

#### HIGH TECH AWARD FOR SENATOR ABRAHAM

Mr. MCCAIN. Mr. President, I rise to inform my colleagues of a significant honor recently bestowed upon our colleague, the Senator from Michigan, Mr. ABRAHAM.

On June 16, Senator ABRAHAM became the first United States Senator to receive the "Cyber Champion" award, from the Business Software Alliance. He was recognized for his legislative accomplishments in support of America's high-technology economy. I would like to congratulate Senator ABRAHAM on receiving this well-deserved honor.

Senator ABRAHAM has been a champion of high-tech since coming to the Senate. He has worked hard on a high-tech agenda to keep Americans employed in good jobs at good wages, and to help our nation keep the edge we need in the global marketplace. It has been my pleasure to work with him on many of these issues.

Whether fighting to expand and rationalize the use of electronic signatures, expanding high-tech visas, increasing charitable giving to our schools so that we can train our kids in the uses of high-technology, keeping the Internet free from unnecessary interference and taxation, or seeing to it that we are prepared for the year 2000, Senator ABRAHAM has been a leader on high-tech issues.

Now Senator ABRAHAM is working to protect property rights on the Internet through his anti-cybersquatting legislation. His bill would empower trademark owners to protect their marks, at the same time protecting consumers from potential fraud.

There is no doubt in my mind that Senator ABRAHAM's efforts will help workers and the economy in Michigan and across the United States. Once again, I congratulate him on this honor, and on the accomplishments that have earned it for him.

---

#### PROTECT ACT

Mr. FEINGOLD. Mr. President, I rise today to discuss an issue of increasing national and international importance.

Mr. President, encryption may not yet be the most common term in the American lexicon, but it may well affect every American as we progress in this Information Age. Encryption systems provide security to conventional and cellular telephone conversation, fax transmissions, local and wide area networks, personal computers, remote key entry systems, and radio frequency communication systems. As we become more reliant on these technologies, encryption becomes a more important application.

For these and other reasons, I come to the floor today to discuss my decision to cosponsor S. 798, the Promote Reliable Online Transactions to En-

courage Commerce and Trade, or PROTECT Act. This bill pushes us toward a thoughtful debate on encryption policy.

I appreciate the efforts of the Chairman of the Commerce Committee, Senator MCCAIN, to push this important legislation forward. As the chairman knows all too well, balancing competing interests, regardless of issue, is a difficult, and often thankless, job. In this case, we must find an equitable balance between personal privacy, technological innovation and public safety.

The rapidly expanding global marketplace and our increasing reliance on new technology has resulted in the almost instantaneous transfer of consumer information. Bank information, medical records, and credit card purchases are transferred at lightning speed. But these transactions, and even browsing on the Internet, can leave consumers vulnerable to unwanted and illegal access to private information. Encryption technology offers an effective way consumers can ensure that only the people they choose can read other communications or their e-mail, review their medical records, or take money out of their bank accounts. Plain and simple, encryption products protect consumers.

Over the past couple of years, we have seen the power of Internet commerce. From amazon.com to eBay to drugstore.com, companies with a dot com have become the darlings of the investment world. For consumers, online commerce provides viable competition and, thus, a cost-effective alternative to traditional brick-and-mortar stores.

The Internet, however, will never achieve its full potential as a center of commerce if consumers do not trust that their transactions and communications remain confidential. If we ever are to realize the commercial and communications potential of the Internet, we must have sophisticated and effective encryption.

For these precise reasons, consumers have an economic interest in the use of strong encryption technology. That economic interest necessitates more research and more development of stronger technology. The current export control climate, however, stifles development of domestic encryption technology. I believe that expansion of the market for U.S. developers will serve to quicken the pace of innovation.

Two recent reports bear this out. The Electronic Privacy Information Center found that the United States is virtually alone in its restrictions on encryption. Another report by researchers at George Washington University found that 35 foreign countries manufacture 805 encryption products. The same GWU report found that of the 15 algorithms now being considered by

the National Institute of Standards for a new American encryption standard, 10 have been developed outside the U.S. Clearly, our outdated policies are doing more to exclude U.S. manufacturers from the marketplace than they are doing to keep encryption technology out of the hands of criminals.

I do not mean to belittle the serious law enforcement implications of encryption. As the FBI has stated, "encryption has been used to conceal criminal activity and thwart law enforcement efforts to collect critical evidence needed to solve serious and often violent criminal activities." The same technology that prevents a computer hacker from stealing one's credit card number can prevent a law enforcement officer, even one with a properly obtained court order, from decrypting illegal information.

But the fact of the matter is that criminals simply can purchase and use an advanced encryption product produced in a foreign country. I understand concerns that some in the law enforcement community may have. Muzzling American development and export, however, is a doomed strategy. I believe there should be criminal penalties for those that use encryption in the furtherance of a crime and I hope the Senate will adopt penalties similar to those found in the leading House encryption bill.

Mr. President, there is no question that this bill moves us forward, both in terms of privacy and technological innovation. I must point out, however, that my support for this bill will not preclude me from advocating a stronger privacy position in the future. My cosponsorship of this bill establishes what I believe should be the starting point for the Congress to begin the encryption debate. I look forward to working with my colleagues on this very important issue.

I yield the floor.

---

#### MESSAGES FROM THE PRESIDENT

Messages from the President of the United States were communicated to the Senate by Mr. Williams, one of his secretaries.

#### EXECUTIVE MESSAGES REFERRED

As in executive session the Presiding Officer laid before the Senate messages from the President of the United States submitting sundry nominations which were referred to the appropriate committees.

(The nominations received today are printed at the end of the Senate proceedings.)

---

#### REPORT OF THE NOTICE OF THE CONTINUATION OF THE IRAQI EMERGENCY—MESSAGE FROM THE PRESIDENT—PM 50

The PRESIDING OFFICER laid before the Senate the following message