

the fungus called scab. In other parts of the country, it has been hurricanes.

The combined result is a farm crisis worse than anything we have seen since I have been in public life. I have been in public life now for over 20 years.

Mr. President, I hope when we return that we are ready to aggressively address this problem. What we did tonight will help. It is not new money. It just moves money forward. That will be of some assistance. But it in no way solves the problem. We have a crisis of staggering dimensions, and it requires our full response.

I thank the Chair. I yield the floor.

I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The legislative clerk proceeded to call the roll.

Mr. JEFFORDS. Mr. President, I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER (Mr. ENZI). Without objection, it is so ordered.

Mr. JEFFORDS. Mr. President, we are now in the closing process for the evening, and we have several matters to be considered.

MORNING BUSINESS

Mr. JEFFORDS. Mr. President, I ask unanimous consent that there now be a period for the transaction of morning business.

The PRESIDING OFFICER. Without objection, it is so ordered.

MEDIA CAMPAIGN HELPS INFORM CONGRESSIONAL ACTION ON ENCRYPTION

Mr. LOTT. Mr. President, I rise to recognize the continuing efforts of Americans for Computer Privacy (ACP), a broad-based advocacy coalition, to energize the discussion now taking place in Washington on encryption. ACP has a role since they represent industry, private citizens and interest groups from all sides of the political spectrum. The computer industry believes, as do many members in both the House and Senate, that it is time to reform America's outdated encryption regime. Last week, an important step was taken when a multimedia campaign was launched to raise Congressional and public awareness on the encryption issue. This campaign includes television commercials, print media, and an online banner component with such statements as, "would you give the government the keys to your safety deposit box or home." In the past few days, television commercials highlighting the need for encryption reform have appeared during Good Morning America, the Today show, Hardball, and Cross Fire.

Mr. President, ACP has an impressive membership which includes such organizations as the Law Enforcement Alliance of America, the Louisiana Sher-

iff's Association, American Small Business Alliance, Americans for Tax Reform, Electronic Commerce Forum, Information Technology Industry Council, the National Association of Manufacturers, the U.S. Chamber of Commerce, and over sixty technology companies. It's bipartisan advisory panel includes several intelligence and law enforcement experts such as former National Security Advisor Richard Allen, former NSA Deputy Director William Crowell, former CIA Director John Deutch, former FBI Director William Webster, and former San Jose Police Chief Joseph McNamara. This array adds credibility to their message.

As you are well aware, encryption plays a significant role in our daily lives. This technology scrambles and unscrambles computer text to keep private communications from being read by unauthorized individuals such as hackers, thieves, and other criminals. Encryption protects private citizens credit card numbers when they buy something over the Internet, ensures that only authorized medical personnel can read a patients' medical records stored on a hospital database, shields tax information that we send to the IRS, and safeguards personal letters that we E-mail to loved ones. Encryption means that American companies can protect confidential employee information, such as salary and performance data; valuable trade secrets and competitive bidding information; and critical target market data.

Encryption also benefits America's security by protecting our nation's critical infrastructures, like the power grid, telecommunications infrastructure, financial networks, air traffic control operations, and emergency response systems. Strong encryption thwarts infiltration attempts by computer hackers and terrorists who have destructive, life threatening intent.

Yes, this is an issue that truly affects all Americans.

By allowing a public policy that limits encryption to continue, we risk sending more potential U.S. business overseas. This approach only serves to harm America's economic and national security interest by encouraging criminals to purchase foreign made products now widely available with unlimited encryption strength. By contrast, the broad development and use of American encryption products should be advantageous to our law enforcement and intelligence communities.

I must say that I am deeply troubled by the comments made by Commerce Under Secretary William Reinsch, head of the Bureau of Export Administration, in response to ACP's efforts. Apparently, Under Secretary Reinsch doubts that this initiative will work—that industry and privacy advocates are wasting their money. I disagree. This media campaign is rightfully educating the public about the importance of encryption in our every day lives. These advertisements make clear that encryption technology preserves our

First Amendment right to freedom of speech and our Fourth Amendment freedom against unreasonable search and seizure. They illustrate that we need strong security to keep all Americans safe from infrastructure attack. And they explain that Americans and computer users everywhere must feel confident in the knowledge that their private information will remain private. Clearly, the development and use and strong encryption is critical if Internet commerce is going to grow to its full potential and sustain the economic engine that is driving this country into the 21st century.

I believe this advertising campaign is yet another indication of industry's willingness and desire to find a reasonable solution to the encryption issue. Industry and privacy groups, for example, have been working in earnest with Administration officials for several months. In May, a proposed interim solution to the encryption issue was offered. The Administration responded that it would take five to six months to review the proposal. This reaction in conjunction with Under Secretary Reinsch's recent comments, lead many in Congress, from both sides of the aisle, to conclude that the Administration, despite what it has been saying publicly, does not want to see a balanced resolution before this Congress adjourns.

Mr. President, I think it is also important to reiterate that the Administration's restrictions against U.S. encryption exports and its proposals to control domestic use just cannot work. Innovation in the high tech industry is relentless and ubiquitous. The government cannot stop it. It is for this reason that industry is trying to persuade the Administration that innovation is the solution to this issue, not the enemy. Two weeks ago, a coalition of thirteen companies proposed "private doorbells", a technology solution that would provide law enforcement with court approved access to computer messages. Clearly, industry leaders want to help officials capture criminals and terrorists. I believe the ideas they have put forward are reasonable and responsible. On the other hand, I do not believe the Administration's response has been forthcoming. Encryption policy can be modernized with the stroke of a pen, but the Administration has shown little willingness. Thus, industry takes appropriate action by implementing a media campaign.

While encryption is a complex and divisive information technology issue, this media initiative reinforces the need for legislation to bring America's encryption policy into the 21st century. The national security and law enforcement communities have legitimate concerns that must be considered. I believe that the best way to deal with these concerns is to pass during this Congress legislation that strikes a balance on encryption. Legislation that would help keep private and corporate communications away from