23 October 1997
Source: http://www.access.gpo.gov/su_docs/aces/aaces002.html

[Congressional Record: October 21, 1997 (Senate)]
[Page S10879-S10881]
From the Congressional Record Online via GPO Access
[wais.access.gpo.gov]
[DOCID:cr21oc97-213]

ENCRYPTION

Mr. LOTT. Mr. President, I would like to report to my colleagues on the activities in the House to establish a new export policy on encryption. This is an issue that is still at the top of my list of legislation I hope this Congress can resolve within the next 2 months. The House's actions last month turned a spotlight on how this issue should ultimately be resolved.

Let me briefly review the issue. Encryption is a mathematical way to scramble and unscramble digital computer information during transmission and storage. The strength of encryption is a function of its size, as measured in computer bits. The more bits an encryption system has, the more difficult it is for someone else to illegally unscramble or hack into that information.

Today's computer encryption systems commonly used by businesses range from 40 bits in key length to 128 bits. A good hacker, let's say a criminal or a business competitor, can readily break into a computer system safeguarded by a lower-technology 40-bit encryption system. On the other hand, the 128-bit encryption systems are much more complex and pose a significant challenge to any would-be hacker.

Obviously, all of us would prefer to have the 128-bit systems. And equally as important, we would like to buy such systems from American companies. Firms we can routinely and safely do business with. Foreign companies and individuals also want to buy such systems from American companies.

[[Page S10880]]

They admire and respect our technological expertise, and trust our business practices. The United States remains the envy of the world in terms of producing top-notch encryption and information security products.

However, current regulations prohibit U.S. companies from exporting encryption systems stronger than the low-end, 40-bit systems. A few exceptions have been made for 56-bit systems. Until recently, it has been the administration's view that stronger encryption products are so inherently dangerous they should be classified at a level equal to munitions, and that the export of strong encryption must be heavily restricted.

While we are restricting our own international commerce, foreign companies are now manufacturing and selling stronger, more desirable encryption systems, including the top-end 128-bit systems, anywhere in the world they want. Clearly, our policy doesn't make sense. Just as

clearly, our export policies on encryption have not kept up to speed with either the ongoing changes in encryption technology or the needs and desires of foreign markets for U.S. encryption products.

My intention is neither to jeopardize our national security nor harm law enforcement efforts. I believe we must give due and proper regard to the national security and law enforcement implications of any changes in our policy regarding export of encryption technology. But it is painfully obvious we must modernize our export policies on encryption technology, so that U.S. companies can participate in the world's encryption marketplace. The legislative initiative on this issue has always been about exports, but this summer that changed.

During the past month, the FBI has attempted to change the debate by proposing a series of new mandatory controls on the domestic sale and use of encryption products. Let me be clear. There are currently no restrictions on the rights of Americans to use encryption to protect their personal financial or medical records or their private e-mail messages. There have never been domestic limitations, and similarly, American businesses have always been free to buy and use the strongest possible encryption to protect sensitive information from being stolen or changed. But now, the FBI proposes to change all that.

The FBI wants to require that any company that produces or offers encryption security products or services guarantee immediate access to plain text information without the knowledge of the user. Their proposal would subject software companies and telecommunications providers to prison sentences for failure to guarantee immediate access to all information on the desktop computers of all Americans. That would move us into an entirely new world of surveillance, a very intrusive surveillance, where every communication by every individual can be accessed by the FBI.

Where is probable cause? Why has the FBI assumed that all Americans are going to be involved in criminal activities? Where is the Constitution?

And how would this proposal possibly help the FBI? According to a forthcoming book by the M.I.T. Press, of the tens of thousands of cases handled annually by the FBI, only a handful have involved encryption of any type, and even fewer involved encryption of computer data. Let's face it--despite the movies, the FBI solves its cases with good old-fashioned police work, questioning potential witnesses, gathering material evidence, and using electronic bugging or putting microphones on informants. Restricting encryption technology in the U.S. would not be very helpful to the FBI.

The FBI proposal won't work. I have talked with experts in the world of software and cryptography, who have explained that the technology which would provide compliance with the FBI standard simply does not exist. The FBI proposal would force a large unfunded mandate on our high technology firms, at a time when there is no practical way to accomplish that mandate.

Rather than solve problems in our export policy, this FBI proposal would create a whole new body of law and regulations restricting our domestic market.

This and similar proposals would also have a serious impact on our foreign market. Overseas businesses and governments believe that the U.S. might use its keys to computer encryption systems to spy on their businesses and politicians. Most U.S. software and hardware manufacturers believe this is bad for business and that nobody will trust the security of U.S. encryption products if this current policy continues. In fact, this proposal appears to violate the European

Union's data-privacy laws, and the European Commission is expected to reject it this week.

So, the FBI proposal would: Invade our privacy; be of minimal use to the FBI; would require nonexistent technology; would create new administrative burdens; and would seriously damage our foreign markets.

This is quite a list.

Mr. President, the FBI proposal is simply wrong. I have learned that even the administration does not support this new FBI proposal. So why does the FBI believe it must now subject all Americans to more and more surveillance?

This independent action by the FBI has created confusion and mixed signals which are troublesome for the Senate as it works on this legislation. Perhaps the FBI and the Justice Department need to focus immediately on a coordinated encryption position.

Mr. President, I congratulate the members of the House Commerce Committee for rejecting this FBI approach by a vote margin of more than 2 to 1.

I am sure all of my colleagues are sympathetic to the fact that emerging technologies create new problems for the FBI.

But we must acknowledge several truths as Congress goes forward to find this new policy solution. People increasingly need strong information security through encryption and other means to protect their personal and business information. This demand will grow, and somebody will meet it. In the long term, it is clearly in our national interest that U.S. companies meet the market demand. Individuals and businesses will either obtain that protection from U.S. firms or from foreign firms. I firmly believe that all of our colleagues want American firms to successfully compete for this business. Today there are hundreds of suppliers of strong encryption in the world marketplace. Strong encryption can be easily downloaded off the Internet. Even if Congress wanted to police or eliminate encryption altogether, I am not sure that is doable.

So, let's deal with reality. Clamping down on the constitutional rights of American citizens, in an attempt to limit the use of a technology, is the wrong solution. The wrong solution. This is especially true with encryption technology because it has so many beneficial purposes. It prevents hackers and espionage agents from stealing valuable information, or worse, from breaking into our own computer networks. It prevents them from disrupting our power supply, our financial markets, and our air traffic control system. This is scary--and precisely why we want this technology to be more available.

Only a balanced solution is acceptable. Ultimately, Congress must empower Americans to protect their own information. Americans should not be forced to only communicate in ways that simply make it more convenient for law enforcement officials. This is not our national tradition. It is not consistent with our heritage. It should not become a new trend.

Mr. President, I would like to establish a framework to resolve this difficult issue. I hope to discuss it with the chairmen and ranking members of the key committees. I especially look forward to working with the chairman of the Commerce, Science and Transportation Subcommittee on Communications, Senator Burns. He was the first to identify this issue and try to solve it legislatively. His approach on this issue has always been fair and equitable, attempting to balance industry wants with law enforcement requirements.

I believe there are other possible ideas which could lead to a consensus resolution of the encryption issue. It is my hope that

industry and law enforcement can come together to address these issues, not add more complexity and problems. The bill passed by the House Commerce Committee included a provision establishing a National Encryption Technology Center. It

[[Page S10881]]

would be funded by in-kind contributions of hardware, software, and technological expertise. The National Encryption Technology Center would help the FBI stay on top of encryption and other emerging computer technologies. This is a big step. This is a big step in the right direction.

It is time to build on that positive news to resolve encryption policy.

Mr. President, there is an op-ed piece which appeared in the Wall Street Journal on Friday, September 26. It is well written and informative, despite the fact that its author is a good friend of mine. Mr. Jim Barksdale is the president and CEO of Netscape Communications and is well-versed in encryption technology. Mr. Barksdale's company does not make encryption products; they license such products from others. They sell Internet and business software and, as Jim has told me many times, his customers require strong encryption features and will buy those products either from us or foreign companies.

Again, let's deal with reality. The credit union manager in Massachusetts, the real estate agent in Mississippi, the father writing an e-mail letter to his daughter attending a California university, each want privacy and security when using the computer. They will buy the best systems available to ensure that privacy and security. And, in just the same way, the banker in Brussels, Belgium, the rancher in Argentina, and the mother writing e-mail to her daughter in a university in Calcutta, India, each of these people also want privacy and security. They also will buy the best systems available to ensure that privacy and security. And they want encryption systems they trust--American systems. That's what this debate is about.

Mr. President, if Congress does not modernize our export controls, we run the real risk of destroying the American encryption industry. And we risk giving a significant and unfair advantage to our foreign business competitors.
