105TH CONGRESS, 1st Session | HOUSE OF REPRESENTATIVES | REPT. 105–108, Part 2

SECURITY AND FREEDOM THROUGH ENCRYPTION (SAFE) ACT

JULY 25, 1997.—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. 695]

The Committee on International Relations, to whom was referred the bill (H.R. 695) 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 121 the following new chapter:

"CHAPTER 122—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', 'judge of competent jurisdiction', and 'electronic storage' have the meanings given those terms in section 2510 of this title;

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

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

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

"(A) any United States citizen;

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

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

"§ 2802. Freedom to use encryption

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

"§ 2803. Freedom to sell encryption

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

"§ 2804. Prohibition on mandatory key escrow

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

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

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

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

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

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

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

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

"(2) ITEMS NOT REQUIRING LICENSES.—No validated license may be required, except pursuant to the Trading With The Enemy Act or the International Emergency Economic Powers Act (but only to the extent that the authority of such

Act is not exercised to extend controls imposed under this Act), for the export or reexport of—

"(A) any consumer product commercially 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 component or subassembly designed for use in a consumer product described in subparagraph (A) which itself contains encryption capabilities and is not capable of military or intelligence end use in its condition as exported;

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

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

"(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 customized for an otherwise lawful use by a specific purchaser or group of purchasers;

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

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

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

"(E) any computer hardware that is generally available, solely because it has encryption capabilities; or

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

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

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

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

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

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

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

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

"(B) the term 'generally available' means—

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

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

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

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

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

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

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

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

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

SEC. 4. SENSE OF CONGRESS REGARDING INTERNATIONAL COOPERATION.

(a) FINDINGS.—The Congress finds that—

(1) implementing export restrictions on widely available technology without the concurrence of all countries capable of producing, transshipping, or otherwise transferring that technology is detrimental to the competitiveness of the United States and should only be imposed on technology and countries in order to protect the United States against a compelling national security threat; and

(2) the President has not been able to come to agreement with other encryption producing countries on export controls on encryption and has imposed excessively stringent export controls on this widely available technology.

(b) SENSE OF CONGRESS.—It is the sense of the Congress that the President should immediately take the necessary steps to call an international conference for the purpose of coming to an agreement with encryption producing countries on policies which will ensure that the free use and trade of this technology does not hinder mutual security.

BACKGROUND AND PURPOSE

H.R. 695, the Security and Freedom Through Encryption (SAFE) Act, represents a strong bipartisan effort to bring U.S. laws on the export of encryption technology into the present and future, by looking at the actual technological developments taking place on the world stage. The SAFE Act enjoys strong support in the House as reflected by the overwhelming number of co-sponsors, including a majority of the Members of the Committee on International Relations.

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 re-

cipients 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 is corresponds to the number of possible combinations that can be used to decode a particular message. A 40-bit key means that 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 that 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, weather satellites, social security system, television networks, civilian and government payrolls, and the Internet are all directly affected by a flow of data managed by countless computers and telecommunication networks around the world. Computer technology now serves as the nervous system of modern society.

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 intrusions, 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 40 bits long—determined to be gravely inadequate by numerous experts. The current Administration proposal, which would allow the export of 56-bit encryption, 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, on the same day that the companion legislation—the McCain-Kerrey bill—was introduced in the Senate calling for a 56-bit limit on encryption exports, a group of independent programmers and researchers cracked a 56-bit code using computers linked across the Internet. This successful breaking of 56-bit encryption clearly dem-

onstrates the anachronistic nature of current U.S. law and reflects how out-of-touch the Administration's policy is with the needs of the global marketplace.

The Administration's proposal would only allow the export of 56-bit encryption 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 it is necessary to decode the plaintext data as part of an 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 of 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 40-bit encryption or at 56-bit 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.

Furthermore, 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 exportable products subject to the same restrictions as their domestic 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 the 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 on. The Software Publishers Association has documented hundreds of foreign encryption products already widely available abroad and which criminals, terrorists, and foreign governments have access to. It is the upstanding, law-abiding citizen who suffers.

The fact is that strong encryption helps to further the goals of law enforcement and national security, more than key recovery could ever hope to. 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.

In summary, if U.S. laws are not changed soon, not as mandated by the Administration's policy or its companion legislation in the Senate, but as H.R. 695 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. government will not have a view into the security technology that replaces U.S. tech-

nology as the world standards. U.S. industries will lose control of information security technologies which are vital to economic security. It will cost the U.S. economy billions of dollars and hundreds of thousands of jobs.

On July 7, 1997, German Economics Minister Guenter Rexrodt called for the removal of restrictions on encryption technology in his opening remarks for 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 as other countries provide their own people and industries. H.R. 695—the SAFE Act—does just that. It is aimed at correcting the unfair and unsafe situation that currently exists under current law as it: prohibits export controls on "generally available" commercial encryption except for military end-users or to identified individuals or organizations in specific foreign countries; does not require reporting for companies after export; prohibits mandatory use of key recovery; denies liability protection and penalties for key holders; denies foreign government access to keys under specified conditions if key holder is used voluntarily; prohibits U.S. government and law enforcement access to keys by court order if key holder is used voluntarily; codifies existing domestic use policy; gives the Secretary of Commerce exclusive jurisdiction over export of commercial encryption except for military end-uses or to identified individuals or organizations in specific foreign countries.

In essence, H.R. 695 prevents economic espionage while protecting hundreds of thousands of American jobs by affording all Americans the freedom to use any type of encryption anywhere in the world; by allowing 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. 695 as it works its way through the legislative process. In the interest of the American people, of U.S. economic leadership and growth, and of national security, the Committee hopes that the House will pass the SAFE Act.

COMMITTEE ACTION

H.R. 695 was introduced by Representative Goodlatte on February 12, 1997, and referred to the Committee on Judiciary and in addition to the Committee on International Relations for a period subsequently to be determined by the Speaker. It was reported to the House by the Committee on the Judiciary, amended, on May 22, 1997 (H. Rept. 105-108). On May 22, 1995, the referral to the Committee on International Relations was extended through July 11, 1997, and on June 26, 1997, the referral to the Committee on International Relations was extended for a period ending not later than July 25, 1997.

On June 26, 1997, the bill was referred, in addition, to Committees on Commerce, National Security, and the Permanent Select Committee on Intelligence for a period ending not later than September 5, 1997, for consideration of such provisions of the bill and the amendment reported by the Committee on the Judiciary as fall within the jurisdiction of those committees pursuant to clause 1(3) and (k), rule X and rule XLVIII, respectively.

On May 8, 1997, the Subcommittee on International Economic Policy and Trade held a hearing entitled: "Encryption: Individual Right to Privacy vs. National Security." Witnesses for this hearing included: Hon. William Reinsch, Under Secretary of Commerce, Bureau of Export Administration; Hon. William Crowell, Deputy Director, National Security Agency; Hon. Robert Litt, Deputy Assistant Attorney General, Criminal Division, U.S. Department of Justice; Mr. John Gage, Director, Science Office, Sun Microsystems, Inc.; Mr. Humphrey Polanen, General Manager, Network Security Products Group, Sun Microsystems, Inc.; Jerry Berman, Executive Director, Center for Democracy and Technology; Tom Parenty, Director of Security, Sybase Corporation; and Stephen T. Walker, President and CEO, Chairman of the Board of Directors, Trusted Information Systems.

On May 29, 1997, the Full Committee held a Members briefing on H.R. 695, "the Security and Freedom through Encryption (SAFE) Act." Speakers for the briefing included Hon. Louis Freeh, Director, Federal Bureau of Investigation and Hon. William Crowell, Deputy Director, National Security Agency.

On June 4, 1997, the Subcommittee on International Economic Policy and Trade held a Members Briefing on the future of U.S.-European trade relations. Speakers for the briefing included: Hon. David L. Aaron, U.S. Ambassador to the Organization for Economic Cooperation and Development (OECD); H.E. Hugo Paemen, Head of the Delegation to the United States of the Commission of the European Union; and Dr. Dominique vanderMensbrugghe, Senior Economist, OECD Development Center.

On June 24, 1997, the Subcommittee on International Economic Policy and Trade held a mark-up of H.R. 695, "the Security and Freedom through Encryption (SAFE) Act". Witnesses included: Congressman Bob Goodlatte.

Amendment.—An en bloc amendment was offered by Ros-Lehtinen, Gejdenson, Campbell and Sherman. The amendment removes the distinction between mass market and customized software thus ensuring that customized software is also subject to liberalized export controls. It expands section 3 on exports of encryption by including consumer products which do not necessarily fall under the umbrella of "computing" products but which also require and use encryption. It broadens the scope and definition of "generally available" to include hardware with encryption capabilities. The amendment also adds a fourth section to the bill in the form of a sense of Congress regarding international cooperation. The amendment passed by voice vote.

A motion to report the bill, as amended, to the Full Committee passed by a roll call vote, as follows:

Voting yes: Ros-Lehtinen, Manzullo, Chabot, Campbell, Blunt, Brady, Rohrabacher, Gejdenson, Danner, Hilliard, Sherman, Rothman, Clement, Luther.

Voting no: Bereuter.

Passed: 14–1.

On June 26, 1997, the Full Committee held a classified Members briefing on the impact of H.R. 695, "the Security and Freedom through Encryption (SAFE) Act" on national security and law enforcement activities. Speakers for the briefing included: Hon. Louis Freeh, Director, Federal Bureau of Investigation; Hon. William Crowell, Deputy Director, National Security Agency; Hon. William Reinsch, Under Secretary of Commerce, Bureau of Export Administration.

On July 22, 1997, the Full Committee marked up the bill in open session, pursuant to notice. The Committee first adopted the amendment recommended by the Subcommittee on International Economic Policy by unanimous consent, as original text for the purposes of amendment. Representatives Goodlatte and Lofgren and representatives of the Administration (The Hon. William Reinsch, Under Secretary of Commerce; Mr. Jim Kallstrom, Federal Bureau of Investigation; Mr. James R. Taylor, National Security Agency; and Mr. Anthony Bocchichio of the Drug Enforcement Agency) responded to questions from members during the course of the markup.

After further consideration, on that date, a quorum being present, the Full Committee by voice vote ordered the bill reported to the House with the recommendation that the bill, as amended, do pass.

ROLLCALL VOTES ON AMENDMENTS

In compliance with clause (2)(l)(2)(B) of rule XI of the Rules of the House of Representatives, the record of committee roll call votes on final passage or amendments during the full committee's consideration of H.R. 695 is set out below, as is a report of the full committee's final action on the bill.

Description of Amendment, Motion, Order, or Other Proposition (votes during markup of H.R. 695—July 22, 1997)

Vote No. 1.—Gilman amendment provide that certain items could not be exported if in the opinion of the President they would endanger the national security.

Voting Yes: Gilman, Leach, Bereuter, Gallegly, Fox, Hamilton, Berman, Menendez, Brown, Danner, Rothman, Clement, and Davis.

Voting No: Smith, Ros-Lehtinen, Ballenger, Rorhabacher, Manzullo, Royce, King, Chabot, Sanford, Houghton, Campbell, Blunt, Moran, Brady, Gejdenson, Ackerman, Hastings, Hilliard, Capps, Sherman, Wexler, and Luther.

Ayes, 13. Noes, 22.

Note: The bill was subsequently ordered reported favorably, amended, by voice vote, a quorum being present, on July 22, 1997.

SECTION-BY-SECTION ANALYSIS

SECTION 1. SHORT TITLE

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

SECTION 2. SALE AND USE OF ENCRYPTION

This section states that, in general, Part I of Title 18, United States Code, is amended by adding a new chapter after chapter 121.

This section also creates "Chapter 122-Encrypted Wire And Electronic Information" which includes sections; 2801. Definitions., 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", judge of competent jurisdiction", "electronic storage", "encrypt", "encryption", "key", and "United States person". Many of these definitions were taken explicitly from 18 U.S.C. 2810.

New section 2802 states that 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.

New section 2803 states that it is legal for any person in the United States to sell in interstate commerce encryption products using any form of encryption regardless of the algorithm, 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 employers computer system, nor as limiting the employer's otherwise lawful means for remedying violations of those policies.

New 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.

New section 2805 make it a crime to use encryption unlawfully in furtherance of some other crime. This new crime is punishable with a sentence of 5 years for a first offence and 10 years. This section requires that for a person to violate this section that person must be found guilty of some other federal felony crime and was deliberately using encryption to avoid detection of that other federal felony crime.

Subsection 2(b) of H.R. 695 provides for a conforming amendment to the table of chapters in Title 18.

SECTION 3. EXPORT OF ENCRYPTION

Subsection 3(a) of H.R. 695 amends the Export Administration Act by creating a new subsection (g) entitled "Computers and Related Equipment," to 50 U.S.C. App. 2416.

New subsection (g)1 place all encryption products, except those specifically designed or modified for military use, under the jurisdiction of the Secretary of Commerce.

New subsection (g)2 allows encryption software that is generally available or in the public domain, like mass-market software products, to be exported freely except pursuant to the Trading With The Enemy Act or the International Emergency Economic Powers Act (but only to the to the extent that the authority of such Act is not exercised to extend controls imposed under this Act.). The Subcommittee on International Economic Policy and Trade, on an amendment offered by Chair Ros-Lehtinen and Ranking Member Gejdenson, and others, amended Subsection (g)2 on a voice vote in Subcommittee to include certain other consumer products, or component or subassembly (provided those components are not capable of military or intelligence end use in its condition as exported.), which have encryption capabilities that are inaccessible to the end user and which are commercially available within the United States or abroad. These product as discussed by the Subcommittee are consumer products such as small dish satellite receivers, digital video disk players, smart cards, Web TV, etc. These products, which are commercially available within the United States or abroad, were viewed by the Subcommittee as being clearly and purely for consumer end-use and not for military purposes. The Ros-Lehtinen amendment also amended (g)2 to include customized software for an otherwise lawful purpose by a specific purchaser or group of purchasers.

New subsection (g)3 requires the Secretary of Commerce to allow other encryption software to be exported unless there is substantial evidence that will be put to military or terrorist uses or that it will be reexported without U.S. authorization.

New subsection (g)4 requires the Secretary to allow the export of hardware with encryption capabilities when the Commerce Department finds that it is commercially available from foreign suppliers without effective restrictions.

New subsection (g)5 provides definitions for this subsection. The subcommittee amendment offered by Chair Ros-Lehtinen, and others also amended this subsection to include the same consumer products added to subsection (g)2.

As the Ros-Lehtinen amendment adopted in the Subcommittee on International Economic Policy and Trade stated, the Committee would like to reiterate that, with the ever increasing use of computer technology and computer information (hardware and software) in consumer product lines for protection of privacy, information security, and intellectual property interests, it intends this legislation to cover all devices—whether traditional computing devices or convergent consumer products that incorporate encryption. The applications covered by this legislation include video, audio, and data communications systems and telecommunication equipment. Hardware and software containing encryption, such as encoders, decoders, and network terminals, which are essential to protect the video signal, are therefore included under section 3(a) of this Act. As well as video, audio, data communications systems containing encryption and decryption capability are used by cable, satellite, and wireless delivery systems. This legislation is also intended to

include set-top devices and other terminals where the encryption is not directly available to the user but is used for purposes such as pay per view, and hardware such as network computers, telephones or cable modems, satellite uplinks and downlinks.

Subsection 3(b) of H.R. 695 provides that for the purposes of carrying out the amendment made by subsection 3(a), the Export Administration Act shall be deemed to be in effect. This statement is necessary because Congress failed to reauthorize the Export Administration Act and it expired in 1994. The Administration maintains the Export Administration Act policies by executive order. The Committee plans to reauthorize the Export Administration Act in this Congress.

SECTION 4. SENSE OF CONGRESS REGARDING INTERNATIONAL COOPERATION

This section asks on the President to call an international conference for the purpose of achieving an agreement among the encryption producing countries on policies which will ensure that the free use and trade of this technology does not hinder mutual technology.

COMMITTEE OVERSIGHT FINDINGS

In compliance with clause 2(l)(3)(A) of rule XI 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 AND OVERSIGHT FINDINGS

No findings or recommendations of the Committee on Government Reform and Oversight were received as referred to in clause 2(l)(3)(D) of rule XI of the Rules of the House of Representatives.

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 2(l)(4) of rule XI 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. 695 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); and Article I, section 8, clause 18 (relating to making all laws necessary and proper for car-

rying into execution powers vested by the Constitution in the government of the United States).

NEW BUDGET AUTHORITY AND TAX EXPENDITURES, CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

The Committee expects to adopt a cost estimate of the Congressional Budget Office as its submission of any new required information on new budget authority, new spending authority, new credit authority, or an increase or decrease in the national debt, which it expects to provide in a supplemental report.

FEDERAL MANDATES STATEMENT

The Committee adopts as its own the estimate of Federal mandates prepared by the Director of the Congressional Budget Office pursuant to section 423 of the Unfunded Mandates Reform Act.

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, July 25, 1997.

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

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed mandates statement for H.R. 695, the Security and Freedom Through Encryption (SAFE) Act. CBO's analysis of the bill's federal costs will be sent to you as soon as it is completed.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contacts are Pepper Santalucia (for the state and local impact) and Matt Eyles (for the private-sector impact).

Sincerely,

JANE E. O'NEILL, *Director.*

Enclosure.

CONGRESSIONAL BUDGET OFFICE MANDATES STATEMENT

H.R. 695—Security and Freedom Through Encryption (SAFE) Act

H.R. 695 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 in the Department of Commerce from restricting the export of most nonmilitary encryption products. Finally, H.R. 695 would establish criminal penalties and fines for the willful use of encryption technologies in committing criminal offenses.

The bill would prohibit states from requiring persons to make encryption keys available to another person or entity. This prohibition would be an intergovernmental mandate as defined in the Unfunded Mandates Reform Act of 1995 (UMRA). However, states would bear no costs as a result of this mandate because none currently require the registration or availability of such keys. H.R. 695 contains no private-sector mandates as defined in UMRA.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3 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, UNITED STATES CODE

* * * * * * *

PART I—CRIMES

Chap.		Sec.
1.	**General provisions**	**1**
	* * * * * * *	
122.	***Encrypted wire and electronic information***	***2801***
	* * * * * * *	

CHAPTER 122—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", "judge of competent jurisdiction", and "electronic storage" have the meanings given those terms in section 2510 of this title;

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

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

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

(A) any United States citizen;

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

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

§ 2802. Freedom to use encryption

Subject to section 2805, it shall be lawful for any person within any State, and for any United States person in a foreign country,

to use any encryption, regardless of the encryption algorithm selected, encryption key length chosen, or implementation technique or medium used.

§ 2803. Freedom to sell encryption

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

§ 2804. Prohibition on mandatory key escrow

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

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

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

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

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

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

* * * * * * *

SECTION 17 OF THE EXPORT ADMINISTRATION ACT OF 1979

SEC. 17. (a) * * *

* * * * * * *

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

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

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

(A) any consumer product commercially 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 component or subassembly designed for use in a consumer product described in subparagraph (A) which itself contains encryption capabilities and is not capable of military or intelligence end use in its condition as exported;

(C) any software, including software with encryption capabilities—

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

(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 customized for an otherwise lawful use by a specific purchaser or group of purchasers;

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

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

(ii) software that is no more technically complex in its encryption capabilties than software that is exempted from any requirement for a validated license under subparagraph (C) but is not designed for installation by the purchaser;

(E) any computer hardware that is generally available, solely because it has encryption capabilities; or

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

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

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

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

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

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

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

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

(B) the term "generally available" means—

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

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

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

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

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

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

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

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

DISSENTING VIEWS

While well-intentioned, this bill's one-dimensional focus on the decontrol of encryption products would upset the vital balance that U.S. policy seeks to strike between the competitiveness of American industry and U.S. national security and law enforcement goals. The bill would prohibit any licensing or review of exports of encrypted software and hardware items. Consequently, its implementation would not only hinder our national security efforts but also undermine the Administration's ability to forge an international consensus on the use and implementation of national key recovery policies.

While SAFE Act advocates correctly point out that the Administration has not yet achieved a multilateral consensus endorsing its preference for a key management infrastructure approach on encryption issues, it should be noted that recent cryptography guidelines adopted by the Organization for Economic Cooperation and Development have stressed the need to balance privacy, law enforcement, national security concerns, and commercial interests. They also underline the fact that failure to coordinate these policies could cripple the global information network and impede international trade.

A July policy brief published by the Brookings Institution by Kenneth Flamm on "Deciphering the Cryptography Debate" noted along the same lines that:

"A level playing field, with common global 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 be sure to 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—Britain, France and (quietly) Japan—are supporting the U.S. approach, and if a few more (like Germany and Israel) can be brought on board, the critical mass around which the core of an international agreement can be assembled will exist."

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 that the development of strong encryption can play a vital role in the development of electronic commerce and promoting privacy but the development of key recovery policies is essential to head off a potential crisis in the years ahead for our law enforcement authorities. If strong encryption is in widespread use in the near future, it will make it virtually impossible to decipher

encrypted communications. Brute force attacks to crack encryption algorithms in that type of environment are not feasible or realistic, especially in the time sensitive cases where law enforcement needs access to encrypted files to save lives.

By removing all controls on the export of any software and hardware with encryption capabilities, this bill threatens U.S. national security and law enforcement interests.

With respect to U.S. national security, encrypted communications make it more difficult for U.S. intelligence agencies to monitor communications relating to terrorism, weapons proliferation, military operations, and other threats to U.S. national security interests. The Administration does not dispute the contention of U.S. software manufacturers that encryption products are in use around the world.

But the Administration also points out that these products are not yet being widely used by individuals, groups, and governments whose activities pose threats to U.S. security and safety. As we understand it, the goal of U.S. export control policy is not to prevent the spread of encryption worldwide—something which clearly cannot be done—but 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 management infrastructure. Such an international key management 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.

The elimination of all U.S. controls on encryption exports will also jeopardize domestic law enforcement. We recognize that encryption is essential to the fulfillment of the promise of electronic commerce and to the protection of individual privacy in a networked world. But encryption also complicates the mission of U.S. law enforcement agencies, because it can make it impossible for law enforcement personnel to understand data and communications to which they have been granted access under court order or other proper legal authority.

This is why current U.S. policy seeks to promote the adoption of key recovery features in encryption products used in the United States. Export controls are a key component of this policy. Under current practice, U.S. firms are permitted to export powerful encryption products if they already include key recovery features or if they pledge to develop such features during the next two years. If we eliminate all U.S. export controls, as this bill would do, the federal government will therefore lose one of its most important means for promoting the development of key recovery in the U.S. market. That will harm U.S. law enforcement.

Lawful wiretapping and duly authorized court-ordered access to information and materials on a timely basis are essential tools for police and law enforcement authorities. If this legislation were to be enacted in its present form, the resultant proliferation of global and interconnected encryption has the very real potential to deny our local, state and federal authorities the timely access they now enjoy to data and other communications, even after a court order has been issued.

More than one half 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% are for drug-related cases. Congressional action on 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.

Attorney General Janet Reno, our nation's chief law enforcement officer, urged the members of our Committee to consider the effects of this legislation in her July 18, 1997, letter to the International Relations Committee. She said that "* * * the misuse of encryption technology will become a matter of life and death in many instances. That is why we urge you to adopt a balanced approach." We invite the attention of Members to correspondence from our Nation's law enforcement and national security leaders, appended below.

During the full committee's consideration of H. R. 695, Chairman Gilman offered an amendment which would have helped to create this necessary balance in the bill. It would have provided the President the authorities to control the export and reexport of encrypted items if he determines that they would adversely affect our national security and our ability to fight crimes such as drug trafficking, terrorism and espionage. This amendment was, unfortunately, not adopted.

Other Committees of the House including National Security, Intelligence and Commerce will now review this legislation through September 5 before it is considered by the full House later this year. We urge our colleagues on these Committees as well as our colleagues on the International Relations and the Judiciary Committees to review this legislation very carefully and consider its impact on our society and our ability to fight terrorism and protect our national security interests.

BENJAMIN A. GILMAN.
LEE H. HAMILTON.
DOUG BEREUTER.

OFFICE OF THE ATTORNEY GENERAL,
Washington, DC, July 18, 1997.

DEAR MEMBER OF CONGRESS: Congress is considering a variety of legislative proposals concerning encryption. Some of these proposals would, in effect, make it impossible for the Federal Bureau of Investigation (FBI), Drug Enforcement Administration (DEA), Secret Service, Customs Service, Bureau of Alcohol, Tobacco and Firearms, and other federal, state, and local law enforcement agencies to lawfully gain access to criminal telephone conversations or electronically stored evidence possessed by terrorists, child pornographers, drug kingpins, spies and other criminals. Since the impact of these proposals would seriously jeopardize safety and national security, we collectively urge you to support a different, balanced approach that strongly supports commercial and privacy interests

but maintains our ability to investigate and prosecute serious crimes.

We fully recognize that encryption is critical to communications security and privacy, and that substantial commercial interests are at stake. Perhaps in recognition of these facts, all the bills being considered allow market forces to shape the development of encryption products. We, too, place substantial reliance on market forces to promote electronic security and privacy, but believe that we cannot rely solely on market forces to protect the public safety and national security. Obviously, the government cannot abdicate its solemn responsibility to protect public safety and national security.

Currently, of course, encryption is not widely used, and most data is stored, and transmitted, in the clear. As we move from a plain text world to an encrypted one, we have a critical choice to make: we can either (1) choose robust, unbreakable encryption that protects commerce and privacy but gives criminals a powerful new weapons, or (2) choose robust, unbreakable encryption that protects commerce and privacy and gives law enforcement the ability to protect public safety. The choice should be obvious and it would be a mistake of historic proportions to do nothing about the dangers to public safety posed by encryption without adequate safeguards for law enforcement.

Let there be no doubt: without encryption safeguards, all Americans will be endangered. No one disputes this fact; not industry, not encryption users, no one. We need to take definitive actions to protect the safety of the public and security of the nation. That is why law enforcement at all levels of government—including the Justice Department, Treasury Department, the National Association of Attorneys General, International Association of Chiefs of Police, the Major City Chiefs, the National Sheriffs' Association, and the National District Attorneys Association—are so concerned about this issue.

We all agree that without adequate legislation, law enforcement in the United States will be severely limited in its ability to combat the worst criminals and terrorists. Further, law enforcement agrees that the widespread use of robust non-key recovery encryption ultimately will devastate our ability to fight crime and prevent terrorism.

Simply stated, technology is rapidly developing to the point where powerful encryption will become commonplace both for routine telephone communications and for stored computer data. Without legislation that accommodates public safety and national security concerns, society's most dangerous criminals will be able to communicate safely and electronically store data without fear of discovery. Court orders to conduct electronic surveillance and court-authorized search warrants will be ineffectual, and the Fourth Amendment's carefully-struck balance between ensuring privacy and protecting public safety will be forever altered by technology. Technology should not dictate public policy, and it should promote, rather than defeat, public safety

We are not suggesting the balance of the Fourth Amendment be tipped toward law enforcement either. To the contrary, we only seek the status quo, not the lessening of any legal standard or the

expansion of any law enforcement authority. The Fourth Amendment protects the privacy and liberties of our citizens but permits law enforcement to use tightly controlled investigative techniques to obtain evidence of crimes. The result has been the freest country in the world with the strongest economy.

Law enforcement has already confronted encryption in high-profile espionage, terrorist, and criminal cases. For example:

> An international terrorist was plotting to blow up 11 U.S.-owned commercial airliners in the Far East. His laptop computer, which was seized in Manila, contained encrypted files concerning this terrorist plot;
>
> A subject in a child pornography case used encryption in transmitting obscene and pornographic images of children over the Internet; and
>
> A major international drug trafficking subject recently used a telephone encryption device to frustrate court-approved electronic surveillance.

And this is just the tip of the iceberg. Convicted spy Aldrich Ames, for example, was told by the Russian Intelligence Service to encrypt computer file information that was to be passed to them.

Further, today's international drug trafficking organizations are the most powerful, ruthless and affluent criminal enterprises we have ever faced. We know from numerous past investigations that they have utilized their virtually unlimited wealth to purchase sophisticated electronic equipment to facilitate their illegal activities. This has included state of the art communication and encryption devices. They have used this equipment as part of their command and control process for their international criminal operations. We believe you share our concern that criminals will increasingly take advantage of developing technology to further insulate their violent and destructive activities.

Requests for cryptographic support pertaining to electronic surveillance interceptions from FBI Field Offices and other law enforcement agencies have steadily risen over the past several years. There has been an increase in the number of instances where the FBI's and DEA's court-authorized electronic efforts were frustrated by the use of encryption that did not allow for law enforcement access.

There have also been numerous other cases where law enforcement, through the use of electronic surveillance, has not only solved and successfully prosecuted serious crimes but has also been able to prevent life-threatening criminal acts. For example, terrorists in New York were plotting to bomb the United Nations building, the Lincoln and Holland Tunnels, and 26 Federal Plaza as well as conduct assassinations of political figures. Court-authorized electronic surveillance enabled the FBI to disrupt the plot as explosives were being mixed. Ultimately, the evidence obtained was used to convict the conspirators. In another example, electronic surveillance was used to stop and then convict two men who intended to kidnap, molest, and kill a child. In all of these cases, the use of encryption might have seriously jeopardized public safety and resulted in the loss of life.

To preserve law enforcement's abilities, and to preserve the balance so carefully established by the Constitution, we believe any

encryption legislation must accomplish three goals in addition to promoting the widespread use of strong encryption. It must establish:

A viable key management infrastructure that promotes electronic commerce and enjoys the confidence of encryption users;

A key management infrastructure that supports a key recovery scheme that will allow encryption users access to their own data should the need arise, and that will permit law enforcement to obtain lawful access to the plain text of encrypted communications and data; and

An enforcement mechanism that criminalizes both improper use of encryption key recovery information and the use of encryption for criminal purposes.

Only one bill, S. 909 (the McCain/Kerrey/Hollings bill), comes close to meeting these core public safety, law enforcement, and national security needs. The other bills being considered by Congress, as currently written, risk great harm to our ability to enforce the laws and protect our citizens. We look forward to working to improve the McCain/Kerrey/Hollings bill.

In sum, while encryption is certainly a commercial interest of great importance to this Nation, it is not solely a commercial or business issue. Those of us charged with the protection of public safety and national security, believe that the misuse of encryption technology will become a matter of life and death in many instances. That is why we urge you to adopt a balanced approach that accomplishes the goals mentioned above. Only this approach will allow police departments, attorneys general, district attorneys, sheriffs, and federal authorities to continue to use their most effective investigative techniques, with court approval, to fight crime and espionage and prevent terrorism.

Sincerely your,

Janet Reno, Attorney General; Louis Freeh, Director, Federal Bureau of Investigation; Thomas A. Constantine, Director, Drug Enforcement Administration; Raymond W. Kelly, Undersecretary for Enforcement, U.S. Department of Treasury; John W. Magaw, Director, Bureau of Alcohol, Tobacco and Firearms; Barry McCaffrey, Director, Office of National Drug Control Policy; Lewis C. Merletti, Director, United States Secret Service; George J. Weise, Commissioner, United States Customs Service.

THE SECRETARY OF DEFENSE,
Washington, DC, July 21, 1997.

DEAR MEMBER OF CONGRESS: Recently you received a letter from the nation's senior law enforcement officials regarding US encryption policies. I am writing today to express my strong support for their views on this important issue.

As you know, the Department of Defense is involved on a daily basis in countering international terrorism, narcotics trafficking, and the proliferation of weapons of mass destruction. The spread of unbreakable encryption, as a standard feature of mass market communication products, presents a significant threat to the ability

of the US and its allies to monitor the dangerous groups and individuals involved in these activities. Passage of legislation which effectively decontrols commercial encryption exports would undermine U.S. efforts to foster the use of strong key recovery encryption domestically and abroad. Key recovery products will preserve governments' abilities to counter worldwide terrorism, narcotics trafficking and proliferation.

It is also important to note that the Department of Defense relies on the Federal Bureau of Investigation for the apprehension and prosecution of spies. Sadly, there have been over 60 espionage convictions of federal employees over the last decade. While these individuals represent a tiny minority of government employees, the impact of espionage activities on our nation's security can be enormous. As the recent arrests of Nicholson, Pitts and Kim clearly indicate, espionage remains a very serious problem. Any policies that detract from the FBI's ability to perform its vital counterintelligence function, including the ability to perform wiretaps, inevitably detract from the security of the Department of Defense and the nation.

Encryption legislation must also address the nation's domestic information security needs. Today, approximately 95% of DoD communications rely on public networks; other parts of government, and industry, are even more dependent on the trustworthiness of such networks. Clearly, we must ensure that encryption legislation addresses these needs. An approach such as the one contained in S. 909 can go a long way toward balancing the need for strong encryption with the need to preserve national security and public safety. I hope that you will work with the Administration to enact legislation that addresses these national security concerns as well as the rights of the American people.

I appreciate your consideration of these views.

Sincerely,

BILL COHEN.

INTERNATIONAL ASSOCIATION OF CHIEFS OF POLICE,
Alexandria, VA, July 21, 1997.

DEAR MEMBER OF CONGRESS: Enclosed is a letter sent to you by the Attorney General, the Director of National Drug Control Policy and all the federal law enforcement heads concerning encryption legislation being considered by congress. Collectively we, the undersigned, represent over 17,000 police departments including every major city police department, over 3,000 sheriffs departments, nearly every district attorney in the United States and all of the state Attorneys General. We fully endorse the position taken by our federal counterparts in the enclosed letter. As we have stated many times, Congress must adopt a balanced approach to encryption that fully addresses public safety concerns or the ability of state and local law enforcement to fight crime and drugs will be severely damaged.

Any encryption legislation that does not ensure that law enforcement can gain timely access to the plaintext of encrypted conversations and information by established legal procedures will cause grave harm to public safety. The risk cannot be left to the uncer-

tainty of market forces or commercial interests as the current legislative proposals would require. Without adequate safeguards, the unbridled use of powerful encryption soon will deprive law enforcement of two of its most effective tools, court authorized electronic surveillance and the search and seizure of information stored in computers. This will substantially tip the balance in the fight against crime towards society's most dangerous criminals as the information age develops.

We are in unanimous agreement that congress must adopt encryption legislation that requires the development, manufacture, distribution and sale of only key recovery products and we are opposed to the bills that do not do so. Only the key recovery approach will ensure that law enforcement can continue to gain timely access to the plaintext of encrypted conversations and other evidence of crimes when authorized by a court to do so. If we lose this ability—and the bills you are considering will have this result—it will be a substantial set back for law enforcement at the direct expense of public safety.

Sincerely yours,

DARRELL L. SANDERS,
President, International Association of Chiefs of Police.

JAMES E. DOYLE,
President, National Association of Attorneys General.

FRED SCORALIC,
President, National Sheriffs' Association.

WILLIAM L. MURPHY,
President, National District Attorneys Association.

○