FILE s377.is

S 377 IS

105th CONGRESS

1st Session

To promote electronic commerce by facilitating the use of strong encryption, and for other purposes.

IN THE SENATE OF THE UNITED STATES

February 27, 1997

Mr. BURNS (for himself, Mr. LEAHY, Mr. LOTT, Mr. NICKLES, Mr. DORGAN, Mrs. HUTCHISON, Mr. CRAIG, Mr. WYDEN, Mr. ASHCROFT, Mr. DOMENICI, Mr. THOMAS, Mr. CAMPBELL, Mrs. BOXER, Mr. BROWNBACK, Mrs. MURRAY, Mr. KEMPTHORNE, Mr. INHOFE, Mr. FAIRCLOTH, Mr. GRAMS, and Mr. ALLARD) introduced the following bill; which was read twice and referred to the Committee on Commerce, Science, and Transportation

A BILL

To promote electronic commerce by facilitating the use of strong encryption, and for other purposes.

[Italic->] Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, [<-Italic]

SECTION 1. SHORT TITLE.

This Act may be cited as the `Promotion of Commerce On-Line in the Digital Era (Pro-CODE) Act of 1997'.

SEC. 2. FINDINGS; PURPOSE.

(a) FINDINGS- The Congress finds the following:

(1) The ability to digitize information makes carrying out tremendous amounts of commerce and personal communication electronically possible.

(2) Miniaturization, distributed computing, and reduced transmission costs make communication via electronic networks a reality.

(3) The explosive growth in the internet and other computer networks reflects the potential growth of electronic commerce and personal communication.

(4) The internet and the global information infrastructure have the potential to revolutionize the way individuals and businesses conduct business.

(5) The full potential of the internet for the conduct of business cannot be realized as long as it is an insecure medium in which confidential business information and sensitive personal information remain at risk of unauthorized viewing, alteration, and use.

(6) Encryption of information enables businesses and individuals to protect themselves against the unauthorized viewing, alteration, and use of information by employing widely understood and readily available science and technology to ensure the confidentiality, authenticity, and integrity of

information.

(7) In order to promote economic growth and meet the needs of businesses and individuals in the United States, a variety of encryption products and programs should be available to promote strong, flexible, and commercially acceptable encryption capabilities.

(8) United States computer, computer software and hardware, communications, and electronics businesses are leading the world technology revolution, as those businesses have developed and are prepared to offer immediately to computer users worldwide a variety of communications and computer hardware and computer software that provide strong, robust, and easy-to-use encryption.

(9) United States businesses seek to market the products described in paragraph (8) in competition with scores of foreign businesses in many countries that offer similar, and frequently stronger, encryption products and programs.

(10) The regulatory efforts by the Secretary of Commerce, acting through the National Institute of Standards and Technology, and other entities to promulgate standards and guidelines in support of government-designed solutions to encryption problems that–

(A) were not developed in the private sector; and

(B) have not received widespread commercial support,

have had a negative impact on the development and marketing of products with encryption capabilities by United States businesses.

(11) Because of outdated Federal controls, United States businesses have been prohibited from exporting strong encryption products and programs.

(12) In response to the desire of United States businesses to sell commercial products to the United States Government and to sell a single product worldwide, the Secretary of Commerce, acting through the National Institute of Standards and Technology, has sought to require them to include features in products sold both in the United States and foreign countries that will allow the Federal Government easy access to the plain text of all electronic information and communications.

(13) The Secretary of Commerce, acting through the National Institute of Standards and Technology, has proposed that United States businesses be allowed to sell products and programs offering strong encryption to the United States Government and in foreign countries only if the products and programs include a feature guaranteeing the Federal Government access to a key that decrypts information (hereafter in this section referred to as `key escrow encryption').

(14) The key escrow encryption approach to regulating encryption is reflected in the approval in 1994 by the National

Institute of Standards and Technology of a Federal information processing standard for a standard of escrowed encryption, known as the `clipper chip', that was flawed and controversial.

(15) The current policy of the Federal Government to require that keys to decrypt information be made available to the Federal Government as a condition of exporting strong encryption technology has had the effect of prohibiting the exportation of strong encryption technology.

(16) The Federal Government has legitimate law enforcement and national security objectives which necessitate the disclosure to the Federal Government of general information that is neither proprietary nor confidential by experts in information security industries, including cryptographers, engineers, and others designated in the design and development of information security products. By relaxing export controls on encryption products and programs, this Act creates an obligation on the part of representatives of companies involved in the export of information security products to share information about those products to designated representatives of the Federal Government.

(17) In order to promote electronic commerce in the twenty-first century and to realize the full potential of the internet and other computer networks–

(A) United States businesses should be encouraged to develop and market products and programs offering encryption capabilities; and

(B) the Federal Government should be prohibited from promulgating regulations and adopting policies that discourage the use and sale of encryption.

(b) PURPOSE- The purpose of this Act is to promote electronic commerce through the use of strong encryption by–

(1) recognizing that businesses in the United States that offer computer hardware and computer software made in the United States that incorporate encryption technology are ready and immediately able, with respect to electronic information that will be essential to conducting business in the twenty-first century to provide products that are designed to–

(A) protect the confidentiality of that information; and

(B) ensure the authenticity and integrity of that information;

(2) restricting the Department of Commerce with respect to the promulgation or enforcement of regulations, or the application of policies, that impose government-designed encryption standards; and

(3) promoting the ability of United States businesses to sell to computer users worldwide computer software and computer hardware that provide the strong encryption demanded by such users by–

(A) restricting Federal or State regulation of the sale of such products and programs in interstate commerce;

(B) prohibiting mandatory key escrow encryption systems; and

(C) establishing conditions for the sale of encryption products and programs in foreign commerce.

SEC. 3. DEFINITIONS.

For purposes of this Act, the following definitions shall apply:

(1) AS IS- The term `as is' means, in the case of computer software (including computer software with encryption capabilities), a computer software program that is not designed, developed, or tailored by a producer of computer software for specific users or purchasers, except that such term may include computer software that–

(A) is produced for users or purchasers that supply certain installation parameters needed by the computer software program to function properly with the computer system of the user or purchaser; or

(B) is customized by the user or purchaser by selecting from among options contained in the computer software program.

(2) COMPUTING DEVICE- The term `computing device' means a device that incorporates one or more microprocessor-based central processing units that are capable of accepting, storing, processing, or providing output of data.

(3) COMPUTER HARDWARE- The term `computer hardware' includes computer systems, equipment, application-specific assemblies, modules, and integrated circuits.

(4) DECRYPTION- The term `decryption' means the unscrambling of wire or electronic communications or information using mathematical formulas, codes, or algorithms.

(5) DECRYPTION KEY- The term `decryption key' means the variable information used in a mathematical formula, code, or algorithm, or any component thereof, used to decrypt wire or electronic communications or information that has been encrypted.

(6) DESIGNED FOR INSTALLATION BY THE USER OR PURCHASER- The term `designed for installation by the user or purchaser' means, in the case of computer software (including computer software with encryption capabilities) computer software–

(A) with respect to which the producer of that computer software–

(i) intends for the user or purchaser (including any licensee or transferee), to install the computer software program on a computing device; and

(ii) has supplied the necessary instructions to do so, except that the producer or distributor of the computer software program (or any agent of such

producer or distributor) may also provide telephone help-line or onsite services for computer software installation, electronic transmission, or basic operations; and

(B) that is designed for installation by the user or purchaser without further substantial support by the supplier.

(7) ENCRYPTION- The term `encryption' means the scrambling of wire or electronic communications or information using mathematical formulas, codes, or algorithms in order to preserve the confidentiality, integrity, or authenticity of such communications or information and prevent unauthorized recipients from accessing or altering such communications or information.

(8) GENERAL LICENSE- The term `general license' means a general authorization that is applicable to a type of export that does not require an exporter of that type of export to, as a condition to exporting–

(A) submit a written application to the Secretary; or

(B) receive prior written authorization by the Secretary.

(9) GENERALLY AVAILABLE- The term `generally available' means, in the case of computer software (including software with encryption capabilities), computer software that–

(A) is distributed via the internet or that is widely offered for sale, license, or transfer (without regard to whether it is offered for consideration), including over-the-counter retail sales, mail order transactions, telephone order transactions, electronic distribution, or sale on approval; or

(B) preloaded on computer hardware that is widely available.

(10) INTERNET- The term `internet' means the international computer network of both Federal and non-Federal interconnected packet-switched data networks.

(11) SECRETARY- The term `Secretary' means the Secretary of Commerce.

(12) STATE- The term `State' means each of the several States of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any Territory or Possession of the United States.

SEC. 4. RESTRICTION OF DEPARTMENT OF COMMERCE ENCRYPTION ACTIVITIES IMPOSING GOVERNMENT ENCRYPTION SYSTEMS.

(a) LIMITATION ON REGULATORY AUTHORITY CONCERNING ENCRYPTION STANDARDS- The Secretary may not (acting through the National Institute of Standards and Technology or otherwise) promulgate, or enforce regulations, or otherwise adopt standards or carry out policies that result in encryption standards intended for use by businesses or entities other than Federal computer systems.

(b) LIMITATION ON AUTHORITY CONCERNING EXPORTS OF COMPUTER HARDWARE AND COMPUTER SOFTWARE WITH ENCRYPTION CAPABILITIES- Except as provided in section 5(c)(3)(B), the Secretary may not promulgate or enforce regulations, or adopt or carry out policies in a manner inconsistent with this act, or that have the effect of imposing government-designed encryption standards on the private sector by restricting the export of computer hardware and computer software with encryption capabilities.

SEC. 5. PROMOTION OF COMMERCIAL ENCRYPTION PRODUCTS.

(a) Prohibition on Restrictions on Sale or Distribution in Interstate Commerce-

(1) IN GENERAL- Except as provided in this Act, neither the Federal government nor any State may restrict or regulate the sale in interstate commerce by any person of any product or program designed to provide encryption capabilities solely because such product or program has encryption capabilities. Nothing in this paragraph may be construed to preempt any provision of Federal or State law applicable to contraband or regulated substances.

(2) APPLICABILITY- Paragraph (1) shall apply without regard to the encryption algorithm selected, encryption key length chosen, or implementation technique or medium used for a product or program with encryption capabilities.

(b) PROHIBITION ON MANDATORY KEY ESCROW- Neither the Federal government nor any State may require, as a condition of sale in interstate commerce, that a decryption key, or access to a decryption key, be given to any other person (including a Federal agency or an entity in the private sector that may be certified or approved by the Federal government or a State).

(c) Control of Exports by Secretary-

(1) GENERAL RULE- Notwithstanding any other provision of law and subject to paragraphs (2), (3), and (4), the Secretary shall have exclusive authority to control exports of all computer hardware, computer software, and technology with encryption capabilities, except computer hardware, computer software, and technology that is specifically designed or modified for military use, including command, control, and intelligence applications.

(2) ITEMS THAT DO NOT REQUIRE INDIVIDUAL LICENSES- Except as provided in paragraph (3)(b) of this subsection, only a general license may be required, except as otherwise provided under the Trading with the Enemy Act (50 U.S.C. App. 1 et seq.) or the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) (but only to the extent that the authority of the International Emergency Economic Powers Act is not exercised to extend controls imposed under the Export Administration Act of 1979), for the export or reexport of–

(A) any computer software, including software with

encryption capabilities, that–

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

(ii) is available on the date of enactment of this Act, or becomes legally available thereafter, in the public domain (including on the internet) or publicly available because it is generally accessible to the interested public in any form; or

(B) any computing device or computer hardware solely because it incorporates or employs in any form computer software (including computer software with encryption capabilities) that is described in subparagraph (A).

(3) Computer software and computer hardware with encryption capabilities-

(A) IN GENERAL- Except as provided in subparagraph (B), the Secretary shall authorize the export or reexport of computer software and computer hardware with encryption capabilities under a general license for nonmilitary end-uses in any foreign country to which those exports of computer software and computer hardware of similar capability are permitted for use by financial institutions that the Secretary determines not to be controlled in fact by United States persons.

(B) EXCEPTION- The Secretary shall prohibit the export or reexport of particular computer software and computer hardware described in this subsection to an identified individual or organization in a specific foreign country if the Secretary determines that there is substantial evidence that such software and computer hardware will be–

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

(ii) modified for military or terrorist end-use, including acts against the national security, public safety, or the integrity of the transportation, communications, or other essential systems of interstate commerce in the United States;

(iii) reexported without the authorization required under Federal law; or

(iv) intentionally used to evade enforcement of United States law or taxation by the United States or by any State or local government.

(4) Reporting-

(A) EXPORTS- The publisher or manufacturer of computer software or hardware with encryption capabilities shall disclose (for reporting purposes only) within 30 days after export to the Secretary such information regarding a program's or product's encryption capabilities as would be required for an individual license to export that program

or product.

(B) REPORT NOT AN EXPORT PRECONDITION- Nothing in this paragraph shall be construed to require, or to permit the Secretary to impose any conditions or reporting requirements, including reporting under subparagraph (A), as a precondition to the exportation of any such product or program.

SEC. 6. INFORMATION SECURITY BOARD.

(a) INFORMATION SECURITY BOARD TO BE ESTABLISHED- The Secretary shall establish an Information Security Board comprised of representatives of agencies within the Federal Government responsible for or involved in the formulation of information security policy, including export controls on products with information security features (including encryption). The Board shall meet at such times and in such places as the Secretary may prescribe, but not less frequently than quarterly. The Federal Advisory Committee Act (5 U.S.C. App.) does not apply to the Board or to meetings held by the Board under subsection (d).

(b) PURPOSES- The purposes of the Board are–

(1) to provide a forum to foster communication and coordination between industry and the Federal government; and

(2) to foster the aggregation and dissemination of general, nonproprietary, and nonconfidential developments in important information security technologies, including encryption.

(c) Requirements-

(1) REPORTS TO AGENCIES- The Board shall regularly report general, nonproprietary, and nonconfidential information to appropriate Federal agencies to keep law enforcement and national security agencies abreast of emerging technologies so they are able effectively to execute their responsibilities.

(2) PUBLICATIONS- The Board shall cause such information (other than classified, proprietary, or confidential information) as it deems appropriate, consistent with its purposes, to be published from time to time through any appropriate medium and to be made available to the public.

(d) MEETINGS- The Secretary shall establish a process for quarterly meetings between the Board and representatives from the private sector with interest or expertise in information security, including cryptographers, engineers, and product managers. The Board may meet at anytime with one or more representatives of any person involved in the development, production, or distribution of encryption technology or of computing devices that contain encryption technology.

SEC. 7. STATUTORY CONSTRUCTION.

Nothing in this Act may be construed to affect any law intended to prevent the–

(1) distribution of descramblers or any other equipment for illegal interceptions of cable and satellite television signals;

(2) illegal or unauthorized distribution or release of classified, confidential, or proprietary information; or
(3) enforcement of Federal or State criminal law.