8 trillion economy, that is not massive.

The next year, 2001, it is \$1.1 billion. Now, that is not huge. In the year 2002, it is \$34.7 billion. In the year 2003, it is \$53.1 billion. In the year 2004, it is \$61.7 billion.

So, Mr. Speaker, over the next 5 years, the tax cuts will total about \$156 billion. That is not risky. That is not irresponsible. These are the numbers, and these are the facts.

This approach by the Republicans is balanced, fair, prudent, and a great tax cut for the American people.

CALL FOR LIBERALS TO EXPLAIN WHY TAX RELIEF PROPOSAL IS SO OFFENSIVE

(Mr. HEFLEY asked and was given permission to address the House for 1 minute.)