FILE s376.is

S 376 IS

105th CONGRESS

1st Session

To affirm the rights of Americans to use and sell encryption products, to establish privacy standards for voluntary key recovery encryption systems, and for other purposes.

IN THE SENATE OF THE UNITED STATES

February 27, 1997

Mr. LEAHY (for himself, Mr. BURNS, Mrs. MURRAY, and Mr. WYDEN) introduced the following bill; which was read twice and referred to the Committee on the Judiciary

A BILL

To affirm the rights of Americans to use and sell encryption products, to establish privacy standards for voluntary key recovery encryption systems, 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 `Encrypted Communications Privacy Act of 1997'.

SEC. 2. PURPOSES.

The purposes of this Act are–

(1) to ensure that Americans have the maximum possible choice in encryption methods to protect the security, confidentiality, and privacy of their lawful wire and electronic communications and stored electronic information; and

(2) to establish privacy standards for key holders who are voluntarily entrusted with the means to decrypt such communications and information, and procedures by which investigative or law enforcement officers may obtain assistance in decrypting such communications and information.

SEC. 3. FINDINGS.

Congress finds that–

(1) the digitization of information and the explosion in the growth of computing and electronic networking offers tremendous potential benefits to the way Americans live, work, and are entertained, but also raises new threats to the privacy of American citizens and the competitiveness of American businesses;

(2) a secure, private, and trusted national and global information infrastructure is essential to promote economic growth, protect privacy, and meet the needs of American citizens and businesses;

(3) the rights of Americans to the privacy and security of their communications and in the conducting of personal and business affairs should be preserved and protected;

(4) the authority and ability of investigative and law

enforcement officers to access and decipher, in a timely manner and as provided by law, wire and electronic communications and stored electronic information necessary to provide for public safety and national security should also be preserved;

(5) individuals will not entrust their sensitive personal, medical, financial, and other information to computers and computer networks unless the security and privacy of that information is assured;

(6) business will not entrust their proprietary and sensitive corporate information, including information about products, processes, customers, finances, and employees, to computers and computer networks unless the security and privacy of that information is assured;

(7) encryption technology can enhance the privacy, security, confidentiality, integrity, and authenticity of wire and electronic communications and stored electronic information;

(8) encryption techniques, technology, programs, and products are widely available worldwide;

(9) Americans should be free to use lawfully whatever particular encryption techniques, technologies, programs, or products developed in the marketplace they desire to use in order to interact electronically worldwide in a secure, private, and confidential manner;

(10) American companies should be free–

(A) to compete and to sell encryption technology, programs, and products; and

(B) to exchange encryption technology, programs, and products through the use of the Internet, as the Internet is rapidly emerging as the preferred method of distribution of computer software and related information;

(11) there is a need to develop a national encryption policy that advances the development of the national and global information infrastructure, and preserves the right to privacy of Americans and the public safety and national security of the United States;

(12) there is a need to clarify the legal rights and responsibilities of key holders who are voluntarily entrusted with the means to decrypt wire and electronic communications and stored electronic information;

(13) Congress and the American people have recognized the need to balance the right to privacy and the protection of the public safety with national security;

(14) the Constitution permits lawful electronic surveillance by investigative or law enforcement officers and the seizure of stored electronic information only upon compliance with stringent standards and procedures; and

(15) there is a need to clarify the standards and procedures by which investigative or law enforcement officers obtain

assistance from key holders who–

(A) are voluntarily entrusted with the means to decrypt wire and electronic communications and stored electronic information; or

(B) have information that enables the decryption of such communications and information.

SEC. 4. DEFINITIONS.

As used in this Act, the terms `decryption key', `encryption', `key holder', and `State' have the same meanings as in section 2801 of title 18, United States Code, as added by section 6 of this Act.

SEC. 5. FREEDOM TO USE ENCRYPTION.

(a) LAWFUL USE OF ENCRYPTION- Except as provided in this Act and the amendments made by this Act, it shall be lawful for any person within any State, and by any United States person in a foreign country, to use any encryption, regardless of encryption algorithm selected, encryption key length chosen, or implementation technique or medium used.

(b) PROHIBITION ON MANDATORY KEY RECOVERY OR KEY ESCROW ENCRYPTION- Neither the Federal Government nor a State may require, as a condition of a sale in interstate commerce, that a decryption key be given to another person.

(c) GENERAL CONSTRUCTION- Nothing in this Act or the amendments made by this Act shall be construed to–

(1) require the use by any person of any form of encryption;

(2) limit or affect the ability of any person to use encryption without a key recovery function; or

(3) limit or affect the ability of any person who chooses to use encryption with a key recovery function to select the key holder, if any, of the person's choice.

SEC. 6. ENCRYPTED WIRE OR ELECTRONIC COMMUNICATIONS AND STORED ELECTRONIC COMMUNICATIONS.

(a) IN GENERAL- Part I of title 18, United States Code, is amended by inserting after chapter 123 the following new chapter:

[BOLD->] `CHAPTER 125–ENCRYPTED WIRE OR ELECTRONIC COMMUNICATIONS AND STORED ELECTRONIC INFORMATION [<-BOLD]

`Sec. 2801. Definitions

`In this chapter–

`(1) the term `decryption key' means the variable information used in or produced by a mathematical formula, code, or algorithm, or any component thereof, used to decrypt a wire

communication or electronic communication or stored electronic information that has been encrypted;

`(2) the term `decryption assistance' means assistance which provides or facilitates access to the plain text of an encrypted wire communication or electronic communication or stored electronic information;

`(3) the term `encryption' means the scrambling of wire communications or electronic communications or stored electronic information using mathematical formulas 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;

`(4) the term `key holder' means a person (including a Federal agency) located within the United States who–

`(A) is voluntarily entrusted by another independent person with the means to decrypt that person's wire communications or electronic communications or stored electronic information for the purpose of subsequent decryption of such communications or information; or

`(B) has information that enables the decryption of such communications or information for such purpose; and

`(5) the terms `person', `State', `wire communication', `electronic communication', `investigative or law enforcement officer', `judge of competent jurisdiction', and `electronic storage' have the same meanings given such terms in section 2510 of this title.

`Sec. 2802. Prohibited acts by key holders

`(a) UNAUTHORIZED RELEASE OF KEY- Except as provided in subsection (b), any key holder who releases a decryption key or provides decryption assistance shall be subject to the criminal penalties provided in subsection (e) and to civil liability as provided in subsection (f).

`(b) AUTHORIZED RELEASE OF KEY- A key holder shall only release a decryption key in the possession or control of the key holder or provide decryption assistance with respect to the key–

`(1) with the lawful consent of the person whose key is possessed or controlled by the key holder;

`(2) as may be necessarily incident to the provision of service relating to the possession or control of the key by the key holder; or

`(3) upon compliance with subsection (c)–

`(A) to investigative or law enforcement officers authorized to intercept wire communications or electronic communications under chapter 119 of this title;

`(B) to a governmental entity authorized to require access to stored wire and electronic communications and transactional records under chapter 121 of this title; or

`(C) to a governmental entity authorized to seize or compel the production of stored electronic information.

`(c) REQUIREMENTS FOR RELEASE OF DECRYPTION KEY OR PROVISION OF DECRYPTION ASSISTANCE-

`(1) WIRE AND ELECTRONIC COMMUNICATIONS- (A) A key holder may release a decryption key or provide decryption assistance to an investigative or law enforcement officer if–

`(i) the key holder is given–

`(I) a court order–

`(aa) signed by a judge of competent jurisdiction directing such release or assistance; and

`(bb) issued upon a finding that the decryption key or decryption assistance sought is necessary for the decryption of a communication that the investigative or law enforcement officer is authorized to intercept pursuant to chapter 119 of this title; or

`(II) a certification in writing by a person specified in section 2518(7) of this title, or the Attorney General, stating that–

`(aa) no court order is required by law;

`(bb) the conditions set forth in section 2518(7) of this title have been met; and

`(cc) the release or assistance is required;

`(ii) the order or certification under clause (i)–

`(I) specifies the decryption key or decryption assistance being sought; and

`(II) identifies the termination date of the period for which the release or assistance is authorized; and

`(iii) in compliance with the order or certification, the key holder provides only the release or decryption assistance necessary for the access specified in the order or certification.

`(B) If an investigative or law enforcement officer receives a decryption key or decryption assistance under this paragraph for purposes of decrypting wire communications or electronic communications, the judge issuing the order authorizing the interception of such communications shall, as part of the inventory required to be served pursuant to subsection (7)(b) or (8)(d) of section 2518 of this title, cause to be served on the persons named in the order, or the application for the order, and on such other parties as the judge may determine in the interests of justice, notice of the receipt of the key or decryption assistance, as the case may be, by the officer.

`(2) STORED WIRE AND ELECTRONIC COMMUNICATIONS AND STORED ELECTRONIC INFORMATION- (A) A key holder may release a decryption key or provide decryption assistance to a governmental entity requiring disclosure of stored wire and electronic communications and transactional records under chapter 121 of this title only if the key holder is directed to

release the key or give such assistance pursuant to a court order issued upon a finding that the decryption key or decryption assistance sought is necessary for the decryption of communications or records the disclosure of which the governmental entity is authorized to require under section 2703 of this title.

`(B) A key holder may release a decryption key or provide decryption assistance under this subsection to a governmental entity seizing or compelling production of stored electronic information only if the key holder is directed to release the key or give such assistance pursuant to a court order issued upon a finding that the decryption key or decryption assistance sought is necessary for the decryption of stored electronic information–

`(i) that the governmental entity is authorized to seize; or

`(ii) the production of which the governmental entity is authorized to compel.

`(C) A court order directing the release of a decryption key or the provision of decryption assistance under subparagraph (A) or (B) shall specify the decryption key or decryption assistance being sought. A key holder may provide only such release or decryption assistance as is necessary for access to the communications, records, or information covered by the court order.

`(D) If a governmental entity receives a decryption key or decryption assistance under this paragraph for purposes of obtaining access to stored wire and electronic communications or transactional records under section 2703 of this title, the notice required with respect to such access under subsection (b) of such section shall include notice of the receipt of the key or assistance, as the case may be, by the entity.

`(3) USE OF KEY- (A) An investigative or law enforcement officer or governmental entity to which a decryption key is released under this subsection may use the key only in the manner and for the purpose and period expressly provided for in the certification or court order authorizing such release and use. Such period may not exceed the duration of the interception for which the key was released or such other period as the court, if any, may allow.

`(B) Not later than the end of the period authorized for the release of a decryption key, the investigative or law enforcement officer or governmental entity to which the key is released shall destroy and not retain the key and provide a certification that the key has been destroyed to the issuing court, if any.

`(4) NONDISCLOSURE OF RELEASE- No key holder, officer, employee, or agent thereof may disclose the release of an

encryption key or the provision of decryption assistance under subsection (b)(3), except as otherwise required by law or legal process and then only after prior notification to the Attorney General or to the principal prosecuting attorney of a State or of a political subdivision of a State, as appropriate.

`(d) RECORDS OR OTHER INFORMATION HELD BY KEY HOLDERS-

`(1) IN GENERAL- A key holder may not disclose a record or other information (not including the key or the contents of communications) pertaining to any person, which record or information is held by the key holder in connection with its control or possession of a decryption key, except–

`(A) with the lawful consent of the person whose key is possessed or controlled by the key holder; or

`(B) to an investigative or law enforcement officer pursuant to a warrant, subpoena, court order, or other lawful process authorized by Federal or State law.

`(2) CERTAIN NOTICE NOT REQUIRED- An investigative or law enforcement officer receiving a record or information under paragraph (1)(B) is not required to provide notice of such receipt to the person to whom the record or information pertains.

`(3) LIABILITY FOR CIVIL DAMAGES- Any disclosure in violation of this subsection shall render the person committing the violation liable for the civil damages provided for in subsection (f).

`(e) CRIMINAL PENALTIES- The punishment for an offense under subsection (a) is–

`(1) if the offense is committed for a tortious, malicious, or illegal purpose, or for purposes of direct or indirect commercial advantage or private commercial gain–

`(A) a fine under this title or imprisonment for not more than 1 year, or both, in the case of a first offense; or

`(B) a fine under this title or imprisonment for not more than 2 years, or both, in the case of a second or subsequent offense; and

`(2) in any other case where the offense is committed recklessly or intentionally, a fine of not more than $5,000 or imprisonment for not more than 6 months, or both.

`(f) CIVIL DAMAGES-

`(1) IN GENERAL- Any person aggrieved by any act of a person in violation of subsection (a) or (d) may in a civil action recover from such person appropriate relief.

`(2) RELIEF- In an action under this subsection, appropriate relief includes–

`(A) such preliminary and other equitable or declaratory relief as may be appropriate;

`(B) damages under paragraph (3) and punitive damages in appropriate cases; and

`(C) a reasonable attorney's fee and other litigation

costs reasonably incurred.

`(3) COMPUTATION OF DAMAGES- The court may assess as damages the greater of–

`(A) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation; or

`(B) statutory damages in the amount of $5,000.

`(4) LIMITATION- A civil action under this subsection shall be commenced not later than 2 years after the date on which the plaintiff first knew or should have known of the violation.

`(g) DEFENSE- It shall be a complete defense against any civil or criminal action brought under this chapter that the defendant acted in good faith reliance upon a warrant, subpoena, or court order or other statutory authorization.

`Sec. 2803. Reporting requirements

`(a) IN GENERAL- In reporting to the Administrative Office of the United States Courts as required under section 2519(2) of this title, the Attorney General, an Assistant Attorney General specially designated by the Attorney General, the principal prosecuting attorney of a State, or the principal prosecuting attorney of any political subdivision of a State shall report on the number of orders and extensions served on key holders under this chapter to obtain access to decryption keys or decryption assistance and the offenses for which the orders and extensions were obtained.

`(b) REQUIREMENTS- The Director of the Administrative Office of the United States Courts shall include in the report transmitted t o Congress under section 2519(3) of this title the number of orders and extensions served on key holders to obtain access to decryption keys or decryption assistance and the offenses for which the orders and extensions were obtained.

`Sec. 2804. Unlawful use of encryption to obstruct justice

`Whoever willfully endeavors by means of encryption to obstruct, impede, or prevent the communication to an investigative or law enforcement officer of information in furtherance of a felony that may be prosecuted in a court of the United States shall–

`(1) in the case of a first conviction, be sentenced to imprisonment for not more than 5 years, fined under this title, or both; or

`(2) in the case of a second or subsequent conviction, be sentenced to imprisonment for not more than 10 years, fined under this title, or both.

`Sec. 2805. Freedom to sell encryption products

`(a) IN GENERAL- It shall be lawful for any person within any State to sell in interstate commerce any encryption, regardless of encryption algorithm selected, encryption key length chosen, or implementation technique or medium used.

`(b) CONTROL OF EXPORTS BY SECRETARY OF COMMERCE-

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

`(2) ITEMS SUBJECT TO LICENSE EXCEPTION- 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), a license exception shall be made available for the export or reexport of–

`(A) any computer software, including computer software with encryption capabilities, that is–

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

`(ii) in the public domain (including computer software available through the Internet or another interactive computer service) or publicly available because the computer software is generally accessible to the interested public in any form;

`(B) any computing device or computer hardware that otherwise would be restricted solely on the basis that it incorporates or employs in any form computer software (including computer software with encryption capabilities) that is described in subparagraph (A);

`(C) any computer software or computer hardware that is otherwise restricted solely on the basis that it incorporates or employs in any form interface mechanisms for interaction with other hardware and software, including encryption hardware and software; or

`(D) any encryption technology related or ancillary to a device, software, or hardware described in subparagraph (A), (B), or (C).

`(3) COMPUTER SOFTWARE, COMPUTER HARDWARE, AND TECHNOLOGY WITH ENCRYPTION CAPABILITIES- (A) Except as provided in subparagraph (B), the Secretary of Commerce shall authorize the export or reexport of computer software, computer hardware, and technology with encryption capabilities under a license exception if–

`(i) a product offering comparable security is commercially available from a foreign supplier without effective restrictions;

`(ii) a product offering comparable security is generally

available in a foreign country; or

`(iii) the sole basis for otherwise withholding the license exception is the employment in the software, hardware, or technology of encryption from a foreign source.

`(B) The Secretary of Commerce shall prohibit the export or reexport of computer software, computer hardware, and technology described in subparagraph (A) to a foreign country if the Secretary determines that there is substantial evidence that such software, hardware, or technology will be–

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

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

`(iii) reexported without requisite United States authorization.

`(4) DEFINITIONS- As used in this subsection–

`(A) 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 the computer software company for specific purchasers, except that such purchasers may supply certain installation parameters needed by the computer software program to function properly with the purchaser's system and may customize the computer software program by choosing among options contained in the computer software program;

`(B) 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;

`(C) the term `computer hardware', when used in conjunction with information security, includes computer systems, equipment, application-specific assemblies, modules, and integrated circuits;

`(D) the term `generally available' means, in the case of computer software (including computer software with encryption capabilities), computer software that is widely offered for sale, license, or transfer including over-the-counter retail sales, mail order transactions, telephone order transactions, electronic distribution, and sale on approval;

`(E) the term `interactive computer service' has the meaning provided that term in section 230(e)(2) of the Communications Act of 1934 (47 U.S.C. 230(e)(2));

`(F) the term `Internet' has the meaning provided that term in section 230(e)(1) of the Communications Act of 1934 (47 U.S.C. 230(e)(1));

`(G) the term `is designed for installation by the purchaser' means, in the case of computer software

(including computer software with encryption capabilities)–

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

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

`(H) the term `license exception' means a general authorization applicable to a type of export that does not require an exporter to, as a condition of exporting–

`(i) submit a written application to the Secretary of Commerce; or

`(ii) receive prior written authorization by the Secretary of Commerce; and

`(I) the term `technology' means specific information necessary for the development, production, or use of a product.

`Sec. 2806. Requirements for release of decryption key or provision of decryption assistance to a foreign country

`(a) IN GENERAL- Except as provided in subsection (b), no investigative or law enforcement officer or key holder may release a decryption key or provide decryption assistance to a foreign country.

`(b) CONDITIONS FOR COOPERATION WITH FOREIGN COUNTRY-

`(1) IN GENERAL- In any case in which the United States has entered into a treaty or convention with a foreign country to provide mutual assistance with respect to decryption, the Attorney General (or the designee of the Attorney General) may, upon an official request to the United States from the foreign country, apply for an order described in paragraph (2) from the district court in which a key holder resides for–

`(A) assistance in obtaining the release of a decryption key from the key holder; or

`(B) obtaining decryption assistance from the key holder.

`(2) CONTENTS OF ORDER- An order described in this paragraph is an order that directs the key holder involved to–

`(A) release a decryption key to the Attorney General (or the designee of the Attorney General) for furnishing to the foreign country; or

`(B) provide decryption assistance to the Attorney General (or the designee of the Attorney General) for furnishing to the foreign country.

`(3) REQUIREMENTS FOR ORDER- A judge of a court described in

paragraph (1) may issue an order described in paragraph (2) if the judge finds, on the basis on an application made by the Attorney General under this subsection, that–

`(A) the decryption key or decryption assistance sought is necessary for the decryption of a communication or information that the foreign country is authorized to intercept or seize pursuant to the law of the foreign country;

`(B) the law of the foreign country provides for adequate protection against arbitrary interference with respect to privacy rights; and

`(C) the decryption key or decryption assistance is being sought in connection with a criminal investigation for conduct that would constitute a violation of a criminal law of the United States if committed within the jurisdiction of the United States.

`(c) DEFINITION- As used in this section, the term `official request' has the meaning given that term in section 3506(c) of this title.'.

(b) CLERICAL AMENDMENT- The chapter analysis for part I of title 18, United States Code, is amended by inserting after the item relating to chapter 123 the following new item:

[Bold->] 2801'. [<-Bold]

SEC. 7. INTELLIGENCE ACTIVITIES.

(a) CONSTRUCTION- Nothing in this Act or the amendments made by this Act constitutes authority for the conduct of any intelligence activity.

(b) CERTAIN CONDUCT- Nothing in this Act or the amendments made by this Act shall affect the conduct, by officers or employees of the United States Government in accordance with other applicable Federal law, under procedures approved by the Attorney General, of activities intended to–

(1) intercept encrypted or other official communications of United States executive branch entities or United States Government contractors for communications security purposes;

(2) intercept radio communications transmitted between or among foreign powers or agents of a foreign power as defined by the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.); or

(3) access an electronic communication system used exclusively by a foreign power or agent of a foreign power as so defined.