regulation for the voluntary labeling or identification of ground beef or lamb, other processed beef or lamb products as United States beef or United States lamb, imported beef or imported lamb, beef blended with imported meat or lamb blended with imported meat, or other designation that identifies the percentage content of United States and imported beef or imported lamb contained in the product, as determined by the Secretary.

''(2) MANDATORY LABELING.—

''(A) IN GENERAL.—Except as provided in subparagraph (B), not later than 18 months after the date of enactment of this subsection, the Secretary shall provide by regulation for the mandatory labeling or identification of ground beef or lamb, other processed beef or lamb products as United States beef or United States lamb, imported beef or imported lamb, beef blended with imported meat or lamb blended with imported meat, or other designation that identifies the percentage content of United States and imported beef or imported lamb contained in the product, as determined by the Secretary.

''(B) APPLICATION.—Subparagraph (A) shall not apply to the extent the Secretary determines that the costs associated with labeling under subparagraph (A) would result in an unreasonable burden on producers, processors, retailers, or consumers.''.

(c) GROUND BEEF AND GROUND LAMB LABELING STUDY.—

(1) IN GENERAL.—The Secretary of Agriculture shall conduct a study of the effects of the mandatory use of imported, blended, or percentage content labeling on ground beef, ground lamb, and other processed beef or lamb products made from imported beef or imported lamb.

(2) COSTS AND RESPONSES.—The study shall be designed to evaluate the costs associated with and consumer response toward the mandatory use of labeling described in paragraph (1).

(3) REPORT.—Not later than 1 year after the date of enactment of this Act, the Secretary shall report the findings of the study conducted under paragraph (1) to the Committee on Agriculture of the House of Representatives and the Committee on Agriculture, Nutrition, and Forestry of the Senate.

SEC. 803. REGULATIONS.

Not later than 120 days after the date of enactment of this Act, the Secretary of Agriculture shall promulgate final regulations to carry out the amendments made by this title.

Mr. COCHRAN. Mr. President, I move to reconsider the vote by which the amendments were agreed to.

Mr. BUMPERS. I move to lay that motion on the table.

The motion to lay on the table was agreed to.

Mr. HATCH. Mr. President, as I am sure my distinguished colleague, the Chairman of the Subcommittee, is aware, the Food and Drug Administration Modernization Act (FDAMA) included a significant provision related to FDA's review and approval of indirect food additives. For the benefit of my colleagues, these are products that are used for containers, wrappings and packaging of food products.

To ensure the safety of indirect food additives, these materials that touch or contain food, the Food and Drug Administration (FDA) must receive safety data submitted by the manufacturer. Often, FDA's process of evaluating these data has been extremely lengthy and has worked to delay the market availability of new and improved products. As a result, many companies have chosen simply not to bring new products to market, thus depriving the public of improvements in products and technology.

In order to address this concern, a provision was included in FDAMA which requires the FDA to establish a new and expedited new product notification and review process that will substantially improve the situation for manufacturers of indirect food additives and thus the consumers of packaged food products. However, under section 309 of FDAMA, the provision will only become effective if the FDA receives an appropriation of $1.5 million for FY 1999. Subject to this new appropriation, FDA would be required to set the program in motion by April 1, 1999.

I am aware that the House mark does include funding for the indirect food additive pre-market notification program, but at a level of $500,000. While this certainly indicates the intention and willingness of the House to fund the program, unfortunately the amount is not sufficient to meet the specific requirements of FDAMA.

I am extremely mindful of the tight allocation under which S. 2159 was crafted, and I recognize that it was not an easy task to bring this bill forward today. I am very grateful for the Subcommittee's efforts under the leadership of Chairman COCHRAN. At the same time, I hope the Chairman will agree with me that funding of this important FDA reform is critically important and that the conferees will try to work this out so that the new program can be implemented next year.

Mr. COCHRAN: The Committee was mindful of this problem, and, in fact, included report language indicating its awareness of the need to implement the premarket notification provisions in order to spur innovation of new and improved food packaging materials. As you said, we are operating under a very tight allocation, but we will do our best to try to work this out.

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

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

The Senator from Mississippi.

MORNING BUSINESS

Mr. COCHRAN. Mr. President, I ask unanimous consent that there now be a period for the transaction of routine morning business, with Senators permitted to speak for up to 10 minutes each.

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

Mr. COCHRAN. Mr. President, I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The assistant legislative clerk proceeded to call the roll.

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

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

CONGRESS NEEDS TO ACT ON ENCRYPTION LEGISLATION

Mr. LOTT. Mr. President, I rise to commend the continuing efforts of America's computer industry to find a technical solution to the encryption issue. On Monday, July 13, a consortium of thirteen high-tech companies announced an alternative to the Administration's proposed key escrow/third party access system. As you will recall, many computer and security exports have stated that key escrow would be an invasion of privacy, technically unworkable, and cost prohibitive.

Unlike the key recovery system advocated by the Administration, industry's ''private doorbells'' approach would not require sensitive encryption keys to be escrowed with third parties in order for law enforcement to gain access to computer messages. Instead, the FBI and other federal, state, and local agencies would be able to combat crime by being provided with court approved, real-time access to communiques at the point where they are sent or at the point where the message is received. Clearly, high-tech executives have not been sitting on the sidelines as the encryption debate continues. As this announcement indicates, the computer industry is working hard to find a balanced solution that ensures the needs of our law enforcement and national security communities while maintaining privacy protections for all U.S. citizens. We owe it to them, and to all Americans, to find a balanced legislative solution to encryption.

Mr. LEAHY. Mr. President, I would also like to applaud the computer industry's efforts to find alternative technical solutions to help law enforcement with the challenge of encrypted data and communications without the need to establish a government-mandated key escrow or key recovery scheme. With the appropriate privacy safeguards in place, as outlined in the E-PRIVACY bill, S.2067, the solution that the companies are proposing appears encouraging. American companies are desperate for a common sense approach to our export policy on encryption. As you are well aware, the Administration, starting with Clipper Chip, has been wedded to key escrow schemes to ensure that the FBI can get access to plaintext, or unscrambled electronic data. This path has been pursued despite the serious questions that experts have raised about the costs, privacy risks and lack of consumer interest in such schemes. As

U.S. companies watch their market share for computer hardware and software products erode because of our country's outdated export controls on encryption, it is imperative that the Administration direct the FBI to consider creative alternatives to key escrow.

Mr. CRAIG. The recent announcement by several leading companies in the computer industry makes it clear that, in addressing both economic and law enforcement concerns, it is important to find a balance between the two. We must create legislation that addresses consumer demand for encrypted products while also meeting the needs of law enforcement—legislation that fosters a global marketplace dominated by U.S. encryption products. Those products, of course, will be a great benefit to our national security.

Mr. BURNS. Industry's plan to allow law enforcement access to the plaintext of some encrypted communications demonstrates that market solutions can truly address many areas of law enforcement's concerns with encryption. At the same time, we should not forget that there is a continuing need for legislative privacy protections governing how and when law enforcement should have access to encrypted data.

Mr. LEAHY. I agree, the announcement by the high-tech companies of alternative means of access to plaintext to encrypted data demonstrates industry's commitment to find solutions that accommodate law enforcement interests. It also reiterates the need for privacy protection legislation to ensure that law enforcement only gets such access with a proper court order. The E-PRIVACY bill, S. 2067, which I have sponsored with Senator ASHCROFT, and others, would provide that privacy protection.

Mr. BURNS. Yes, these recent developments continue to highlight the desperate need for a change in U.S. encryption policy. Last week the Administration announced it would make exceptions in encryption export policy allowing banks and certain financial institutions to export strong encryption, without vulnerable key recovery systems, to their subsidiaries in a select group of 40 countries. This is a welcome development for those companies that will qualify for this narrow exception but it does not provide the same protection of online privacy for everyday Americans.

Mr. LOTT. Americans want and need strong encryption to protect their most sensitive data and communications from unauthorized access. Yet the Administration continues to pursue an encryption policy that limits exports, requires key recovery backdoors for law enforcement, and ultimately stifles American innovation. Instead of keeping technology out of the hands of criminals, continuing export controls will only ensure that U.S. citizens have less protection than other computer users throughout the globe. The financial institutions announcement confirms what many in Congress have been saying for some time: users of electronic commerce will be best served by providing relief from current export control regulations. Allowing advanced encryption to be exported ensures that sensitive data is protected while helping American companies compete globally. Individual consumers, as well as multinational financial institutions, will not buy and will not use encryption systems when government mandated recovery keys for these products are provided to third parties. This system, as many experts have reported, creates a host of security risks, making our online communications vulnerable to attack by thieves, hackers and other criminals.

Mr. CRAIG. From an economic standpoint, foreign companies are winning an increasing number of contracts because consumers are unwilling to buy products that ensure third party access or require that keys be stored with government certified or operated facilities. This is particularly true since they can buy stronger encryption overseas from either foreign-owned companies or American owned companies on foreign soil. We must act quickly and prudently in addressing this problem.

Mr. ASHCROFT. Mr. President, for several years we have debated, argued and discussed the real economic impact of continuing to follow the Administration's wrong-headed policy on encryption. In addition to the Administration, several members of Congress on both sides of the aisle have refused to consider many of the facts of encryption technology and the importance of the technology sector to our robust economy. After all these years, we have an historical opportunity to debate encryption on the floor of the U.S. Senate.

Mr. CRAIG. I agree. With the rapid expansion of the ''super highway'' and Internet commerce, it is crucial we bring encryption legislation to the forefront. A secure, private and trusted national global information infrastructure is essential to promote citizens' privacy and economic growth.

Mr. LEAHY. Encryption technology is not only a critical tool for protecting the confidentiality of our online communications and the privacy of our stored electronic information, it is also the building block for digital signatures. The future of electronic commerce requires that parties conducting business online be able to trust the authenticity of the contracts they enter and that the parties with whom they are dealing are who they say they are. In fact, a number of States, including my own State of Vermont, are making progress on crafting the rules for digital signatures and online commercial transactions.

Mr. BURNS. Encryption is also an essential part of new ''digital signature'' techniques used to identify parties and authenticate transactions online. These techniques are widely viewed as an essential feature of electronic commerce. The use of digital signatures raises complex business and privacy issues, but these issues are completely separate from the questions raised by encryption used for confidentiality. There is a great deal of ongoing activity in the private sector and at the state level attempting to sort out these complex issues of business use and consumer protection. Federal digital signature legislation is clearly needed, but should be dealt with separately from encryption reform legislation.

Mr. ASCHROFT. As in everything regarding the topic of encryption, we face some decisions and difficulties. Some would like to weigh down the already contentious issue of encryption with other unrelated issues, such as digital signatures. Now, at first blush, many may believe that these two issues are fundamentally tied, or that one necessarily raises the other. However, this is not true. While digital signature products may use some sort of encryption, they are not encryption. The potential debate on federal level digital signature legislation is a worthy debate, the nuances of what potential legislation may look like are many, and the differences in arguments regarding digital signatures and encryption are great.

Mr. LEAHY. These are important issues that can and should be addressed separately from the immediate need for encryption legislation that protects privacy and confidentiality.

Mr. ASHCROFT. I have heard that some object to even allowing for encryption and digital signature legislation to reside in different pieces of legislation, even if both were brought to the floor. They express their concern that without the inclusion of digital signatures that public networks cannot be adequately secure. This argument gives me great pause, mainly because it demonstrates a fundamental misconception of a digital signature. A digital signature does not secure the network but rather secures the signature. Applying the same logic to the analog world would dictate that contracts could not be written until we could adequately solve for the potential of forgeries. Obviously, we have not taken this approach yet individuals enter into millions of contracts every year.

Mr. LEAHY. While digital signature legislation at the Federal level may help encourage the development of online commercial transaction rules, we must be careful not to stifle the development of efficient and inexpensive digital signature services by prematurely regulating —or granting Federal agencies unfettered authority to regulate—in this area. We must particularly avoid creating a federal system for digital signatures that will become the national i.d. card for cyberspace. The Administration in its ''Framework for Global Electronic Commerce'' got it right when it said that ''participants in the marketplace—including consumers, business,

financial institutions, and on-line service providers—should define and articulate most of the rules that will govern electronic commerce.''

Mr. ASHCROFT. All that said, encryption and digital signatures do not and should not be joined in the same legislation. The opportunity we have before us is to bring the encryption debate into the open and to pass legislation that adequately addresses the concerns of law enforcement, national security, privacy, and system security.

Mr. ABRAHAM. At the same time, we have the opportunity to affect real growth in digital signature technologies by addressing digital signature as a separate piece of legislation during this Congress. We should not allow differences in encryption policy to stifle innovation and improvements in this exciting technology. Digital signature is crucial to ensuring the continued dynamic growth of electronic commerce in this country. Many in Congress recognize this, industry recognizes this, and the Administration agrees.

Mr. CRAIG. In order to pass legislation in a timely manner it is important that it be in a clean bill with only the most essential language related to encryption; language that seeks to protect individual privacy, while at the same time addressing national security and law enforcement concerns.

Mr. SHELBY. Mr. President, I rise because I have concerns about efforts to ease or remove export restrictions on certain hardware and software encryption products. Export controls on encryption and on other products serve a clearly defined purpose—to protect our nation's security. The Intelligence Committee believes that the effects on U.S. national security must be the paramount concern when considering any proposed change to encryption export policy, and the Committee will seek referral of any legislation regarding encryption export policy under its jurisdiction established under Senate Resolution 400. With our on-going investigation into the possible technology transfers to China, the Vice Chairman and I are also concerned that any effort to change U.S. export policy on encryption be consistent with the export policy review included in our investigation.

Export restrictions on encryption products assist the Intelligence Community in its signals intelligence mission. By collecting and analyzing signals intelligence, U.S. intelligence agencies seek to understand the policies, intentions, and plans of foreign state and nonstate actors. Signals intelligence plays an important role in the formation of American foreign and defense policy. It is also a significant factor in the U.S. efforts to protect its citizens and armed forces against terrorism, the proliferation of weapons of mass destruction, narcotics trafficking, international crime and other threats to our nation's security.

While the Committee recognizes the commercial interest in easing or removing export restrictions, it believes the safety of our citizens and armed forces should be the predominant concern when considering U.S. policy towards the export of any product. The Committee supports the continued control of encryption products, and believes that a comprehensive strategy on encryption export policy can be developed that addresses national security concerns as well as the promotion of American commercial interests abroad.

I look forward to working with Senator LOTT and others as legislation moves through the Senate.

Mr. ASHCROFT. The bottom line to all of this is that we can move encryption legislation in this Congress, with the support of the majority leader. To hold up this progress works against national security, works against support of our law enforcement and erodes individual's privacy protections. We should all diligently work to craft an encryption bill that can come to the floor this session.

Mr. LOTT. I agree with my colleagues. While I strongly support the passage of legislation on both encryption and on digital signatures, I am convinced that the best approach during this session is to deal with these matters in separate bills. Let me say again, that in order to pass legislation on both of these issues during this Congress, we must recognize that there are significant differences between these important and complex policy issues. Digital signature and certificate authority have appeared in various proposals in association with encryption. However, these matters need to be considered separately because they raise different questions and complications.

A digital signature is a technical method for authenticating the identity of a sender or author.

As its name implies, it is a digital version of a person's written signature. Encryption is a means to ensure confidentiality. It is a set of algorithms used to scramble and unscramble text in order to keep unauthorized person's from reading your computer data and messages. It is a technology that protects medical, business, and individual files from invasion. Again, encryption for confidentiality, and digital signatures for authentication and related certificate authorities, are not the same issue. Dealing with encryption and digital signatures in one piece of legislation could lead to the demise of such a weighted bill. Consequently, I am prepared and committed to moving separate bills dealing with these issues during this session. I urge my colleagues to support this dual track approach as my colleagues have recommended. I share the belief that this is the best chance for legislation to be passed in both of these areas during the 105th Congress.

Congress needs to stop debating these issues and enact balanced legislation that will ensure the privacy rights of individuals while protecting America's public safety, economic, and national security interests.

Mr. BURNS. I commend the Majority Leader and Senators LEAHY, CRAIG, ASHCROFT, ABRAHAM, and SHELBY for their continuing hard work and vision on these difficult but critical issues. I hope we will be able to move forward legislatively on both encryption reform and digital signatures this session.

HAPPY BIRTHDAY, MAX FISHER

Mr. LOTT. Mr. President, I am always reluctant to add another national holiday to our calendar, but were we to do so, then July 15 would be a good bet. For today is Max Fisher's birthday.

In fact, it is his 90th birthday. But longevity, important as it is, is the least of his accomplishments.

Many of our colleagues, from both sides of the aisle, know Max very well. He has long been one of the most prominent and influential leaders in the American Jewish community.

He has advised every Republican President since Richard Nixon. He has advised every Israeli Prime Minister since Golda Meir. He was a critical force behind the airlift that helped save Israel in the darkest days of the 1973 Yom Kippur War.

The great work of his life has been building bridges between Israel and the United States. But that is only one of many reasons to honor him.

Max is one of our Nation's greatest philanthropists. He played a vital role in his home city of Detroit after the tragic riots of 1967 by promoting reconciliation and economic opportunity. He continues in that effort today.

No one will ever know how many people have benefited from his quiet generosity.

Max, of course, would prefer the term social responsibility. Whatever the words, the meaning is the same, and so is the inspiration. As the Book of Proverbs teaches, ''He who is gracious to the poor lends to the Lord.''

Ten years ago, when Max celebrated his eightieth birthday, accolades came in from around the world. President Reagan called him ''a legend.''

Today, ten years later, the legend continues to build. He still works quietly, behind the scenes.

It is no coincidence that his biography is entitled, ''The Quiet Diplomat.'' That book documents what all of his friends and admirers know so well: His dedication to the cause of peace, his energy in the cause of justice, his wisdom and effectiveness in working for a better world.

At some point, with a man like Max, we run out of accolades. He has heard them all—and probably been impressed by none of them.

His eye is always on the future: What remains to be done, what is still to be built, what has not yet been set right.

In that spirit, on behalf of the Senate of the United States, I want to wish