106TH CONGRESS, 1st Session | HOUSE OF REPRESENTATIVES | REPT. 106–117 Part 3

SECURITY AND FREEDOM THROUGH ENCRYPTION (SAFE) ACT

JULY 19, 1999.—Ordered to be printed

Mr. GILMAN, from the Committee on International Relations, submitted the following

R E P O R T

together with

DISSENTING VIEWS

[To accompany H.R. 850]

[Including cost estimate of the Congressional Budget Office]

The Committee on International Relations, to whom was referred the bill (H.R. 850) to amend title 18, United States Code, to affirm the rights of United States persons to use and sell encryption and to relax export controls on encryption, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

The amendment is as follows:

Strike out all after the enacting clause and insert in lieu thereof the following:

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 123 the following new chapter:

"CHAPTER 125—ENCRYPTED WIRE AND ELECTRONIC INFORMATION

"2801. Definitions.
"2802. Freedom to use encryption.
"2803. Freedom to sell encryption.
"2804. Prohibition on mandatory key escrow.
"2805. Unlawful use of encryption in furtherance of a criminal act.

"§ 2801. Definitions

"As used in this chapter—

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

"(2) the term 'decrypt' means to retransform or unscramble encrypted data, including communications, to its readable form;

"(3) the terms 'encrypt', 'encrypted', and 'encryption' mean the scrambling of wire communications, electronic communications, or electronically stored 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 communications or information;

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

"(5) the term 'key recovery information' means information that would enable obtaining the key of a user of encryption;

"(6) the term 'plaintext access capability' means any method or mechanism which would provide information in readable form prior to its being encrypted or after it has been decrypted;

"(7) 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) GENERAL PROHIBITION.—Neither the Federal Government nor a State may require that, or condition any approval on a requirement that, a key, access to a key, key recovery information, or any other plaintext access capability be—

"(1) built into computer hardware or software for any purpose;

"(2) given to any other person, including a Federal Government agency or an entity in the private sector that may be certified or approved by the Federal Government or a State to receive it; or

"(3) retained by the owner or user of an encryption key or any other person, other than for encryption products for use by the Federal Government or a State.

"(b) EXCEPTION FOR GOVERNMENT NATIONAL SECURITY AND LAW ENFORCEMENT PURPOSES.—The prohibition contained in subsection (a) shall not apply to any department, agency, or instrumentality of the United States, or to any department, agency, or political subdivision of a State, that has a valid contract with a nongovernmental entity that is assisting in the performance of national security or law enforcement activity.

"(c) EXCEPTION FOR ACCESS FOR LAW ENFORCEMENT PURPOSES.—Subsection (a) shall not affect the authority of any investigative or law enforcement officer, or any member of the intelligence community as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 401a), acting under any law in effect on the effective date of this chapter, to gain access to encrypted communications or information.

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

"(a) ENCRYPTION OF INCRIMINATING COMMUNICATIONS OR INFORMATION UNLAWFUL.—Any person who, in the commission of a felony under a criminal statute of the United States, knowingly and willfully encrypts incriminating communications or information relating to that felony with the intent to conceal such communications or information for the purpose of avoiding detection by law enforcement agencies or prosecution—

"(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) USE OF ENCRYPTION NOT A BASIS FOR PROBABLE CAUSE.—The use of encryption by any person shall not be the sole basis for establishing probable cause with respect to a criminal offense or a search warrant.".

(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 123 the following new item:

"125. Encrypted wire and electronic information ..... 2801".

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) CERTAIN CONSUMER PRODUCTS, COMPUTERS, AND RELATED EQUIPMENT.—

"(1) GENERAL RULE.—Subject to paragraphs (2) and (3), the Secretary shall have exclusive authority to control exports of all computer hardware, software, computing devices, customer premises equipment, communications network equipment, 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.—After a 1-time technical review by the Secretary, which shall be completed not later than 30 working days after submission of the product concerned for such technical review, no export 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 computer hardware or software or computing device, including computer hardware or software or computing devices with encryption capabilities—

"(i) that is generally available;

"(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

"(iii) that is used in a commercial, off-the-shelf, consumer product or any component or subassembly designed for use in such a consumer product available within the United States or abroad which—

"(I) includes encryption capabilities which are inaccessible to the end user; and

"(II) is not designed for military or intelligence end use;

"(B) any computing device solely because it incorporates or employs in any form—

"(i) computer hardware or software (including computer hardware or software with encryption capabilities) that is exempted from any requirement for a license under subparagraph (A); or

"(ii) computer hardware or software that is no more technically complex in its encryption capabilities than computer hardware or software that is exempted from any requirement for a license under subparagraph (A) but is not designed for installation by the purchaser;

"(C) any computer hardware or software or computing device solely on the basis that it incorporates or employs in any form interface mechanisms for interaction with other computer hardware or software or computing devices, including computer hardware and software and computing devices with encryption capabilities;

"(D) any computing or telecommunication device which incorporates or employs in any form computer hardware or software encryption capabilities which—

"(i) are not directly available to the end user; or

"(ii) limit the encryption to be point-to-point from the user to a central communications point or link and does not enable end-to-end user encryption;

"(E) technical assistance and technical data used for the installation or maintenance of computer hardware or software or computing devices with encryption capabilities covered under this subsection; or

"(F) any encryption hardware or software or computing device not used for confidentiality purposes, such as authentication, integrity, electronic signatures, nonrepudiation, or copy protection.

"(3) COMPUTER HARDWARE OR SOFTWARE OR COMPUTING DEVICES WITH ENCRYPTION CAPABILITIES.—After a 1-time technical review by the Secretary, which shall be completed not later than 30 working days after submission of the product concerned for such technical review, the Secretary shall authorize the export or reexport of computer hardware or software or computing devices with encryption capabilities for nonmilitary end uses in any country—

"(A) to which exports of computer hardware or software or computing devices of comparable strength are permitted for use by financial institutions not controlled in fact by United States persons, unless there is credible evidence that such computer hardware or software or computing devices will be—

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

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

"(iii) reexported without any authorization by the United States that may be required under this Act; or

"(B) if the Secretary determines that a computer hardware or software or computing device offering comparable security is commercially available outside the United States from a foreign supplier, without effective restrictions.

"(4) EXPORTS TO MAJOR DRUG-TRANSIT AND ILLICIT DRUG PRODUCING COUNTRIES.—The Secretary, before approving any export or reexport of encryption products to any major drug-transit country or major illicit drug producing country identified under section 490(h) of the Foreign Assistance Act of 1961, shall consult with the Attorney General of the United States, the Director of the Federal Bureau of Investigation, and the Administrator of the Drug Enforcement Administration on the potential impact of such export or reexport on the flow of illicit drugs into the United States. This paragraph shall not authorize the denial of an export of an encryption product, or of the issuance of a specific export license, for which such denial is not otherwise appropriate, solely because the country of destination is a major drug-transit country or major illicit drug producing country.

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

"(A)(i) the term 'encryption' means the scrambling of wire communications, electronic communications, or electronically stored 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 communications or information;

"(ii) the terms 'wire communication' and 'electronic communication' have the meanings given those terms in section 2510 of title 18, United States Code;

"(B) the term 'generally available' means, in the case of computer hardware or computer software (including computer hardware or computer software with encryption capabilities)—

"(i) computer hardware or computer software that is—

"(I) distributed through the Internet;

"(II) 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;

"(III) preloaded on computer hardware or computing devices that are widely available for sale to the public; or

"(IV) assembled from computer hardware or computer software components that are widely available for sale to the public;

"(ii) not designed, developed, or tailored by the manufacturer for specific purchasers or users, except that any such purchaser or user may—

"(I) supply certain installation parameters needed by the computer hardware or software to function properly with the computer system of the user or purchaser; or

"(II) select from among options contained in the computer hardware or computer software;

"(iii) with respect to which the manufacturer of that computer hardware or computer software—

"(I) intended for the user or purchaser, including any licensee or transferee, to install the computer hardware or software and has supplied the necessary instructions to do so, except that the manufacturer of the computer hardware or software, or any agent of such manufacturer, may also provide telephone or electronic mail help line services for installation, electronic transmission, or basic operations; and

"(II) the computer hardware or software is designed for such installation by the user or purchaser without further substantial support by the manufacturer; and

"(iv) 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 '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;

"(D) the term 'computer hardware' includes, but is not limited to, computer systems, equipment, application-specific assemblies, smart cards, modules, integrated circuits, and printed circuit board assemblies;

"(E) the term 'customer premises equipment' means equipment employed on the premises of a person to originate, route, or terminate communications;

"(F) the term 'technical assistance' includes instruction, skills training, working knowledge, consulting services, and the transfer of technical data;

"(G) the term 'technical data' includes blueprints, plans, diagrams, models, formulas, tables, engineering designs and specifications, and manuals and instructions written or recorded on other media or devices such as disks, tapes, or read-only memories; and

"(H) the term 'technical review' means a review by the Secretary of computer hardware or software or computing devices with encryption capabilities, based on information about the product's encryption capabilities supplied by the manufacturer, that the computer hardware or software or computing device works as represented.".

(b) NO REINSTATEMENT OF EXPORT CONTROLS ON PREVIOUSLY DECONTROLLED PRODUCTS.—Any encryption product not requiring an export license as of the date of enactment of this Act, as a result of administrative decision or rulemaking, shall not require an export license on or after such date of enactment.

(c) APPLICABILITY OF CERTAIN EXPORT CONTROLS.—

(1) IN GENERAL.—Nothing in this Act shall limit the authority of the President under the International Emergency Economic Powers Act, the Trading with the enemy Act, or the Export Administration Act of 1979, to—

(A) prohibit the export of encryption products to countries that have been determined to repeatedly provide support for acts of international terrorism;

(B) prohibit the export or reexport of any encryption product with an encryption strength of more than 56 bits to any military unit of the People's Republic of China, including the People's Liberation Army (as defined in section 1237(c) of the Strom Thurmond National Defense Authorization Act for Fiscal Year 1999 (50 U.S.C. 1701 note)); or

(C) impose an embargo on exports to, and imports from, a specific country.

(2) SPECIFIC DENIALS.—The Secretary of Commerce may prohibit the export of specific encryption products to an individual or organization in a specific foreign country or countries identified by the Secretary, if the Secretary, in consultation with the Secretary of Defense, the Secretary of State, the Attorney General, the Director of the Federal Bureau of Investigation, the Administrator of the Drug Enforcement Administration, and the Director of Central Intelligence, determines that there is credible evidence that such encryption products will be used—

(A) for military or terrorist end-use;

(B) to facilitate the import of illicit drugs into the United States;

(C) in the manufacture of weapons of mass destruction or otherwise to assist in the proliferation of weapons of mass destruction; or

(D) for illegal activities involving the sexual exploitation of, abuse of, or sexually explicit conduct with minors.

(3) OTHER EXPORT CONTROLS.—Any encryption product is subject to export controls for any reason other than the existence of encryption capability, including export controls imposed on high performance computers. Nothing in this Act or the amendments made by this Act alters the ability of the Secretary of Commerce to control exports for reasons other than encryption capabilities.

(4) DEFINITION.—As used in this subsection and subsection (b), the term "encryption" has the meaning given that term in section 17(g)(5)(A) of the Export Administration Act of 1979, as added by subsection (a) of this section.

(d) 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.

SEC. 4. EFFECT ON LAW ENFORCEMENT ACTIVITIES.

(a) COLLECTION OF INFORMATION BY ATTORNEY GENERAL.—The Attorney General shall compile, and maintain in classified form, data on the instances in which encryption (as defined in section 2801 of title 18, United States Code) has interfered with, impeded, or obstructed the ability of the Department of Justice to enforce the criminal laws of the United States.

(b) AVAILABILITY OF INFORMATION TO THE CONGRESS.—The information compiled under subsection (a), including an unclassified summary thereof, shall be made available, upon request, to any Member of Congress.

BACKGROUND AND PURPOSE

H.R. 850, the Security And Freedom through Encryption (SAFE) Act, represents a strong bipartisan effort to bring U.S. laws on the export of encryption technology in line with international realities. The SAFE Act enjoys strong support in the House as reflected by the overwhelming number of cosponsors, including the majority of the Members of the International Relations Committee.

While differences still remain and the debate continues between U.S. economic and commercial priorities and individual civil liberties, on the one hand, and the needs and concerns of law enforcement and national security agencies, the SAFE Act is generating the political will to reform the existing regulatory process to meet today's realities.

Encryption has been defined as referring to the use of software or hardware to scramble 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. While anyone can encrypt a message, only an authorized person can convert a scrambled message back into its original form.

The basic idea of modern encryption, or cryptography, is that any message can be represented as a set of numbers (the plaintext) used to transform the plaintext into a different set of numbers (the ciphertext.) Simply stated, keys consist of a series of ones and zeros (called bits), and are described in terms of their "length", which corresponds to the number of possible combinations of ones and zeros equals 2 to the 40th power. It then follows that a 56-bit key is 2 to the 56th power, which means that it is 2 to the 16th power stronger than a 40-bit key.

Once the exclusive domain of the national security and intelligence sectors, encryption now has an expanded application, impacting the everyday lives of millions of Americans. Today, banking systems, stock markets, air traffic control systems, credit bureaus, telephone networks, civilian and government payrolls, and the Internet are all directly affected by a flow of data managed by countless computers and telecommunications networks around the

world. Computer technology now serves as the nervous system of modern technology.

It is increasingly difficult to protect the privacy and confidentiality of transactions at all levels, and increasingly important to do so. The Justice Department has estimated that annual losses related to computer security breaches could be as high as $7 billion. If this were adjusted to include the number of undocumented cases by companies reluctant to report such intrusions, the figure could be even higher. The National Counterintelligence Center in their "Annual Report to Congress on Foreign Economic Collection and Industrial Espionage" concluded that such "specialized technical operations (including computer intrusion, telecommunications targeting and intercept, and private sector encryption weaknesses) account for the largest portion of economic and industrial information lost by corporations."

Therefore, stronger encryption tools are widely viewed as the key to providing security and privacy for the information superhighway.

Current U.S. policy restricts the export of "strong" encryption hardware or software products with keys greater than 56-bits long-determined to be gravely inadequate by numerous experts. The current Administration policy is viewed as not meeting the needs of U.S. companies to conduct business in a secure manner with their suppliers, their business partners, their customers, and even their affiliated companies outside the United States.

Supporting the need for higher encryption standards is the fact that a group of independent programmers and researchers cracked a 56-bit code in less than 24 hours using computers linked across the Internet. This successful breaking of 56-bit encryption clearly demonstrates the anachronistic nature of current U.S. law and reflects how out-of-touch the Administration's policy is with regard the needs of the global marketplace.

As predicted, the Administration's policy can not realistically enforce its ban on exports of encryption over 56 bits. Anybody can carry strong encryption across the U.S. border on a single diskette hidden in his pocket without being detected or, alternatively, can download it off the Internet from anywhere in the world.

In addition, the Administration's policy only allows the export of greater than 56-bit encryption in limited circumstances, or for those who promise to build in "key recovery." "Key recovery" or "key escrow" essentially means that when stored data or electronic communications are encrypted, a third party has a copy of the key needed to decrypt the information. As presented by proponents of this policy, escrowed encryption is intended to provide for encryption protection for legitimate uses but also enable law enforcement officials to gain access to the key when necessary to decode the plaintext date as part of and investigation.

This has been interpreted as an attempt to use the export control process to manipulate and control the market for and expansion of encryption technology, by making it easy to export products with key recovery and difficult for those products without. The logical basis for this policy is flawed as it is rooted in the wrongful assumption that foreign competitors can be convinced to alter their policy to parallel what U.S. policy is calling for. The current policy

is not based on fact, but on the optimistic view that the U.S. can influence other countries not to export strong encryption without an escrow system.

Speculation does not make for good laws. Individually and as a unit, many of our European allies have clearly illustrated their commitment to allow market forces and individual needs to dictate the levels of encryption. In its April 1997 proposal entitled, "A European Initiative in Electronic Commerce," the European Union stated as key elements of the Initiative to ensure a framework which "boosts the trust and confidence of businesses for investments and consumers to make use of electronic commerce by dismantling remaining legal and regulatory barriers and preventing the creation of new obstacles." It goes on to say that: "The use of strong encryption which ensures the confidentiality of both sensitive commercial and personal data is one of the foundation stones of electronic commerce. * * * The Community (European Community) shall work at the international level towards the removal of trade barriers for encryption products."

Even the more conservative recommendations made in March 1997 by the Council of the Organization for Economic Cooperation and Development, clearly state that: "Users should have access to cryptography that meets their needs, so that they can trust in the security of information and communications systems, and the confidentiality and integrity of data on those systems." The Council further underscores that: "Government controls on cryptographic methods * * * should respect user choice to the greatest extent possible * * * and should not be interpreted as implying that governments should initiate legislation which limits user choice." Finally, they add: "The development and provision of cryptographic methods should be determined by the market in an open and competitive environment. Such an approach would best ensure that solutions keep pace with changing technology, the demands of users and evolving threats to communications systems security."

While U.S. companies are kept at 56-bit encryption with the condition that they commit to develop key recovery, non-U.S. exporters, particularly the countries of the European Union, are producing packages that include encryption technology using 128 bits leaving American companies far behind in the race to capture new markets.

American companies are placed at a competitive disadvantage by being forced to create and deploy two separate systems to meet two separate standards. Because of the nightmare this would create, most U.S. businesses end up making their domestic products subject to the same restrictions as their exportable products. By not allowing U.S. industries to provide secure products in the face of strong foreign competitors who are not restricted by outdated export controls, current law is hurting U.S. businesses. No one will buy encryption products for which the U.S. government can obtain a key. A recent report by the CEOs of 13 large American technology companies concluded that the U.S. computer industry could potentially lose up to $30–60 billion annually by the year 2000 due to these export controls.

At a fundamental level, evaluating the value of key recovery systems in and of themselves, eleven of the world's top cryptographers

concluded that key recovery systems would create new vulnerabilities. A key recovery system would create serious difficulties as it would require a vast infrastructure of recovery agents and oversight entities to manage access to keys. In their May 1997 report entitled, "The Risks of Key Recovery, Key Escrow, and Trusted Third Party Encryption", these experts also determined that "the field of cryptography has no experience in deploying secure systems of this scope and complexity" and that such systems could potentially cost many billions of dollars.

Key recovery systems do not even meet the national security needs on which the policy is based. Several noted studies have documented hundreds of foreign encryption products already widely available abroad and to which criminals, terrorists, and foreign governments have access. Just recently, a George Washington University study entitled "Growing Development of Foreign Encryption Products in the Fact of U.S. Export Regulations" found that there are currently over 800 strong encryption products in the marketplace incorporating cryptography manufactured in 35 countries outside the U.S., which is a 22 percent increase since 1997. It is the upstanding, law abiding citizen who suffers.

The fact is that strong encryption helps further the goals of law enforcement and national security, more than key recovery could ever hope to. The use of strong encryption reduces the likelihood of theft of private information of American citizens and businesses, making the job of law enforcement easier and decreasing the occurrence of industrial espionage. In its landmark report on encryption policy, the blue-ribbon National Research Council concluded the following about the use of strong encryption:

> If cryptography can protect the trade secret and proprietary information of business 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 nationally critical information systems and networks against unauthorized penetration (which it can), it also supports the national security of the United States.

With a reach beyond the practical issues of national security and economic competitiveness, the debate over encryption penetrates the heart of our American identity: First and Fourth Amendment Rights, the right to privacy, and the struggle for democracy abroad. Many legal scholars argue that aspects of the Administration's current encryption regime place unconstitutional restraints on protected speech. In *Bernstein* v. *Department of State,* a California district court held that source code was protected by the First Amendment and current licensing requirements constituted an unconstitutional prior restraint. This decision was recently upheld by the 9th Circuit Court of Appeals. In addition, many consumer and privacy advocates have voiced concern that weak encryption and the key escrow policy is a threat to personal privacy. Confidentiality of our personal, medical, and financial records may be compromised if our keys gets into the wrong hands or if somebody cracks weak encryption codes. Furthermore, dissidents around the world rely on

strong encryption to defy totalitarian regimes in their struggle for democracy.

If U.S. laws are not changed soon, as H.R. 850 attempts to do, world standards for security technology will shift away from the U.S. as customers buy products from foreign manufacturers. The U.S. economy will lose billions of dollars and our workers hundreds of thousands of jobs. As U.S. industries lose their competitive edge to foreign companies, our law enforcement and national security agencies will not enjoy the same access or insight into the security technology that replaces U.S. technology as the world standards. Foreign companies are less likely to cooperate or share technological secrets with the U.S. Government to solve crimes or to defend our country.

On July 7, 1997, German Economics Minister Guenter Rexrodt called for the removal of restrictions on encryption technology in his opening remarks or a two-day conference on Internet commerce attended by 40 government ministers from the European Union, The United States, Russia, Japan, and Canada. "Users can only protect themselves against having data manipulated, destroyed or spied on through the use of strong encryption procedures," Rexrodt said, "that is why we have to use all of our powers to promote such procedures instead of blocking them."

Individual Americans and U.S. businesses should be afforded the same protection and the same opportunities that other countries provide their own people and industries. H.R. 850—the SAFE Act—does just that. It is aimed at correcting the unfair and unsafe situation that currently exists under current law. Specifically the bill as passed by the Judiciary and International Relations Committees allows the export of generally available encryption products after a one-time, 30 working day technical review and custom products after the same review, if such products are commercially available from foreign companies or are approved for use by foreign banks, and codifies existing law regarding the use and sale of cnryption domestically. Additionally, the bill prohibits the government from mandating a key escrow or key recovery system on the private sector, but does not prohibit the government from using recoverable encryption on its own systems or from requiring the use of recoverable encryption in national security of law enforcement-related contracts. Finally, H.R. 850 allows the President to prohibit exports to terrorist states, to prohibit the export of encryption products over 56 bits to any military unit of the People's Republic of China, and to impose embargoes; contains criminal penalties for the use of encryption to cover up criminal activity; and allows the Secretary of Commerce, in consultation with the Secretary of Defense, Secretary of State, Attorney General, FBI Director, DEA Administrator, and CIA Director, to stop the export of specific products to individuals or organizations in specific countries if there is credible evidence that such products will be used for military or terrorist purposes, used to facilitate the import of illegal drugs into the U.S. used in the manufacture of weapons of mass destruction, or used for activities relating to child pornography.

In essence, H.R. 850 prevents economic espionage while protecting hundreds of thousands of American jobs by affording all Americans the freedom to use any type of encryption to be sold in

the United States; and creates a level playing field by permitting the export of the generally available software, hardware, and other encryption-related computer products.

The Committee hopes that other Members realize the need, value, and importance of H.R. 850 as it works its way thorough the legislative process. In the interest of the American people, of U.S. economic leadership and growth, and of national security, the Committee hopes the House will pass the SAFE Act.

COMMITTEE ACTION

INTRODUCTION AND CONSIDERATION OF THE BILL

H.R. 850, the Security and Freedom through Encryption (SAFE) Act, was introduced by Rep. Goodlatte on February 25, 1999, and referred to the Committee on the Judiciary, and in addition to the Committee on International Relations. On April 27, 1999 it was reported from the Committee on the Judiciary (H. Rept. 106–117, part I), and the referral to the Committee on International Relations was extended for a period ending not later than July 2, 1999. On April 27, it was also referred to the Committees on Armed Services, Commerce, and Intelligence, for a period ending not later than July 2. On July 2, it was reported from the Committee on Commerce (H. Rept. 106–117, part II), and the referral period was extended to not later than July 16 for the Committee on International Relations and to not later than July 23 for the Committees on Armed Service and Intelligence.

On May 18, 1999, the International Economic Policy and Trade Subcommittee held a hearing on encryption. Testimony was received from the following witnesses: The Honorable William A. Reinsch, Undersecretary of Commerce, Bureau of Export Administration; The Honorable Barbara McNamara, Deputy Director, National Security Agency; The Honorable Ron Lee, Assistant Attorney General, National Security, Department of Justice; and several private sector witnesses including Ira Rubinstein, Senior Corporate Attorney of the Microsoft Corporation on behalf of the Business Software Alliance; Dinah PoKempner, Deputy General Counsel of Human Rights Watch; David Weiss, Vice President for Product Marketing of Citrix, Incorporated; Edward J. Black, President of the Computer and Communications Industry Association; Jeffrey H. Smith, Counsel of Americans for Computer Privacy; and Alan B. Davidson, Staff Counsel of the Center for Democracy and Technology.

MARKUP OF THE BILL

On March 23, 1999, H.R. 850 was referred to the Subcommittee on International Economic Policy and Trade which subsequently waived consideration of the measure.

The Full Committee marked up the bill, pursuant to notice, in open session, on July 13, 1999. The following amendments were considered:

(1) Gilman amendment—page 12, line 18, adding paragraph "(4) Exports to major drug-transit and illicit drug producing countries." The amendments was agreed to by voice vote, as amended by #3.

(2) Gejdenson amendment to Gilman amendment (#1)—page 17, line 22, adding "(3) Drug producing and trafficking entities."—This amendment was withdrawn.

(3) Gejdenson/Campbell amendment to Gilman amendment (#1)—at the end of the Gilman amendment add, "This provision shall not authorize the denial of export of an encryption product, or the issuance of a specific export license, for which such denial is not otherwise appropriate, solely because the country of destination is a major drug-transit country or major illicit drug-producing country." The amendment was agreed to by voice vote.

(4) Berman amendment—page 13, strike lines 16–23 and redesignate the succeeding subclauses accordingly; page 14, line 18, strike "and" * * * Mr. Berman asked Unanimous Consent to strike lines 1 and 2 of his amendment, and to change the word "distribution" in line 12 to "approval". There was no objection. The amendment was agreed to by voice vote.

(5) Gilman amendment—page 17, after line 22, "(3) Other Export Controls." The amendment, as amended by #6, was agreed to by voice vote.

(6) Campbell amendment to the Gilman amendment (#5)—strike the last sentence of the Gilman (#5) amendment. The amendment was agreed to by unanimous consent.

(7) Berman amendment—changes the "15-day" technical review by the Secretary to 30 working days and changed the standard to provide for the normal, extensive end use and verification checks. The amendment, as amended by #8, was agreed to by voice vote.

(8) Gejdenson substitute amendment to #7—changes the "15-day" technical review by the Secretary to 30 days but deleted the restoration of the current safeguards. A Gejdenson unanimous consent request to change "30 days" to "30 working days" was agreed to. The amendment was agreed to by a recorded vote of 21–11.

(9) Gilman en block amendment. The amendment, as amended by #10, was agreed to by voice vote.

(10) Gejdenson/Gilman amendment to #49—page 17, strike lines 16–22, and insert the following: "(2) Specific Denials.—" By unanimous consent, the word "shall" on line 1 of the amendment was changed to "may". The amendment was agreed to by unanimous consent.

(11) Davis amendment—page 12, line 3, strike "substantial" and insert "credible"; page 17, line 20 strike "substantial" and insert "credible". The amendment was agreed to by voice vote.

(12) Berman amendment—page 6, strike lines 3–15 and insert the following, "(b) Exception for Government National Security and Law Enforcement Purposes." The amendment was agreed to by voice vote.

(13) Berman amendment—page 17, line 13, strike "or" after the semicolon; page 17, line 15, strike the period and insert "; or", page 17, after line 15, insert "(C) require a license for, or other control of, the export of an encryption product pursuant to a binding multilateral export control regime in which the United States participates." The amendment was defeated by a recorded vote of 15–22.

With a quorum being present, the Committee, by a recorded vote of 33 ayes to five nays, ordered the bill, as amended, reported to

the House, with the recommendation that the bill, as amended, do pass.

RECORD VOTES

Clause (3)(b) of the rule XIII of the Rules of the House of Representatives requires that the results of each record vote on an amendment or motion to report, together with the names of those voting for or against, be printed in the committee report.

Descripion of amendment, motion order, or other proposition (Votes during markup of H.R. 850—July 13, 1999)

Vote No. 1 (1:43 p.m.)—Gejdenson amendment (#8) to the Berman amendment (#7), which changed the time allowed for a technical review by the Secretary from 15 days to 30 working days and eliminated from the Berman amendment a provision that would have maintained the normal end use check and verifications.

Voting Yes: Goodling, Burton, Ballenger, Rohrabacher, Manzullo, Chabot, Salmon, Houghton, Campbell, Radanovich, Gejdenson, Ackerman, Payne, Menendez, McKinney, Hilliard, Sherman, Delahunt, Lee, Crowley, and Hoeffel.

Voting No: Gilman, Bereuter, Royce, King, Tancredo, Berman, Brown, Danner, Rothman, Davis, and Pomeroy.

Ayes 12. Noes 11.

Vote No. 2 (2:20 p.m.)—Berman amendment (#13) which states that "Nothing in this Act shall limit the authority of the President under the International Emergency Economic Powers Act, the Trading with the Enemy Act, or the Export Administration Act of 1979, to require a license for, or other control of, the export of an encryption product pursuant to a binding multilateral export control regime in which the U.S. participates."

Voting Yes: Gilman, Goodling, Bereuter, Gallegly, Ballenger, Royce, King, Radanovich, Cooksey, Berman, Danner, Hilliard, Rothman, Davis, and Pomeroy.

Voting No: Ros-Lehtinen, Rohrabacher, Manzullo, Chabot, Sanford, Salmon, Houghton, Campbell, Brady, Gillmore, Tancredo, Gejdenson, Ackerman, Payne, Menendez, Brown, McKinney, Sherman, Meeks, Lee, Crowley, and Hoeffel.

Ayes 15. Noes 22.

Vote No. 3 (2:26 p.m.)—Motion to favorably report the bill, as amended.

Voting Yes: Goodling, Gallegly, Ballenger, Rohrabacher, Manzullo, Royce, Chabot, Sanford, Salmon, Houghton, Campbell, Brady, Gillmor, Radanvoich, Cooksey, Tancredo, Gejdenson, Ackerman, Faleomavaega, Martinez, Payne, Menendez, Brown, McKinney, Danner, Hilliard, Sherman, Davis, Pomeroy, Meeks, Lee, Crowley, and Hoeffel.

Voting No: Gilman, Bereuter, King, Berman, and Rothman.

Ayes 33. Noes 5.

OTHER MATTERS

COMMITTEE OVERSIGHT FINDINGS

In compliance with clause 3(c)(1) of rule XIII of the Rules of the House of Representatives, the Committee reports the findings and

recommendations of the Committee, based on oversight activities under clause 2(b)(1) of rule X of the Rules of the House of Representatives, are incorporated in the descriptive portions of this report.

COMMITTEE ON GOVERNMENT REFORM FINDINGS

Clause 3(c)(4) of rule XIII of the Rules of the House of Representatives requires each committee report to contain a summary of the oversight findings and recommendations made by the Government Reform Committee pursuant to clause (4)(c)(2) of rule X of those rules. The Committee on International Relations has received no such findings or recommendations from the Committee on Government Reform.

ADVISORY COMMITTEE STATEMENT

No advisory committees within the meaning of section 5(b) of the Federal Advisory Committee Act were created by this legislation.

APPLICABILITY TO THE LEGISLATIVE BRANCH

The Committee finds that the legislation does not relate to the terms and conditions of employment or access to public services or accommodations within the meaning of section 102(b)(3) of the Congressional Accountability Act.

CONSTITUTIONAL AUTHORITY STATEMENT

In compliance with clause 3(d)(1) of rule XIII of the Rules of the House of Representatives, the Committee cites the following specific powers granted to the Congress in the Constitution as authority for enactment of H.R. 850 as reported by the Committee: Article I, section 8, clause 1 (relating to providing for the common defense and general welfare of the United States); Article I, section 8, clause 3 (relating to the regulation of commerce with foreign nations); and Article I, section 8, clause 18 (relating to making all laws necessary and proper for carrying into execution powers vested by the Constitution in the government of the United States).

PREEMPTION CLARIFICATION

Section 423 of the Congressional Budget Act of 1974 requires the report of any committee on a bill or joint resolution to include a committee statement on the extent to which the bill or joint resolution is intended to preempt state or local law. H.R. 850 would preempt and is apparently intended to preempt state law, including common law, relating to the ability of states and localities to require the use of plaintext recovery systems of various types. It would—for example—bar states from requiring their contractors to both encrypt data the contractors process on behalf of the states and at the same time to require the use of plaintext recovery system. (It might be noted that H.R. 850 similarly bars the United States from making such a provision by regulation with respect to its contractors or suppliers.) The bill might even bar the states from making voluntary contractual arrangements along those lines with suppliers or customers. It would also bar the states from using their police powers to require that certain sensitive data in

industries they regulate be both encrypted and recoverable or to require that if data used in such industries were encrypted, a plaintext recovery system be available.

NEW BUDGET AUTHORITY AND TAX EXPENDITURES, CONGRESSIONAL BUDGET OFFICE COST ESTIMATE, AND FEDERAL MANDATES STATEMENTS

Clause 3(c)(2) of rule XIII of the Rules of the House of Representatives requires each committee report that accompanies a measure providing new budget authority, new spending authority, or new credit authority or changing revenues or tax expenditures to contain a cost estimate, as required by section 308(a)(1) of the Congressional Budget Act of 1974, as amended, and, when practicable with respect to estimates of new budget authority, a comparison of the estimated funding level for the relevant program (or programs) to the appropriate levels under current law.

Clause 3(d) of rule XIII of the Rules of the House of Representatives requires committees to include their own cost estimates in certain committee reports, which include, when practicable, a comparison of the total estimated funding level for the relevant program (or programs) with the appropriate levels under current law.

Clause 3(c)(3) of rule XIII of the Rules of the House of Representatives requires the report of any committee on a measure which has been approved by the Committee to include a cost estimate prepared by the Director of the Congressional Budget Office, pursuant to section 403 of the Congressional Budget Act of 1974, if the cost estimate is timely submitted.

Section 423 of the Congressional Budget Act requires the report of any committee on a bill or joint resolution that includes any Federal mandate to include specific information about such mandates. The Committee states that H.R. 850 does not include any Federal mandate.

The Committee adopts the cost estimate of the Congressional Budget Office as its own submission of any new required information with respect to H.R. 850 on new budget authority, new spending authority, new credit authority, or an increase or decrease in the national debt. It also adopts the estimate of Federal mandates prepared by the Director of the Congressional Budget Office pursuant to section 423 of the Unfunded Mandates Reform Act. The estimate and report which has been received is set out below.

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, June 16, 1999.

Hon. BENJAMIN A. GILMAN,
Chairman, Committee on International Relations,
House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 850, the Security and Freedom Through Encryption (SAFE) Act.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contacts are Mark Grabowicz (for costs of the Department of Justice), Mark Hadley (for costs of the

Department of Commerce), and Shelley Finlayson (for the state and local impact).

Sincerely,

BARRY B. ANDERSON
(For Dan L. Crippen, Director).

Enclosure.

H.R. 850—Security and Freedom Through Encryption (SAFE) Act

Summary: H.R. 850 would allow individuals in the United States to use and sell any form of encryption and would prohibit states or the federal government from requiring individuals to relinquish the key to encryption technologies to any third party. The bill also would prevent the Bureau of Export Administration (BXA) in the Department of Commerce from restricting the export of most nonmilitary encryption products, unless there is credible evidence that such exports would be used in connection with certain military, criminal, or terrorist activities. H.R. 850 would establish criminal penalties and fines for the use of encryption technologies to conceal incriminating information relating to a felony from law enforcement officials. Finally, the bill would require the Attorney General to maintain data on the instances in which encryption impedes or obstructs the ability of the Department of Justice (DOJ) to enforce the criminal laws.

Assuming appropriation of the necessary amounts, CBO estimates that implementing H.R. 850 would result in additional discretionary spending, by DOJ, of $3 million to $5 million over the 2000–2004 period. (The department's spending for activities related to encryption exports is negligible under current law.) Enacting H.R. 850 also would affect direct spending and receipts, beginning in fiscal year 2000, through the imposition of criminal fines and the resulting spending from the Crime Victims Fund. Therefore, pay-as-you-go procedures would apply. CBO estimates, however, that the amounts of additional direct spending and receipts would not be significant.

H.R. 850 contains intergovernmental mandates on state governments. CBO estimates, however, that states would not incur any costs to comply with the mandates. Local and tribal governments would not affected by the bill. H.R. 850 contains no new private-sector mandates as defined in the Unfunded Mandates Reform Act (UMRA).

Estimated cost to the Federal Government: The expense of compiling and maintaining data on the instances in which encryption impedes or obstructs the ability of the department to enforce the criminal laws is difficult to ascertain because the number of such instances is unknown—but DOJ believes that if H.R. 850 were enacted they would be numerous. CBO estimates that such efforts would cost DOJ between $500,000 and $1 million a year, assuming appropriation of the necessary amounts. These costs would fall within budget function 750 (administration of justice).

Under current policy, BXA would likely spend about $500,000 a year reviewing exports of encryption products, pursuant to a November 1996 executive order and memorandum that authorized BXA to control the export of all nonmilitary encryption products. If H.R. 850 were enacted, BXA would still be required to review re-

quests to export most computer hardware and software with encryption capabilities. Thus, enacting H.R. 850 would not significantly affect BXA's spending.

CBO estimates that the collections from criminal fines established by the bill—for the use of encryption technologies to conceal incriminating information relating to a felony—would not be significant.

Pay-as-you-go considerations: The Balanced Budget and Emergency Deficit Control Act sets up pay-as-you-go procedures for legislation affecting direct spending or receipts. H.R. 850 would affect direct spending and receipts by imposing criminal fines for encrypting incriminating information related to a felony. Collections of such fines are recorded in the budget as governmental receipts (i.e., revenues), which are deposited in the Crime Victims Fund and spent in subsequent years. Any additional collections under this bill are likely to be negligible because the federal government would probably not pursue many additional cases under the bill. Because any increase in direct spending would equal the fines collected (with a lag of one year or more), the additional direct spending also would be negligible.

Estimated impact on state, local, and tribal governments: H.R. 850 would preempt state law by prohibiting states from requiring persons to build decryption keys into computer hardware or software, make decryption keys available to another person or entity, or retain encryption keys. These preemptions would be mandates as defined by UMRA. However, states would bear no costs as the result of these mandates because none currently require the availability of such keys.

Estimated impact on the private sector: This bill would impose no new private-sector mandates as defined in UMRA.

Previous CBO estimates: On April 21, 1999, CBO transmitted a cost estimate for H.R. 850, the Security and Freedom Through Encryption (SAFE) Act, as ordered reported by the House Committee on the Judiciary on March 24, 1999. On July 1, 1999, CBO transmitted a cost estimate for H.R. 850 as ordered reported by the House Committee on Commerce on June 23, 1999. On July 9, 1999, CBO transmitted a cost estimate for S. 798, the Promote Reliable Online Transactions to Encourage Commerce and Trade (PROTECT) Act of 1999, as ordered reported by the Senate Committee on Commerce, Science, and Transportation on June 23, 1999. CBO estimated that the Judiciary Committee's version of H.R. 850 would cost between $3 million and $5 million over the 2000–2004 period and that the Commerce Committee's version of that bill and S. 798 would increase costs by at least $25 million over the same period.

Estimate prepared by: Federal costs: Mark Grabowicz for DOJ and Mark Hadley for BXA; impact on state, local, and tribal governments: Shelley Finlayson.

Estimate approved by: Robert A. Sunshine, Deputy Assistant Director for Budget Analysis.

SECTION-BY-SECTION ANALYSIS

Section 1. Short title

This section states that the Act may be cited at the "Security and Freedom through Encryption (SAFE) Act".

Section 2. Sale and use of encryption

This section states that Part I of Title 18, United States Code, is amended by adding a new chapter after chapter 123.

This section also creates "Chapter 125—Encrypted Wire and Electronic Information" which includes sections: 2801. Definition; 2802. Freedom to Use Encryption; 2803. Freedom to Sell Encryption; 2804. Prohibition on Mandatory Key Escrow; 2805. Unlawful Use of Encryption in the furtherance of a criminal act.

Section 2801 is titled, "definitions" and provides definitions for, "person", "State", "wire communication", "electronic communication", "investigative or law enforcement officer", and "judge of competent jurisdiction". It also defines the terms "encrypt", "encrypted" and "encryption", "key", "key recovery information", "plaintext access capability" and "United States person".

Section 2802 states that subject to Section 2805 it is legal for any person in the United States or any United States person in a foreign country, to use any form of encryption regardless of the algorithm, key length, or technique used in the encryption.

Section 2803 states that subject to Section 2805, it is legal for any person within any State to sell in interstate commerce any encryption, regardless of the encryption algorithm selected, key length or technique used. The Committee intends that Sections 2802 and 2803 be read as limitations on government power. They should not be read as overriding otherwise lawful employer policies concerning employee use of the employer's computer system, nor as limiting the employer's otherwise lawful means to remedy violations of those policies.

Section 2804 specifically prohibits requiring any person in lawful possession of an encryption key to turn that key over to another person. This section prevents any form of mandatory key escrow system with an exception for any law enforcement personnel or a member of the intelligence community. It also contains an exception whereby this prohibition does not apply to any department, agency or political subdivision of a State that has a valid contract with a non-government entity that is assisting in the performance of national security or law enforcement activity.

Section 2805 makes it a crime to use encryption unlawfully in furtherance of some other crime. This new crime is punishable with a sentence of five years for a first offense and ten years for a second or subsequent offense. It also provides that the use of encryption by any person shall not be the sole basis for establishing probable cause with respect to a criminal offense or a search warrant and makes a conforming amendment for the table of chapters for Part I of Title 18.

Section 3. Export of encryption

Subsection 3(a) of H.R. 850 amends the Export Administration Act of 1979 by creating a new subsection (g) entitled, "Certain Con-

sumer Products, Computers, and Related Equipment", to 50 U.S.C. App. 2416.

Subsection (g)(1), subject to paragraphs 2 and 3, places all encryption products under the jurisdiction of the Secretary of Commerce.

Subsection (g)(2) provides that after a one time technical review by the Secretary, to be completed no later than 30 working days after the product's submission for review, no export license may be required—except pursuant to the Trading With the Enemy Act or the International Emergency Economic Powers Act (and 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) computer hardware or software that is generally available, that is in the public domain, or that is available to the public because it is generally accessible or that is used in a commercial, off-the-shelf consumer product which includes encryption capabilities in accessible to the end user and not designed for military or intelligence end use; (B) any computing device solely because it incorporates hardware or software that is exempted from any requirement for a license under subparagraph (A); (C) any computer hardware or software with solely on the basis that it incorporates any interface mechanisms; (D) any computing devices with encryption capabilities that are not directly available to the end user or otherwise limit the encryption; (E) technical assistance used for the installation or maintenance of computer hardware or software with encryption capabilities; and (F) any encryption hardware or software not used for confidentiality purposes.

Subsection (g)(3) provides that after a one time technical review of no later than 30 working days the Secretary shall authorize the export or reexport of computer hardware or software with encryption capabilities for nonmilitary end uses in any country (A) where such exports are permitted for use by financial institutions unless there is credible evidence that there would be diversion of the computer hardware or software to military or terrorist end use or reexported without authorization or (B) if the Secretary determines that a computer hardware or software offering comparable security is commercially available outside the United States from a foreign supplier without effective restrictions.

Subsection (g)(4) states that the Secretary, before approving the export or reexport of encryption products to any major drug-transit country or any major drug producing country identified under Section 490(h) of the Foreign Assistance Act, shall consult with all relevant officials including the Attorney General, Director of the Federal Bureau of Investigation and the Administrator of the Drug Enforcement Administration on the potential impact of such export on the flow of illegal products into the U.S. It specifically does not authorize the denial of an export of an encryption product or of the issuance of a specific license solely because the country of destination is a major drug-transit country or major illicit drug producing country. The committee adopted an approach to exporting encryption devices as related to the war on drugs abroad that—irrespective where one stands on controlling the export of encryption technology—is clearly merited and was accepted by voice vote in committee. Each year, under section 490(h) of the Foreign Assist-

ance Act of 1961, as amended, the President provides to the Congress a list of those "major" drug-producing or "major" transit nations that substantially impact the United States from the flow of drugs from their nation into ours. It is only logical that there be law enforcement input and consultation into decisions whether to export encryption products to countries on the "majors" list. We should not do anything in regard to our export encryption products to countries on the "majors" list. We should not do anything in regard to our export policy to make their full cooperation with us any more difficult to obtain. This law enforcement consultation process will help to ensure that we do nothing to impair any and all law enforcement tools, including court-approved wire intercepts, which can turn the strength of the drug cartels, their command and control networks, into a weakness.

Subsection (g)(5) defines a number of terms including "encryption", "wire communication", "electronic communication", "generally available", "computing device", "computer hardware", "customer premises equipment", "technical assistance", "technical data", and "technical review".

Subsection 3(b) provides that any encryption product not requiring an export license as of the date of enactment, as a result of administrative action or rulemaking, shall not require an export license.

Subsection 3(c) states that in general nothing in the Act under the authority of the President under the International Emergency Economic Powers Act, Trading with the enemy Act or the Export Administration Act of 1979 to (A) prohibit the export of encryption products to countries determined to have provided support on a repeated basis for acts of terrorism, (B) prohibit the export of encryption products with a strength of more than 56 bits to any military unit of the People's Republic of China, including the People's Liberation Army, or (C) impose an embargo on exports to, and imports from, a specific country. The Secretary may also prohibit the export of encryption products to an individual or organization in a specific foreign country or countries identified by the Secretary, if the Secretary, in consultation with the Secretary of State, the Secretary of Defense, the Attorney General, the Director of the Federal Bureau of Investigation and the Administrator of the Drug Enforcement Administration, and the Director of Central Intelligence, determines there is credible evidence that such encryption products will be used for: (A) military or terrorist end use, (B) facilitation of the import of illicit drugs into the United States, (C) the manufacture of weapons of mass destruction or otherwise assist in the proliferation of weapons of mass destruction, or (D) illegal activities involving the sexual exploitation of minors. It also provides that any encryption product is subject to export controls for any reason other than the existence of encryption capability, including export controls imposed on high performance computers and defines the term, "encryption".

Subsection 3(d) deems the Export Administration Act of 1979 to be in effect for the purposes of carrying out the amendment made by subsection (a).

Section 4. Effect on law enforcement activities

This section directs the Attorney General to compile, and maintain in classified form, data on the instances in which encryption has obstructed or interfered with the ability of the Department of Justice to enforce the criminal law of the United States and provides that the information compiled shall be made available, upon request, to any Member of Congress.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (new matter is printed in italic and existing law in which no change is proposed is shown in roman):

TITLE 18 OF THE UNITED STATES CODE

* * * * * * *

PART I—CRIMES

* * * * * * *

125. Encrypted wire and electronic information ***2801***

* * * * * * *

CHAPTER 125—ENCRYPTED WIRE AND ELECTRONIC INFORMATION

2801. Definitions.
2802. Freedom to use encryption.
2803. Freedom to sell encryption.
2804. Prohibition on mandatory key escrow.
2805. Unlawful use of encryption in furtherance of a criminal act.

§ 2801. Definitions

As used in this chapter—

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

(2) the term "decrypt" means to retransform or unscramble encrypted data, including communications, to its readable form;

(3) the terms "encrypt", "encrypted", and "encryption" mean the scrambling of wire communications, electronic communications, or electronically stored 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 communications or information;

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

(5) the term "key recovery information" means information that would enable obtaining the key of a user of encryption;

(6) the term "plaintext access capability" means any method or mechanism which would provide information in readable form prior to its being encrypted or after it has been decrypted;

(7) 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) GENERAL PROHIBITION.—Neither the Federal Government nor a State may require that, or condition any approval on a requirement that, a key, access to a key, key recovery information, or any other plaintext access capability be—

(1) built into computer hardware or software for any purpose;

(2) given to any other person, including a Federal Government agency or an entity in the private sector that may be certified or approved by the Federal Government or a State to receive it; or

(3) retained by the owner or user of an encryption key or any other person, other than for encryption products for use by the Federal Government or a State.

(b) EXCEPTION FOR GOVERNMENT NATIONAL SECURITY AND LAW ENFORCEMENT PURPOSES.—The prohibition contained in subsection (a) shall not apply to any department, agency, or instrumentality of the United States, or to any department, agency, or political subdivision of a State, that has a valid contract with a nongovernmental entity that is assisting in the performance of national security or law enforcement activity.

(c) EXCEPTION FOR ACCESS FOR LAW ENFORCEMENT PURPOSES.—Subsection (a) shall not affect the authority of any investigative or law enforcement officer, or any member of the intelligence community as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 401a), acting under any law in effect on the effective date of this chapter, to gain access to encrypted communications or information.

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

(a) ENCRYPTION OF INCRIMINATING COMMUNICATIONS OR INFORMATION UNLAWFUL.—Any person who, in the commission of a felony under a criminal statute of the United States, knowingly and willfully encrypts incriminating communications or information relating to that felony with the intent to conceal such communications or information for the purpose of avoiding detection by law enforcement agencies or prosecution—

(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) USE OF ENCRYPTION NOT A BASIS FOR PROBABLE CAUSE.—The use of encryption by any person shall not be the sole basis for establishing probable cause with respect to a criminal offense or a search warrant.

* * * * * * *

SECTION 17 OF THE EXPORT ADMINISTRATION ACT OF 1979

EFFECT ON OTHER ACTS

SEC. 17. (a) * * *

* * * * * * *

(g) CERTAIN CONSUMER PRODUCTS, COMPUTERS, AND RELATED EQUIPMENT.—

(1) GENERAL RULE.—Subject to paragraphs (2) and (3), the Secretary shall have exclusive authority to control exports of all computer hardware, software, computing devices, customer premises equipment, communications network equipment, 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.—After a 1-time technical review by the Secretary, which shall be completed not later than 30 working days after submission of the product concerned for such technical review, no export 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 computer hardware or software or computing device, including computer hardware or software or computing devices with encryption capabilities—

(i) that is generally available;

(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

(iii) that is used in a commercial, off-the-shelf, consumer product or any component or subassembly designed for use in such a consumer product available within the United States or abroad which—

(I) includes encryption capabilities which are inaccessible to the end user; and

(II) is not designed for military or intelligence end use;

(B) any computing device solely because it incorporates or employs in any form—

(i) computer hardware or software (including computer hardware or software with encryption capabilities) that is exempted from any requirement for a license under subparagraph (A); or

(ii) computer hardware or software that is no more technically complex in its encryption capabilities than computer hardware or software that is exempted from any requirement for a license under subparagraph (A) but is not designed for installation by the purchaser;

(C) any computer hardware or software or computing device solely on the basis that it incorporates or employs in any form interface mechanisms for interaction with other computer hardware or software or computing devices, including computer hardware and software and computing devices with encryption capabilities;

(D) any computing or telecommunication device which incorporates or employs in any form computer hardware or software encryption capabilities which—

(i) are not directly available to the end user; or

(ii) limit the encryption to be point-to-point from the user to a central communications point or link and does not enable end-to-end user encryption;

(E) technical assistance and technical data used for the installation or maintenance of computer hardware or software or computing devices with encryption capabilities covered under this subsection; or

(F) any encryption hardware or software or computing device not used for confidentiality purposes, such as authentication, integrity, electronic signatures, nonrepudiation, or copy protection.

(3) COMPUTER HARDWARE OR SOFTWARE OR COMPUTING DEVICES WITH ENCRYPTION CAPABILITIES.—After a 1-time technical review by the Secretary, which shall be completed not later than 30 working days after submission of the product concerned for such technical review, the Secretary shall authorize the export or reexport of computer hardware or software or computing devices with encryption capabilities for nonmilitary end uses in any country—

(A) to which exports of computer hardware or software or computing devices of comparable strength are permitted for use by financial institutions not controlled in fact by United States persons, unless there is credible evidence that

such computer hardware or software or computing devices will be—

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

(ii) modified for military or terrorist end use; or

(iii) reexported without any authorization by the United States that may be required under this Act; or

(B) if the Secretary determines that a computer hardware or software or computing device offering comparable security is commercially available outside the United States from a foreign supplier, without effective restrictions.

(4) EXPORTS TO MAJOR DRUG-TRANSIT AND ILLICIT DRUG PRODUCING COUNTRIES.—The Secretary, before approving any export or reexport of encryption products to any major drug-transit country or major illicit drug producing country identified under section 490(h) of the Foreign Assistance Act of 1961, shall consult with the Attorney General of the United States, the Director of the Federal Bureau of Investigation, and the Administrator of the Drug Enforcement Administration on the potential impact of such export or reexport on the flow of illicit drugs into the United States. This paragraph shall not authorize the denial of an export of an encryption product, or of the issuance of a specific export license, for which such denial is not otherwise appropriate, solely because the country of destination is a major drug-transit country or major illicit drug producing country.

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

(A)(i) the term "encryption" means the scrambling of wire communications, electronic communications, or electronically stored 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 communications or information;

(ii) the terms "wire communication" and "electronic communication" have the meanings given those terms in section 2510 of title 18, United States Code;

(B) the term "generally available" means, in the case of computer hardware or computer software (including computer hardware or computer software with encryption capabilities)—

(i) computer hardware or computer software that is—

(I) distributed through the Internet;

(II) 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;

(III) preloaded on computer hardware or computing devices that are widely available for sale to the public; or

(IV) assembled from computer hardware or computer software components that are widely available for sale to the public;

(ii) not designed, developed, or tailored by the manufacturer for specific purchasers or users, except that any such purchaser or user may—

(I) supply certain installation parameters needed by the computer hardware or software to function properly with the computer system of the user or purchaser; or

(II) select from among options contained in the computer hardware or computer software;

(iii) with respect to which the manufacturer of that computer hardware or computer software—

(I) intended for the user or purchaser, including any licensee or transferee, to install the computer hardware or software and has supplied the necessary instructions to do so, except that the manufacturer of the computer hardware or software, or any agent of such manufacturer, may also provide telephone or electronic mail help line services for installation, electronic transmission, or basic operations; and

(II) the computer hardware or software is designed for such installation by the user or purchaser without further substantial support by the manufacturer; and

(iv) 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 "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;

(D) the term "computer hardware" includes, but is not limited to, computer systems, equipment, application-specific assemblies, smart cards, modules, integrated circuits, and printed circuit board assemblies;

(E) the term "customer premises equipment" means equipment employed on the premises of a person to originate, route, or terminate communications;

(F) the term "technical assistance" includes instruction, skills training, working knowledge, consulting services, and the transfer of technical data;

(G) the term "technical data" includes blueprints, plans, diagrams, models, formulas, tables, engineering designs and specifications, and manuals and instructions written or recorded on other media or devices such as disks, tapes, or read-only memories; and

(H) the term "technical review" means a review by the Secretary of computer hardware or software or computing devices with encryption capabilities, based on information

about the product's encryption capabilities supplied by the manufacturer, that the computer hardware or software or computing device works as represented.

DISSENTING VIEWS

While well-intentioned, H.R. 850 would gravely undermine the efforts of our law enforcement and national security agencies to protect the security and safety of the American people by giving our adversaries abroad and law breakers at home increased access to unrecoverable encryption. This legislation also adversely affects the Administration's ability to forge an international consensus on the creation of a multilateral export control arrangement.

We recognize that the development of strong encryption can play a vital role in promoting electronic commerce, protecting the privacy of all Americans and safeguarding our government's own data base. In the past, timely detection has prevented untold death and devastation through the monitoring of communications relating to terrorism, weapons proliferation, military operations, and other threats to U.S. security. If strong encryption is in widespread use in the near future, deciphering encrypted communications will become virtually impossible as a result of such proliferation.

Brute force attacks trying to crack cutting-edge encryption algorithms may not be feasible within a realistic time frame. For domestic law enforcement officials, strong encryption would deny access to data and communications to which they have been granted access under court order. Regrettably, since much of this important deciphering activity remains classified, much of the general public is not aware of the grave dangers of relaxing export restrictions.

The Administration does not dispute the contention of U.S. software manufacturers that encryption products above 56 bits without key recovery systems are in use around the world. First of all, foreign software companies produce and sell encryption above 56 bits. However, American products are still more sophisticated then "comparable products" or software with similar key lengths, produced by foreign competitors. Secondly, there is no doubt strong encryption can be undetectable transferred across borders and easily downloaded off the Internet. However, for complicated reasons—one of which is that consumers need to trust the suppliers of their encryption products—the surprising fact is that these products are not yet being widely used by individuals, groups, and governments which threaten the United States.

Accordingly, what H.R. 850 defines as "generally available" encryption products in a country may not be relevant in a national security context. Just because an Afghani bank in Kabul has access to high-end encryption software, it does not necessarily mean that Osama bin Laden can easily get his hands on it. Properly understood, U.S. export control policy aims not to unrealistically prevent the spread of strong encryption worldwide, but rather to discourage the flow of these products to certain groups and to give U.S. counter-encryption experts the breathing space to keep up with rapid technological advancements.

Despite the improvements made to this measure adopted by the Committee during its consideration of the SAFE Act on July 13, we remain concerned that in its present form H.R. 850 could still increase the availability of these products to individuals, groups, and governments hostile to the U.S. Specifically, this bill would allow exports of encryption to nonmilitary end-users which may inadvertently include objectionable recipients such as terrorists, criminals, certain companies potentially associated with weapons of mass destruction (WMD), and agents of proliferation that masquerade as corporate subsidiaries. Louis Freeh, Director of the Federal Bureau of Investigation (FBI) has warned, "Law enforcement remains in unanimous agreement that the widespread use of robust non-recoverable encryption will ultimately devastate our ability to fight crime and terrorism. Unbreakable encryption overseas would allow drug lords, terrorists, and even violent gangs to communicate about their criminal intentions with impunity and to maintain electronically stored evidence of the crimes impervious to lawful search and seizure."

More than one half of the annual court-ordered wire taps are at the state and local level, and of the national total for all such wire taps, more than 70 percent are for drug-related cases. Congressional action of this legislation has the potential to affect our cities and towns where the devastating impact of illicit drugs already causes nearly $70 billion in annual societal costs. We ought not to add to that carnage and destruction by denying law enforcement one of the most effective tools against this scourge, timely access to lawful requests for information needed to combat these crimes.

According to a recent analysis by the Department of Defense, H.R. 850 would impose additional difficulties for law enforcement and national security officials beyond those introduced by the elimination of the bit ceiling on encryption exports. First, this legislation would assign the Secretary of Commerce the sole authority to grant export licenses. However, the Secretary of Commerce may not be in the best position to determine whether a product will be diverted or modified. Second, the bill's definition of technical review is far from comprehensive. Third, H.R. 850 would eliminate end-use and post-export reporting which provide protection on the proper end use and monitoring of sensitive items and combat proliferation-related activities in countries of concern.

Another goal of the Administration's policy is to slow down the spread of these products enough to give U.S. led diplomacy an opportunity to achieve increased multilateral cooperation on common export control policies and on the adoption of a global key managements infrastructure. Such an infrastructure would enable U.S. intelligence and law enforcement agencies to cooperate with their counterparts in friendly countries in gaining access to communications that threaten common security and safety interests.

A level playing field, with common rules of the game, is needed to avoid giving economic rivals competitive advantages over one another. The administration made an important and correct decision in seeking an international consensus on the key recovery approach to strong encryption and must continue to work hard in seeking this common global approach. While it has yet to achieve such a consensus within the OECD, many of the key players with the

technical capability to ship advanced cryptography products and affect global markets are supporting the U.S. approach, and if a few more can be brought onboard, an international agreement on this issue can take shape.

If enacted in its current form, this bill would undermine any prospects for achieving such consensus and would compel a number of the OECD countries to put additional import restrictions in place, blocking the entry of our strongest encryption products.

We recognize the importance of American competitiveness in the encryption market for jobs and America's technological leadership. In September 1998, the Administration announced the relaxation of encryption export regulations to meet the needs of industry, the national security community as well as the average American, all to ensure that their communications remain confidential and private. Last year's update of our encryption policy opened a significant portion of the world's economies to our encryption products. As a result, the strongest encryption products with any key length can be exported to those markets that clearly require stronger encryption.

We fully support the Administration's exemption for encryption products exported to the U.S. and foreign bank and financial institutions and their customers, the health/medical sector, the insurance sector, American corporations and their overseas subsidiaries, foreign trading partners with American partners, on-line merchants, and other business categories. We urge the Administration to continue its dialogue with the private sector on expanding the scope of some of these sectors and, where appropriate, to further liberalize our export control policy over the next several months dependent on the actions of our key allies in Europe and Asia. Furthermore, as mentioned above, multilateral agreements could further minimize the impact of export controls on American software companies.

Prompted by sincere conviction, many supporters of H.R. 850 have, in our view, overstated the negative effects of the current policy on the U.S. software industry. Granted the Administration export regime is mostly unilateral, U.S. companies, nevertheless, remain on the cutting edge of the encryption industry and we applaud the Administration's efforts in helping to open 80 percent of the world's economies to U.S. encryption products.

BENJAMIN A. GILMAN.
DOUG BEREUTER.

ADDITIONAL DISSENTING VIEWS

As a general matter, there is a very strong argument to eliminate export controls where those controls are made ineffective by reason of the wide availability of products similar to those being controlled. In the context of today's encryption marketplace, in which encryption products are widely available throughout much of the world, it is reasonable to ask how export controls can inhibit the availability of strong encryption to terrorist organizations or militaries adverse to U.S. interests. But for the time being, controls continue to have significant effectiveness. The arguments put forth in closed briefings by the national security and law enforcement community distinguishing "wide availability" from "side usages" are unassailable.

It is generally accepted that *if* there were a binding multilateral agreement that would effectively control exports of strong encryption, such a multilateral approach, with international cooperation, would be preferable to unilateral decontrol. Our best option is to encourage the President to take steps to make the currently non-binding Wassenaar Arrangement binding upon the 33 countries that are signatory. Alternatively, we should encourage the president to take the lead in developing a new binding multilateral agreement on the control of dual-use technologies, including encryption. I offered an amendment that would acknowledge this preference by providing simply that nothing in H.R. 850 would limit the President's ability to meet U.S. obligations pursuant to a binding multilateral agreement.

In contrast to the validity of the national security arguments, some of the arguments put forth by proponents of H.R. 850 are not persuasive. For example, the countries most cited as relaxing encryption export controls are either in a similar stage of analysis as the U.S., in that they maintain a licensing regime and are simply considering the evolution of that regime to keep pace with the development of new technologies, or they currently have a far more stringent policy than the U.S. Thus, a "relaxation" of their policy would not result in a more relaxed policy than the current Clinton Administration policy. Further, proponents argue that U.S. manufacturers have very limited access to foreign markets. However, according to the Administration, and I have not heard this fact disputed, over 80% of the legitimate world market for encryption can be accessed by U.S. manufacturers under the Administration's current policy for license exceptions. This is not to say that the license exception process cannot be improved, or that the Clinton Administration policymaking is adequately keeping pace with technological evaluation. However, I take issue with the approach of H.R. 850, essentially a unilateral, complete and instant decontrol of the export of the strongest encryption without effective means for the government to address national security concerns.

It is not necessary to essentially eliminate export controls, as H.R. 850 does, to meet the needs of encryption manufactures and those who want to be able to export and use strong encryption products. Some proponents of H.R. 850 acknowledge this. Testifying before the House Permanent Select Committee on Intelligence on June 9, 1999, Christopher Caine, Vice President, Governmental Programs, IMB Corporation, emphasized that as to encryption, "a good dynamic regulatory approach is the best solution," absent that, IBM supports H.R. 850. In fact, Mr. Caine had a much more moderate view of what was needed when compared to this bill. Not, as he characterized the view of some proponents, "a binary approach—all or nothing."

This bill is an all or nothing proposition. Were this bill enacted, there would be no effective controls on export even to the seven countries known to the U.S. government as supporters of terrorist activities. H.R. 850, as introduced, pays lip service to the concerns that strong encryption should be controlled sufficiently to avoid exports to these seven countries, and to countries subject to an embargo or to individuals or organizations involved in terrorist or military activity. There are provisions in the bill to theoretically prohibit such export, but there are no effective means to implement these provisions. There is no effective mechanism for the government to identify the destination of even the strongest encryption products. In fact, the provisions of H.R. 850 preclude such review.

Were this bill enacted as introduced, the Secretary of Commerce would be unable to obtain from the manufacturer sufficient information to determine the destinations where the encryption product may be exported or consult with the proper government experts to determine the national security implications. H.R. 850 originally provided for a one-time, 15-day "technical review" by only the Secretary of Commerce prior to export. I offered an amendment that in part, extended the technical review to 30 working days. Of the several provisions within my amendment, only this extension of the duration of the review was adopted—however, my goal was to make this review meaningful, as well as of sufficient duration.

The current "technical review" is simply a "product review," wherein the government can assess only that the product works as described by the manufacturer. This review does not allow for assessment of the actual or potential destinations for the encryption product, does not allow the government to require a manufacturer to disclose how the product actually works, and does not allow for the government to require disclosure of the quantity of the product that is expected to be exported, or is actually exported after the review. This information is necessary for the government to assess where a product could be used and by whom. Under the H.R. 850 "technical review," there is no opportunity for the government to determine where the product may end up. As to national security concerns, it is a meaningless review.

My amendment would have given the government the opportunity to get the information that it needs to decide if it should restrict an export to keep it out of the hands of terrorists or adverse military end-users, as it does today. Specifically, it would have given the Secretary of Commerce the opportunity to consult with the Secretaries of State and Defense, the Attorney General and the

Director of the CIA, those who have the information needed to properly assess the risks to national security. Further, my amendment would have allowed the government to require a manufacturer to periodically report where a product is actually exported to, and in what quantity. Simple mechanisms, within a reasonable time frame—a system adequate to keep track of strong encryption and substantially maintain the government's current ability to keep strong encryption out of the wrong hands.

Further, the one-time technical review provided for in H.R. 850 does not provide for any reporting if the product undergoes significant changes. A more familiar example of the kind of change I am referring to is that of Microsoft Windows. This product, introduced as Windows in 1985 was extraordinarily less sophisticated than Windows 95, and even further from what we can expect from Windows 2000. And we certainly know that the evolution of a product can now be much faster. But under this provision, if this were an encryption product, after the review of the original Windows product, no further reporting about the capabilities of the evolved product could be required. A simple encryption product, possibly not even what is currently considered strong encryption, could be submitted for technical review. After a year, the product may evolve to provide very sophisticated strong encryption. But the manufacturer can continue to export the evolved product pursuant to the "one-time technical review" of the original product. This problem is exasperated by the fact that many manufacturers submit products for government review before the product is "final." Substantial changes may occur between the time of review and the time the product is made commercially available. My amendment would have addressed this problem by allowing the Secretary of Commerce to require reporting by the manufacturer of any significant changes to the product.

I am not opposed to relaxing export controls on encryption products. However, we should not do so to such an extent that we exacerbate the availability of strong encryption to terrorists, criminals and adverse military end-users in a manner disproportionate to the benefit achieved for manufacturers and legitimate users of encryption products. As we consider H.R. 850, we should keep in mind that the Administration's policy is evolving. The remedy to the problems with the current policy may better be addressed by administrative changes, rather than legislation that is essentially a complete decontrol of exports of strong encryption. If we are to provide a legislative remedy, we should not do it at the peril of national security.

HOWARD L. BERMAN.

○