Congress all strongly support the basic intent of the Migratory Bird Treaty Act that our migratory bird resources must be protected from overexploitation. Sportsmen have consistently demonstrated their commitment to the wise use of renewable wildlife resources through reasoned management and enforcement of appropriate regulations.

Over the years, various prohibitions on the manner and methods of taking migratory birds have been embodied in regulations. Many of these prohibitions are decades old and have the support of all persons concerned with protecting migratory birds. In my judgment, it would be appropriate to incorporate these regulations in statutory law, and my proposed bill accomplishes that objective. This provision does not, however, restrict or alter the Secretary of the Interior's annual responsibilities to establish bag limits or duration of seasons. Nor does it prevent additional prohibitions, including hunting methods of migratory birds, from being implemented.

Second, a fundamental goal of the Migratory Bird Treaty Reform Act of 1997 is to address the baiting issue. Under my proposed legislation, no person may take migratory birds by the aid of bait, or on or over bait, where that person knew or should have known the bait was present. The provision removes the strict liability interpretation made first by a Federal court in Kentucky in 1939, and presently followed by a majority of Federal courts. With this provision, uniformity in the application of the prohibition is established.

As important, however, is the establishment of a standard that permits a determination of the actual guilt of the defendant. If the facts demonstrate that the hunter knew or should have known of the alleged bait, liability—which includes fines and potential incarceration—will be imposed. If by the evidence, however, the hunter could not have reasonably known that the alleged bait was present, liability would not be imposed and penalties would not be assessed. This would be a question of fact to be determined by the court based on the totality of the evidence presented.

Furthermore, the exceptions to baiting prohibitions contained in Federal regulations have been amended to permit exemption for grains found on a hunting site as a result of normal agricultural planting and harvesting as well as normal agricultural operations. This proposed change will establish reasonable guidelines for both the hunter and the law enforcement official.

To determine what is a normal agricultural operation in a given region, the U.S. Fish and Wildlife Service will be required to annually publish, in the Federal Register, a notice for public comment defining what is a normal agricultural operation for that particular geographic area. This determination is to be made only after meaningful consultation with relevant State and Federal agencies and an opportunity for public comment. Again, the goal of this effort is to provide uniformity and clarity for landowners, farmers, wildlife managers, law enforcement officials, and hunters so they know what a normal agricultural operation is for their region.

In addition, the proposed legislation permits the scattering of various substances like grains and seeds, which are currently considered bait, if it is done to feed farm animals and is a normal agricultural operation in a given area, as recognized by the Fish and Wildlife Service and published in the Federal Register.

Finally, the term bait is defined as the intentional placing of the offending grain, salt, or other feed. This concept removes from violation the accidental appearance of bait at or near the hunting venue. There have been cases where hunters have been charged with violating baiting regulations as a result of grain being unintentionally spilled on a public road, where foreign grain was inadvertently mixed in with other seed by the seller and later found at a hunting site, and where foreign grain was deposited by animals or running water. These are examples of actual cases where citations were given to individuals for violations of the baiting regulations.

Under my proposed legislation, the hunter would also be permitted to introduce evidence at trail on what degree the alleged bait acted as the lure or attraction for the migratory birds in a given area. In cases where 13 kernels of corn were found in a pond in the middle of a 300-acre field planted in corn or where 34 kernels of corn were found in a wheat field next to a freshwater river, the bait was clearly not the reason migratory birds were in the hunting area. First, it was not intentionally placed there and, second, it could not be considered an effective lure or attraction under the factual circumstances. These are questions of fact to be determined in a court of law. Currently, however, evidence of these matters is entirely excluded as irrelevant under the strict liability doctrine.

In 1934, Congress enacted the Migratory Bird Conservation Act as a mechanism to provide badly needed funds to purchase suitable habitat for migratory birds. Today, that need still exists, and my legislation will require that all fines and penalties collected under the MBTA be deposited into the Migratory Bird Conservation Fund. These funds are essential to the long-term survival of our migratory bird populations.

Finally, this measure proposes that personal property that is seized can be returned to the owner by way of a bond or other surety, prior to trial, at the discretion of the court.

Mr. Speaker, the purpose of the proposed Migratory Bird Treaty Reform Act is to provide clear guidance to landowners, farmers, wildlife managers, hunters, law enforcement officials, and the courts on what are the restrictions on the taking of migratory birds. The conflict within the Federal judicial system and the inconsistent application of enforcement within the U.S. Fish and Wildlife Service must be resolved. The proposed legislation accomplishes that objective without, in any manner, weakening the intent of current restrictions on the method and manner of taking migratory birds; nor do the proposed provisions weaken protection of the resource. Finally, the proposed legislation does not alter or restrict the Secretary of the Interior's ability to promulgate annual regulations nor inhibit the issuance of further restrictions on the taking of migratory birds.

Mr. Speaker, I urge my colleagues to carefully review the Migratory Bird Treaty Reform Act of 1997. It is a long overdue solution to several ongoing problems that regrettably continue to unfairly penalize many law-abiding hunters in this country.

TRIBUTE TO MONTEFIORE MEDICAL CENTER

HON. JOSÉ E. SERRANO

OF NEW YORK

IN THE HOUSE OF REPRESENTATIVES

Wednesday, February 12, 1997

Mr. SERRANO. Mr. Speaker, I rise today to pay tribute to Montefiore Medical Center for 50 years of caring in our Bronx community.

Mr. Speaker, this year, 1997, marks the 50th anniversary of the Montefiore Home Health Agency. Since its inception as the first hospital-based home health agency in the United States, Montefiore has cared for tens of thousands of patients.

Montefiore offers a variety of programs. The long term home health care program, provides a continuum of care at home to the chronically ill, who would otherwise require nursing home placement. The teleCare program provides 24-hour access to emergency assistance in the home. The certified home health agency provides short-term care to patients in the post-hospital period. Such programs have been vital to patients recovery and recuperation.

I would like to highlight the staff's devotion and energy in tending to the individual needs of each patient. Medical social workers provide unique and personal care. They teach patients how to use a variety of assistance devices. From nurses to occupational and physical therapists, these fine professionals are there when needed.

Montefiore and its home health care staff stand out in their field. Montefiore succeeds in dramatically improving patients' quality of life.

Mr. Speaker, let us join in the celebration of this milestone and acknowledge this outstanding agency for 50 years of accomplishment and service.

THE INTRODUCTION OF THE SECURITY AND FREEDOM THROUGH ENCRYPTION [SAFE] ACT

HON. BOB GOODLATTE

OF VIRGINIA

IN THE HOUSE OF REPRESENTATIVES

Wednesday, February 12, 1997

Mr. GOODLATTE. Mr. Speaker, today I am pleased, along with 54 of my colleagues, to introduce the Security And Freedom through *Encryption [SAFE] Act of 1997.*

This much-needed, bipartisan legislation accomplishes several important goals. First, it aids law enforcement by preventing piracy and white-collar crime on the Internet. It an ounce of prevention is worth a pound of cure, then an ounce of encryption is worth a pound of subpoenas. With the speed of transactions and communications on the Internet, law enforcement cannot possibly deal with pirates and criminal hackers by waiting to react until after the fact.

Only by allowing the use of strong encryption, not only domestically but internationally as well, can we hope to make the Internet a safe and secure environment. As the National Research Council's Committee on National Cryptography Policy concluded:

If cryptography can protect the trade secrets and proprietary information of businesses and thereby reduce economic espionage (which it can), it also supports in a

most important manner the job of law enforcement. If cryptography can help protect national critical information systems and networks against unauthorized penetration (which it can), it also supports the national security of the United States.

Second, if the Global Information Infrastructure is to reach its true potential, citizens and companies alike must have the confidence that their communications and transactions will be secure. The SAFE Act, by allowing all Americans to use the highest technology and strongest security available, will provide them with that confidence.

Third, with the availability of strong encryption overseas and on the Internet, our current export controls only serve to tie the hands of American business. According to an economic study released in December 1995 by the Computer Systems Policy Project, failure to remove these export controls by the year 2000—just 3 short years from now—will cost our economy $60 billion and 200,000 jobs.

The SAFE Act remedies this situation by allowing the unencumbered export of generally available software and hardware if a product with comparable security features is commercially available from foreign suppliers. Removing these export barriers will free U.S. industry to remain the world leader in software, hardware, and Internet development. And by allowing the U.S. computer industry to use and export the highest technology available with the strongest security features available, America will be leading the way into the 21st century information age and beyond.

This bipartisan legislation enjoys the support of members and organizations across the spectrum of all ideological and political beliefs. Groups as varied as the American Civil Liberties Union, National Rifle Association, Americans for Tax Reform, Netscape, Microsoft, Novell, Lotus, Adobe, Software Publishers Association, Information Technology Association of America, Citizens for a Sound Economy, Competitive Enterprise Institute, Business Leadership Council, IBM, Small Business Survival Committee, Sybase, RSA Data Security, Semiconductor Industry Association, Telecommunications Industry Association, and National Association of Manufacturers strongly support this legislation, to name just a few.

The SAFE Act enjoys this support not only because it is a commonsense approach to solving a very immediate problem, but also because ordinary Americans' personal privacy and computer security is being assaulted by this administration. Amazingly enough, the administration wants to mandate a back door into peoples' computer systems in order to access their private information and confidential communications. In fact the administration has said that if private citizens and companies do not voluntarily create this back door, it will seek legislation forcing Americans to give the Government access to their information by means of a key escrow system requiring computer users to put the keys to decode their encrypted communications into a central data bank. This is the technological equivalent of mandating that the Federal Government be given a key to every home in America.

The SAFE Act, on the other hand, will prevent the administration from placing roadblocks on the information superhighway by prohibiting the Government from mandating a back door into the computer systems of private citizens and businesses. Additionally, the SAFE Act ensures that all Americans have the right to choose any security system to protect their confidential information.

Mr. Speaker, with the millions of communications, transmissions, and transactions that occur on the Internet every day, American citizens and businesses must have the confidence that their private information and communications are safe and secure. That is precisely what the SAFE Act will ensure. I urge each of my colleagues to join and support this bipartisan effort.

The original cosponsors are Representatives LOFGREN, DELAY, BOEHNER, COBLE, SENSENBRENNER, BONO, PEASE, CANNON, CONYERS, BOUCHER, GEKAS, SMITH (TX), INGLIS, BRYANT (TN), CHABOT, BARR, JACKSON-LEE, WATERS, ACKERMAN, BAKER (NC), BARTLETT, CAMPBELL, CHAMBLISS, CUNNINGHAM, DAVIS (VA), DICKEY, DOOLITTLE, EHLERS, ENGEL, ESHOO, EVERETT, EWING, FARR, GEJDENSON, GILLMOR, GOODE, Delegate HOLMES-NORTON, Representatives HORN, Mrs. EDDIE BERNICE JOHNSON (TX), Mr. SAM JOHNSON (TX), KOLBE, MCINTOSH, MCKEON, MANZULLO, MATSUI, MICA, MINGE, MOAKLEY, NETHERCUTT, PACKARD, SESSIONS, UPTON, WHITE, and WOOLSEY.

Mr. Speaker, I would like the text of this legislation reprinted in the RECORD.

H.R.—

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Security and Freedom Through Encryption (SAFE) Act".

SEC. 2. SALE AND USE OF ENCRYPTION.

(a) IN GENERAL.—Part I of title 18, United States Code, is amended by inserting after chapter 121 the following new chapter:

"CHAPTER 122—ENCRYPTED WIRE AND ELECTRONIC INFORMATION

§2801. Definitions

"As used in this chapter—

"(1) the terms 'person', 'State', 'wire communication', 'electronic communication', 'investigative or law enforcement officer', 'judge of competent jurisdiction', and 'electronic storage' have the meanings given those terms in section 2510 of this title;

"(2) the terms 'encrypt' and 'encryption' refer to the scrambling of wire or electronic information using mathematical formulas or algorithms in order to preserve the confidentiality, integrity, or authenticity of, and prevent unauthorized recipients from accessing or altering, such information;

"(3) the term 'key' means the variable information used in a mathematical formula, code, or algorithm, or any component thereof, used to decrypt wire or electronic information that has been encrypted; and

"(4) the term 'United States person' means—

"(A) any United States citizen;

"(B) any other person organized under the laws of any State, the District of Columbia, or any commonwealth, territory, or possession of the United States; and

"(C) any person organized under the laws of any foreign country who is owned or controlled by individuals or persons described in subparagraphs (A) and (B).

"§2802. Freedom to use encryption

"Subject to section 2805, it shall be lawful for any person within any State, and for any United States person in a foreign country, to use any encryption, regardless of the encryption algorithm selected, encryption key length chosen, or implementation technique or medium used.

"§2803. Freedom to sell encryption

"Subject to section 2805, it shall be lawful for any person within any State to sell in interstate commerce any encryption, regardless of the encryption algorithm selected, encryption key length chosen, or implementation technique or medium used.

"§2804. Prohibition on mandatory key escrow

"(a) PROHIBITION.—No person in lawful possession of a key to encrypted information may be required by Federal or State law to relinquish to another person control of that key.

"(B) EXCEPTION FOR ACCESS FOR LAW ENFORCEMENT PURPOSES.—Subsection (a) shall not affect the authority of any investigative or law enforcement officer, acting under any law in effect on the effective date of this chapter, to gain access to encrypted information.

"§2805. Unlawful use of encryption in furtherance of a criminal act

"Any person who willfully uses encryption in furtherance of the commission of a criminal offense for which the person may be prosecuted in a court of competent jurisdiction—

"(1) in the case of a first offense under this section, shall be imprisoned for not more than 5 years, or fined in the amount set forth in this title, or both; and

"(2) in the case of a second or subsequent offense under this section, shall be imprisoned for not more than 10 years, or fined in the amount set forth in this title, or both.".

(b) CONFORMING AMENDMENT.—The table of chapters for part I of title 18, United States Code, is amended by inserting after the item relating to chapter 33 of the following new item:

SEC. 3. EXPORTS OF ENCRYPTION.

(a) AMENDMENT TO EXPORT ADMINISTRATION ACT OF 1979.—Section 17 of the Export Administration Act of 1979 (50 U.S.C. App. 2416) is amended by adding at the end thereof the following new subsection:

"(g) COMPUTERS AND RELATED EQUIPMENT.—

"(1) GENERAL RULE.—Subject to paragraphs (2), (3), and (4), the Secretary shall have exclusive authority to control exports of all computer hardware, software, and technology for information security (including encryption), except that which is specifically designed or modified for military use, including command, control, and intelligence applications.

"(2) ITEMS NOT REQUIRING LICENSES.—No validated license may be required, except pursuant to the Trading With the Enemy Act or the International Emergency Economic Powers Act (but only to the extent that the authority of such Act is not exercised to extend controls imposed under this Act), for the export or reexport of—

"(A) any software, including software with encryption capabilities—

"(i) that is generally available, as is, and is designed for installation by the purchaser; or

"(ii) that is in the public domain for which copyright or other protection is not available under title 17, United States Code, or that is available to the public because it is generally accessible to the interested public in any form; or

"(B) any computing device solely because it incorporates or employs in any form software (including software with encryption capabilities) exempted from any requirement

for a validated license under subparagraph (A).

"(3) SOFTWARE WITH ENCRYPTION CAPABILITIES.—The Secretary shall authorize the export or reexport of software with encryption capabilities for nonmilitary end uses in any country to which exports of software of similar capability are permitted for use by financial institutions not controlled in fact by United States persons, unless there is substantial evidence that such software will be—

"(A) diverted to a military end use or an end use supporting international terrorism;

"(B) modified for military or terrorist end use; or

"(C) reexported without any authorization by the United States that may be required under this Act.

"(4) HARDWARE WITH ENCRYPTION CAPABILITIES.—The Secretary shall authorize the export or reexport of computer hardware with encryption capabilities if the Secretary determines that a product offering comparable security is commercially available outside the United States from a foreign supplier, without effective restrictions.

"(5) DEFINITIONS.—As used in this subsection—

"(A) the term 'encryption' means the scrambling of wire or electronic information using mathematical formulas or algorithms in order to preserve the confidentiality, integrity, or authenticity of, and prevent unauthorized recipients from accessing or altering, such information;

"(B) the term 'generally available' means, in the case of software (including software with encryption capabilities), software that is offered for sale, license, or transfer to any person without restriction, whether or not for consideration, including, but not limited to, over-the-counter retail sales, mail order transactions, phone order transactions, electronic distribution, or sale on approval;

"(C) the term 'as is' means, in the case of software (including software with encryption capabilities), a software program that is not designed, developed, or tailored by the software publisher for specific purchasers, except that such purchasers may supply certain installation parameters needed by the software program to function properly with the purchaser's system and may customize the software program by choosing among options contained in the software program;

"(D) the term 'is designed for installation by the purchaser' means, in the case of software (including software with encryption capabilities) that—

"(i) the software publisher intends for the purchaser (including any licensee or transferee), who may not be the actual program user, to install the software program on a computing device and has supplied the necessary instructions to do so, except that the publisher may also provide telephone help line services for software installation, electronic transmission, or basic operations; and

"(ii) the software program is designed for installation by the purchaser without further substantial support by the supplier;

"(E) the term 'computing device' means a device which incorporates one or more microprocessor-based central processing units that can accept, store, process, or provide output of data; and

"(F) the term 'computer hardware', when used in conjunction with information security, includes, but is not limited to, computer systems, equipment, application-specific assemblies, modules, and integrated circuits.".

(b) CONTINUATION OF EXPORT ADMINISTRATION ACT.—For purposes of carrying out the amendment made by subsection (a), the Export Administration Act of 1979 shall be deemed to be in effect.

Document No. 50