divulged that he had not been discussing export controls, he had been talking about domestic controls on encryption designed by Americans for Americans. Mr. Freeh and his 80 lobbyists apparently never thought to bring this up so that it could be part of the Judiciary Committee's hearings on the legislation from the very beginning.

Why? Perhaps he knew the reception he would receive to the proposal that Americans should no longer be able to design, manufacture or import encryption unless the encryption technique ensured that a government approved third party could have access to the information without the user's knowledge. Thus, he would prefer that every time an American encrypts information to store it on a computer or to send it over the Internet, a third party must be able to access the information and the user would never know that the information had been accessed. This would change over 200 years of free speech.

IMPACT OF REQUIRING FBI'S PROPOSED DOMESTIC CONTROLS

I am a strong proponent of law enforcement. But I do not believe that we should adopt a system that our best and brightest say will be nearly impossible to design, hard to keep secure and probably very costly to consumers.

To my knowledge, no one has ever built or even begun to test the reliability, security, and costs of such a system. I have seen a report by another group of extremely well-known American scientists who tell me that they have no idea of how to design and implement this proposed domestic key recovery system. They also say that such a system could create greater vulnerability for its users. Apparently encryption techniques are not foolproof, and adding sufficient complexity to permit third party access will make the encryption even less secure. It also appears to be highly dependent upon the honesty and integrity of those third parties who have access to the information. Who, ultimately, do we trust?

I understand that while advances in technology have generally provided the FBI and other law enforcement with more investigatory tools, this one advance may make it more difficult for them. I propose instead that we look at methods that will help law enforcement to combat these new hurdles, rather than choosing the more simplistic approach of building law enforcement access into each and every encryption product.

I also can only image the bureaucracy necessary to handle the magnitude of information regarding encryption keys. It would have to rival many agencies we have spent years trying to reduce in size—the Internal Revenue Service and the Department of Commerce to name just a few.

While we are expending all of our efforts trying to lessen government intrusion in our lives, domestic encryption controls as proposed by Mr. Freeh would create probably the largest intrusion yet.

Finally, I have a basic concern about requiring American citizens to provide access to their information if they decide to encrypt it. If I write a letter in the privacy of my own home and leave it in my desk drawer, I do not have to provide a copy of my house key and desk drawer key with the local police so that they may look at it easily without my knowledge. I do not see why this should change if I write this letter on my computer and decide to encrypt it. Why should this act require me to let others have the capability of viewing it without my knowledge? I agree with the constitutional law professors who stated that this would have a ''chilling effect'' on American speech.

FOREIGNERS SIMPLY WILL NOT PURCHASE AND CRIMINALS WILL NOT USE AMERICAN DESIGNED MANDATORY KEY RECOVERY ENCRYPTION PRODUCTS

Ultimately, foreigners will not purchase or use American encryption products if they provide mandatory third party access to information. Neither will criminals. They know that the encryption technique is strongly desired by American law enforcement because law enforcement can monitor or otherwise access the information. Why would they voluntarily use such a product when they can use a 128-bit product they can obtain today over the Internet from tens of countries.

The FBI alleges that all foreign governments are eager to adopt similar controls on their citizens. While this is true of France, it is not true of the European Union for example, which categorically rejected the administration's proposal for a worldwide key recovery infrastructure requirement.

The only impact of the FBI proposal is that normal, law abiding American citizens will use American designed encryption programs. Foreigners will turn to foreign sources for their nonkey recovery products, and criminals will certainly turn to the same foreign sources. Thus, the FBI proposal does not address the real problem created by encryption technology. I do not want to put in place a large, costly bureaucracy that will not permit law enforcement to bet the information it believes necessary.

WHAT IS BEST FOR AMERICA

The United States should not try to control the export of something that by its very nature is uncontrollable. The United States should also not take a lead in forcing its citizens to adopt a costly technology that will insure easy monitoring and intrusion by law enforcement. Our constitutional guarantees of free speech and our rights to privacy should not be in any way lessened in order to accomplish Louis Freeh's desire for a fourth amendment for the 21st century. We in Congress should act now to relax export controls on encryption technology and to ensure that Americans remain free to speak in whatever manner they desire, using whatever encryption they choose.

INTRODUCTION OF LEGISLATION REQUIRING PEER REVIEW IN OSHA RULEMAKING

HON. CASS BALLENGER

OF NORTH CAROLINA

IN THE HOUSE OF REPRESENTATIVES

Friday, November 7, 1997

Mr. BALLENGER. Mr. Speaker, today I am introducing legislation to require that future occupational safety and health standards be subject to peer review as part of the rulemaking process.

Part of the Clinton Administration's promise to reinvent OSHA was the commitment to commonsense regulations. Whatever else that might mean, surely it must mean that such regulations are based on sound science.

The congressionally mandated Presidential-Congressional Commission on Risk Assessment and Risk Management said this about peer review in its recent report: ''Peer review is an important and effective mechanism for evaluating the accuracy or appropriateness of technical data, observations, interpretations, and the scientific and economic aspects of regulatory decisions. Peer review should provide balanced, independent views. When used well, peer review can serve as a system of checks and balances for the technical aspects of the regulatory process'' (Risk Assessment and Risk Management in Regulatory Decision-Making, Volume 2, page 103).

While other Federal regulatory agencies have adopted politics on peer review of major regulatory actions, OSHA has not adopted such a policy and only rarely has conducted peer review in conjunction with regulations. A draft policy circulated near the end of the Bush administration, was left unfinished and never implemented by the Clinton administration.

It will no doubt be alleged by some that requiring peer review is intended to delay or draw out the rulemaking process. In fact, peer review can prevent OSHA from errors that can save years of controversy and litigation. As the Presidential-Congressional Commission on Risk Assessment and Risk Management noted: ''An open process of sharing the findings and conclusions from peer review can increase the credibility of a risk assessment and stakeholders confidence in the conclusions. Peer review might even be useful in the first stage of putting a problem in context, drawing in experienced health officials and researchers'' (Volume 2, page 103).

The legislation generally requires that peer review be part of OSHA's rulemaking process. However, where the rule is adopted through negotiated rulemaking, conducted in accordance with the Negotiated Rulemaking Act which insures that affected persons are adequately represented in the negotiations, a separate peer review of the scientific and economic basis for the standard is not required.

Mr. Speaker, I look forward to working with my colleagues in adopting this important legislation.

CONGRATULATION TO STANTON J. BLUESTONE

HON. THOMAS M. BARRETT

OF WISCONSIN

IN THE HOUSE OF REPRESENTATIVES

Friday, November 7, 1997

Mr. BARRETT of Wisconsin. Mr. Speaker, today, I ask the House to join me in congratulating Stanton J. Bluestone the 1997 recipient of the American Jewish Committee's Institute of Human Relations award.

Stanton started in retail at Shillito's Department Store in Cincinnati, in 1957. His rise through the industry took Stanton and his family to New York, Illinois, Indiana, and finally Wisconsin. Today, as Chairman of the Board and CEO of Carson Pirie Scott & Co., Stanton Bluestone oversees a chain of 56 department stores from the company's Mulwaukee headquarters. Throughout his career, his creativity, his dedication, and his unique ability to bring out the best in his assocates have earned Stanton the respect of his coworkers and peers.

The AJC's Institute of Human Relations Award recognizes not only Stanton's personal