

105TH CONGRESS
1ST SESSION

S. 376

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.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Encrypted Commu-
5 nications Privacy Act of 1997”.

6 **SEC. 2. PURPOSES.**

7 The purposes of this Act are—

1 (1) to ensure that Americans have the maxi-
2 mum possible choice in encryption methods to pro-
3 tect the security, confidentiality, and privacy of their
4 lawful wire and electronic communications and
5 stored electronic information; and

6 (2) to establish privacy standards for key hold-
7 ers who are voluntarily entrusted with the means to
8 decrypt such communications and information, and
9 procedures by which investigative or law enforcement
10 officers may obtain assistance in decrypting such
11 communications and information.

12 **SEC. 3. FINDINGS.**

13 Congress finds that—

14 (1) the digitization of information and the ex-
15 plosion in the growth of computing and electronic
16 networking offers tremendous potential benefits to
17 the way Americans live, work, and are entertained,
18 but also raises new threats to the privacy of Amer-
19 ican citizens and the competitiveness of American
20 businesses;

21 (2) a secure, private, and trusted national and
22 global information infrastructure is essential to pro-
23 mote economic growth, protect privacy, and meet the
24 needs of American citizens and businesses;

1 (3) the rights of Americans to the privacy and
2 security of their communications and in the conduct-
3 ing of personal and business affairs should be pre-
4 served and protected;

5 (4) the authority and ability of investigative
6 and law enforcement officers to access and decipher,
7 in a timely manner and as provided by law, wire and
8 electronic communications and stored electronic in-
9 formation necessary to provide for public safety and
10 national security should also be preserved;

11 (5) individuals will not entrust their sensitive
12 personal, medical, financial, and other information
13 to computers and computer networks unless the se-
14 curity and privacy of that information is assured;

15 (6) business will not entrust their proprietary
16 and sensitive corporate information, including infor-
17 mation about products, processes, customers, fi-
18 nances, and employees, to computers and computer
19 networks unless the security and privacy of that in-
20 formation is assured;

21 (7) encryption technology can enhance the pri-
22 vacy, security, confidentiality, integrity, and authen-
23 ticity of wire and electronic communications and
24 stored electronic information;

1 (8) encryption techniques, technology, pro-
2 grams, and products are widely available worldwide;

3 (9) Americans should be free to use lawfully
4 whatever particular encryption techniques, tech-
5 nologies, programs, or products developed in the
6 marketplace they desire to use in order to interact
7 electronically worldwide in a secure, private, and
8 confidential manner;

9 (10) American companies should be free—

10 (A) to compete and to sell encryption tech-
11 nology, programs, and products; and

12 (B) to exchange encryption technology,
13 programs, and products through the use of the
14 Internet, as the Internet is rapidly emerging as
15 the preferred method of distribution of com-
16 puter software and related information;

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

23 (12) there is a need to clarify the legal rights
24 and responsibilities of key holders who are volun-
25 tarily entrusted with the means to decrypt wire and

1 electronic communications and stored electronic in-
2 formation;

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

7 (14) the Constitution permits lawful electronic
8 surveillance by investigative or law enforcement offi-
9 cers and the seizure of stored electronic information
10 only upon compliance with stringent standards and
11 procedures; and

12 (15) there is a need to clarify the standards
13 and procedures by which investigative or law en-
14 forcement officers obtain assistance from key holders
15 who—

16 (A) are voluntarily entrusted with the
17 means to decrypt wire and electronic commu-
18 nications and stored electronic information; or

19 (B) have information that enables the
20 decryption of such communications and infor-
21 mation.

22 **SEC. 4. DEFINITIONS.**

23 As used in this Act, the terms “decryption key”,
24 “encryption”, “key holder”, and “State” have the same

1 meanings as in section 2801 of title 18, United States
2 Code, as added by section 6 of this Act.

3 **SEC. 5. FREEDOM TO USE ENCRYPTION.**

4 (a) **LAWFUL USE OF ENCRYPTION.**—Except as pro-
5 vided in this Act and the amendments made by this Act,
6 it shall be lawful for any person within any State, and
7 by any United States person in a foreign country, to use
8 any encryption, regardless of encryption algorithm se-
9 lected, encryption key length chosen, or implementation
10 technique or medium used.

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

16 (c) **GENERAL CONSTRUCTION.**—Nothing in this Act
17 or the amendments made by this Act shall be construed
18 to—

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

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

1 (3) limit or affect the ability of any person who
 2 chooses to use encryption with a key recovery func-
 3 tion to select the key holder, if any, of the person’s
 4 choice.

5 **SEC. 6. ENCRYPTED WIRE OR ELECTRONIC COMMUNICA-**
 6 **TIONS AND STORED ELECTRONIC COMMU-**
 7 **NICATIONS.**

8 (a) IN GENERAL.—Part I of title 18, United States
 9 Code, is amended by inserting after chapter 123 the fol-
 10 lowing new chapter:

11 **“CHAPTER 125—ENCRYPTED WIRE OR**
 12 **ELECTRONIC COMMUNICATIONS AND**
 13 **STORED ELECTRONIC INFORMATION**

“Sec.

“2801. Definitions.

“2802. Prohibited acts by key holders.

“2803. Reporting requirements.

“2804. Unlawful use of encryption to obstruct justice.

“2805. Freedom to sell encryption products.

“2806. Requirements for release of decryption key or provision of encryption as-
 sistance to a foreign country.

14 **“§ 2801. Definitions**

15 “In this chapter—

16 “(1) the term ‘decryption key’ means the vari-
 17 able information used in or produced by a mathe-
 18 matical formula, code, or algorithm, or any compo-
 19 nent thereof, used to decrypt a wire communication
 20 or electronic communication or stored electronic in-
 21 formation that has been encrypted;

1 “(2) the term ‘decryption assistance’ means as-
2 sistance which provides or facilitates access to the
3 plain text of an encrypted wire communication or
4 electronic communication or stored electronic infor-
5 mation;

6 “(3) the term ‘encryption’ means the scram-
7 bling of wire communications or electronic commu-
8 nications or stored electronic information using
9 mathematical formulas or algorithms in order to
10 preserve the confidentiality, integrity, or authenticity
11 of such communications or information and prevent
12 unauthorized recipients from accessing or altering
13 such communications or information;

14 “(4) the term ‘key holder’ means a person (in-
15 cluding a Federal agency) located within the United
16 States who—

17 “(A) is voluntarily entrusted by another
18 independent person with the means to decrypt
19 that person’s wire communications or electronic
20 communications or stored electronic information
21 for the purpose of subsequent decryption of
22 such communications or information; or

23 “(B) has information that enables the
24 decryption of such communications or informa-
25 tion for such purpose; and

1 “(5) the terms ‘person’, ‘State’, ‘wire commu-
2 nication’, ‘electronic communication’, ‘investigative
3 or law enforcement officer’, ‘judge of competent ju-
4 risdiction’, and ‘electronic storage’ have the same
5 meanings given such terms in section 2510 of this
6 title.

7 **“§ 2802. Prohibited acts by key holders**

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

13 “(b) AUTHORIZED RELEASE OF KEY.—A key holder
14 shall only release a decryption key in the possession or
15 control of the key holder or provide decryption assistance
16 with respect to the key—

17 “(1) with the lawful consent of the person
18 whose key is possessed or controlled by the key hold-
19 er;

20 “(2) as may be necessarily incident to the provi-
21 sion of service relating to the possession or control
22 of the key by the key holder; or

23 “(3) upon compliance with subsection (c)—

1 “(A) to investigative or law enforcement
2 officers authorized to intercept wire commu-
3 nications or electronic communications under
4 chapter 119 of this title;

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

9 “(C) to a governmental entity authorized
10 to seize or compel the production of stored elec-
11 tronic information.

12 “(c) REQUIREMENTS FOR RELEASE OF DECRYPTION
13 KEY OR PROVISION OF DECRYPTION ASSISTANCE.—

14 “(1) WIRE AND ELECTRONIC COMMUNICA-
15 TIONS.—(A) A key holder may release a decryption
16 key or provide decryption assistance to an investiga-
17 tive or law enforcement officer if—

18 “(i) the key holder is given—

19 “(I) a court order—

20 “(aa) signed by a judge of com-
21 petent jurisdiction directing such re-
22 lease or assistance; and

23 “(bb) issued upon a finding that
24 the decryption key or decryption as-
25 sistance sought is necessary for the

1 decryption of a communication that
2 the investigative or law enforcement
3 officer is authorized to intercept pur-
4 suant to chapter 119 of this title; or

5 “(II) a certification in writing by a
6 person specified in section 2518(7) of this
7 title, or the Attorney General, stating
8 that—

9 “(aa) no court order is required
10 by law;

11 “(bb) the conditions set forth in
12 section 2518(7) of this title have been
13 met; and

14 “(cc) the release or assistance is
15 required;

16 “(ii) the order or certification under clause
17 (i)—

18 “(I) specifies the decryption key or
19 decryption assistance being sought; and

20 “(II) identifies the termination date of
21 the period for which the release or assist-
22 ance is authorized; and

1 “(iii) in compliance with the order or cer-
2 tification, the key holder provides only the re-
3 lease or decryption assistance necessary for the
4 access specified in the order or certification.

5 “(B) If an investigative or law enforcement offi-
6 cer receives a decryption key or decryption assist-
7 ance under this paragraph for purposes of
8 decrypting wire communications or electronic com-
9 munications, the judge issuing the order authorizing
10 the interception of such communications shall, as
11 part of the inventory required to be served pursuant
12 to subsection (7)(b) or (8)(d) of section 2518 of this
13 title, cause to be served on the persons named in the
14 order, or the application for the order, and on such
15 other parties as the judge may determine in the in-
16 terests of justice, notice of the receipt of the key or
17 decryption assistance, as the case may be, by the of-
18 ficer.

19 “(2) STORED WIRE AND ELECTRONIC COMMU-
20 NICATIONS AND STORED ELECTRONIC INFORMA-
21 TION.—(A) A key holder may release a decryption
22 key or provide decryption assistance to a govern-
23 mental entity requiring disclosure of stored wire and
24 electronic communications and transactional records
25 under chapter 121 of this title only if the key holder

1 is directed to release the key or give such assistance
2 pursuant to a court order issued upon a finding that
3 the decryption key or decryption assistance sought is
4 necessary for the decryption of communications or
5 records the disclosure of which the governmental en-
6 tity is authorized to require under section 2703 of
7 this title.

8 “(B) A key holder may release a decryption key
9 or provide decryption assistance under this sub-
10 section to a governmental entity seizing or compel-
11 ling production of stored electronic information only
12 if the key holder is directed to release the key or
13 give such assistance pursuant to a court order issued
14 upon a finding that the decryption key or decryption
15 assistance sought is necessary for the decryption of
16 stored electronic information—

17 “(i) that the governmental entity is author-
18 ized to seize; or

19 “(ii) the production of which the govern-
20 mental entity is authorized to compel.

21 “(C) A court order directing the release of a
22 decryption key or the provision of decryption assist-
23 ance under subparagraph (A) or (B) shall specify
24 the decryption key or decryption assistance being
25 sought. A key holder may provide only such release

1 or decryption assistance as is necessary for access to
2 the communications, records, or information covered
3 by the court order.

4 “(D) If a governmental entity receives a
5 decryption key or decryption assistance under this
6 paragraph for purposes of obtaining access to stored
7 wire and electronic communications or transactional
8 records under section 2703 of this title, the notice
9 required with respect to such access under sub-
10 section (b) of such section shall include notice of the
11 receipt of the key or assistance, as the case may be,
12 by the entity.

13 “(3) USE OF KEY.—(A) An investigative or law
14 enforcement officer or governmental entity to which
15 a decryption key is released under this subsection
16 may use the key only in the manner and for the pur-
17 pose and period expressly provided for in the certifi-
18 cation or court order authorizing such release and
19 use. Such period may not exceed the duration of the
20 interception for which the key was released or such
21 other period as the court, if any, may allow.

1 “(B) Not later than the end of the period au-
2 thorized for the release of a decryption key, the in-
3 vestigative or law enforcement officer or govern-
4 mental entity to which the key is released shall de-
5 stroy and not retain the key and provide a certifi-
6 cation that the key has been destroyed to the issuing
7 court, if any.

8 “(4) NONDISCLOSURE OF RELEASE.—No key
9 holder, officer, employee, or agent thereof may dis-
10 close the release of an encryption key or the provi-
11 sion of decryption assistance under subsection
12 (b)(3), except as otherwise required by law or legal
13 process and then only after prior notification to the
14 Attorney General or to the principal prosecuting at-
15 torney of a State or of a political subdivision of a
16 State, as appropriate.

17 “(d) RECORDS OR OTHER INFORMATION HELD BY
18 KEY HOLDERS.—

19 “(1) IN GENERAL.—A key holder may not dis-
20 close a record or other information (not including
21 the key or the contents of communications) pertain-
22 ing to any person, which record or information is
23 held by the key holder in connection with its control
24 or possession of a decryption key, except—

1 “(A) with the lawful consent of the person
2 whose key is possessed or controlled by the key
3 holder; or

4 “(B) to an investigative or law enforce-
5 ment officer pursuant to a warrant, subpoena,
6 court order, or other lawful process authorized
7 by Federal or State law.

8 “(2) CERTAIN NOTICE NOT REQUIRED.—An inves-
9 tigative or law enforcement officer receiving a record
10 or information under paragraph (1)(B) is not re-
11 quired to provide notice of such receipt to the person
12 to whom the record or information pertains.

13 “(3) LIABILITY FOR CIVIL DAMAGES.—Any dis-
14 closure in violation of this subsection shall render
15 the person committing the violation liable for the
16 civil damages provided for in subsection (f).

17 “(e) CRIMINAL PENALTIES.—The punishment for an
18 offense under subsection (a) is—

19 “(1) if the offense is committed for a tortious,
20 malicious, or illegal purpose, or for purposes of di-
21 rect or indirect commercial advantage or private
22 commercial gain—

23 “(A) a fine under this title or imprison-
24 ment for not more than 1 year, or both, in the
25 case of a first offense; or

1 “(B) a fine under this title or imprison-
2 ment for not more than 2 years, or both, in the
3 case of a second or subsequent offense; and

4 “(2) in any other case where the offense is com-
5 mitted recklessly or intentionally, a fine of not more
6 than \$5,000 or imprisonment for not more than 6
7 months, or both.

8 “(f) CIVIL DAMAGES.—

9 “(1) IN GENERAL.—Any person aggrieved by
10 any act of a person in violation of subsection (a) or
11 (d) may in a civil action recover from such person
12 appropriate relief.

13 “(2) RELIEF.—In an action under this sub-
14 section, appropriate relief includes—

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

17 “(B) damages under paragraph (3) and
18 punitive damages in appropriate cases; and

19 “(C) a reasonable attorney’s fee and other
20 litigation costs reasonably incurred.

21 “(3) COMPUTATION OF DAMAGES.—The court
22 may assess as damages the greater of—

23 “(A) the sum of the actual damages suf-
24 fered by the plaintiff and any profits made by
25 the violator as a result of the violation; or

1 “(B) statutory damages in the amount of
2 \$5,000.

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

7 “(g) DEFENSE.—It shall be a complete defense
8 against any civil or criminal action brought under this
9 chapter that the defendant acted in good faith reliance
10 upon a warrant, subpoena, or court order or other statu-
11 tory authorization.

12 **“§ 2803. Reporting requirements**

13 “(a) IN GENERAL.—In reporting to the Administra-
14 tive Office of the United States Courts as required under
15 section 2519(2) of this title, the Attorney General, an As-
16 sistant Attorney General specially designated by the Attor-
17 ney General, the principal prosecuting attorney of a State,
18 or the principal prosecuting attorney of any political sub-
19 division of a State shall report on the number of orders
20 and extensions served on key holders under this chapter
21 to obtain access to decryption keys or decryption assist-
22 ance and the offenses for which the orders and extensions
23 were obtained.

24 “(b) REQUIREMENTS.—The Director of the Adminis-
25 trative Office of the United States Courts shall include

1 in the report transmitted to Congress under section
2 2519(3) of this title the number of orders and extensions
3 served on key holders to obtain access to decryption keys
4 or decryption assistance and the offenses for which the
5 orders and extensions were obtained.

6 **“§ 2804. Unlawful use of encryption to obstruct jus-**
7 **tice**

8 “Whoever willfully endeavors by means of encryption
9 to obstruct, impede, or prevent the communication to an
10 investigative or law enforcement officer of information in
11 furtherance of a felony that may be prosecuted in a court
12 of the United States shall—

13 “(1) in the case of a first conviction, be sen-
14 tenced to imprisonment for not more than 5 years,
15 fined under this title, or both; or

16 “(2) in the case of a second or subsequent con-
17 viction, be sentenced to imprisonment for not more
18 than 10 years, fined under this title, or both.

19 **“§ 2805. Freedom to sell encryption products**

20 “(a) IN GENERAL.—It shall be lawful for any person
21 within any State to sell in interstate commerce any
22 encryption, regardless of encryption algorithm selected,
23 encryption key length chosen, or implementation technique
24 or medium used.

1 “(b) CONTROL OF EXPORTS BY SECRETARY OF COM-
2 MERCE.—

3 “(1) GENERAL RULE.—Notwithstanding any
4 other law and subject to paragraphs (2), (3), and
5 (4), the Secretary of Commerce shall have exclusive
6 authority to control exports of all computer hard-
7 ware, computer software, and technology for infor-
8 mation security (including encryption), except com-
9 puter hardware, software, and technology that is
10 specifically designed or modified for military use, in-
11 cluding command, control, and intelligence applica-
12 tions.

13 “(2) ITEMS SUBJECT TO LICENSE EXCEP-
14 TION.—Except as otherwise provided under the
15 Trading With The Enemy Act (50 U.S.C. App. 1 et
16 seq.) or the International Emergency Economic
17 Powers Act (50 U.S.C. 1701 et seq.) (but only to
18 the extent that the authority of the International
19 Emergency Economic Powers Act is not exercised to
20 extend controls imposed under the Export Adminis-
21 tration Act of 1979), a license exception shall be
22 made available for the export or reexport of—

23 “(A) any computer software, including
24 computer software with encryption capabilities,
25 that is—

1 “(i) generally available, as is, and de-
2 signed for installation by the user or pur-
3 chaser; or

4 “(ii) in the public domain (including
5 computer software available through the
6 Internet or another interactive computer
7 service) or publicly available because the
8 computer software is generally accessible
9 to the interested public in any form;

10 “(B) any computing device or computer
11 hardware that otherwise would be restricted
12 solely on the basis that it incorporates or em-
13 ploys in any form computer software (including
14 computer software with encryption capabilities)
15 that is described in subparagraph (A);

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

22 “(D) any encryption technology related or
23 ancillary to a device, software, or hardware de-
24 scribed in subparagraph (A), (B), or (C).

1 “(3) COMPUTER SOFTWARE, COMPUTER HARD-
2 WARE, AND TECHNOLOGY WITH ENCRYPTION CAPA-
3 BILITIES.—(A) Except as provided in subparagraph
4 (B), the Secretary of Commerce shall authorize the
5 export or reexport of computer software, computer
6 hardware, and technology with encryption capabili-
7 ties under a license exception if—

8 “(i) a product offering comparable security
9 is commercially available from a foreign sup-
10 plier without effective restrictions;

11 “(ii) a product offering comparable secu-
12 rity is generally available in a foreign country;
13 or

14 “(iii) the sole basis for otherwise withhold-
15 ing the license exception is the employment in
16 the software, hardware, or technology of
17 encryption from a foreign source.

18 “(B) The Secretary of Commerce shall prohibit
19 the export or reexport of computer software, com-
20 puter hardware, and technology described in sub-
21 paragraph (A) to a foreign country if the Secretary
22 determines that there is substantial evidence that
23 such software, hardware, or technology will be—

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

1 “(ii) modified for military or terrorist end-
2 use; or

3 “(iii) reexported without requisite United
4 States authorization.

5 “(4) DEFINITIONS.—As used in this sub-
6 section—

7 “(A) the term ‘as is’ means, in the case of
8 computer software (including computer software
9 with encryption capabilities), a computer soft-
10 ware program that is not designed, developed,
11 or tailored by the computer software company
12 for specific purchasers, except that such pur-
13 chasers may supply certain installation param-
14 eters needed by the computer software program
15 to function properly with the purchaser’s sys-
16 tem and may customize the computer software
17 program by choosing among options contained
18 in the computer software program;

19 “(B) the term ‘computing device’ means a
20 device which incorporates one or more micro-
21 processor-based central processing units that
22 can accept, store, process, or provide output of
23 data;

24 “(C) the term ‘computer hardware’, when
25 used in conjunction with information security,

1 includes computer systems, equipment, applica-
2 tion-specific assemblies, modules, and inte-
3 grated circuits;

4 “(D) the term ‘generally available’ means,
5 in the case of computer software (including
6 computer software with encryption capabilities),
7 computer software that is widely offered for
8 sale, license, or transfer including over-the-
9 counter retail sales, mail order transactions,
10 telephone order transactions, electronic dis-
11 tribution, and sale on approval;

12 “(E) the term ‘interactive computer serv-
13 ice’ has the meaning provided that term in sec-
14 tion 230(e)(2) of the Communications Act of
15 1934 (47 U.S.C. 230(e)(2));

16 “(F) the term ‘Internet’ has the meaning
17 provided that term in section 230(e)(1) of the
18 Communications Act of 1934 (47 U.S.C.
19 230(e)(1));

20 “(G) the term ‘is designed for installation
21 by the purchaser’ means, in the case of com-
22 puter software (including computer software
23 with encryption capabilities)—

24 “(i) that the computer software com-
25 pany intends for the purchaser (including

1 any licensee or transferee), who may not
2 be the actual program user, to install the
3 computer software program on a comput-
4 ing device and has supplied the necessary
5 instructions to do so, except that the com-
6 pany may also provide telephone help-line
7 services for software installation, electronic
8 transmission, or basic operations; and

9 “(ii) that the computer software pro-
10 gram is designed for installation by the
11 purchaser without further substantial sup-
12 port by the supplier;

13 “(H) the term ‘license exception’ means a
14 general authorization applicable to a type of ex-
15 port that does not require an exporter to, as a
16 condition of exporting—

17 “(i) submit a written application to
18 the Secretary of Commerce; or

19 “(ii) receive prior written authoriza-
20 tion by the Secretary of Commerce; and

21 “(I) the term ‘technology’ means specific
22 information necessary for the development, pro-
23 duction, or use of a product.

1 **“§ 2806. Requirements for release of decryption key**
2 **or provision of decryption assistance to a**
3 **foreign country**

4 “(a) IN GENERAL.—Except as provided in subsection
5 (b), no investigative or law enforcement officer or key
6 holder may release a decryption key or provide decryption
7 assistance to a foreign country.

8 “(b) CONDITIONS FOR COOPERATION WITH FOREIGN
9 COUNTRY.—

10 “(1) IN GENERAL.—In any case in which the
11 United States has entered into a treaty or conven-
12 tion with a foreign country to provide mutual assist-
13 ance with respect to decryption, the Attorney Gen-
14 eral (or the designee of the Attorney General) may,
15 upon an official request to the United States from
16 the foreign country, apply for an order described in
17 paragraph (2) from the district court in which a key
18 holder resides for—

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

21 “(B) obtaining decryption assistance from
22 the key holder.

23 “(2) CONTENTS OF ORDER.—An order de-
24 scribed in this paragraph is an order that directs the
25 key holder involved to—

1 “(A) release a decryption key to the Attor-
2 ney General (or the designee of the Attorney
3 General) for furnishing to the foreign country;
4 or

5 “(B) provide decryption assistance to the
6 Attorney General (or the designee of the Attor-
7 ney General) for furnishing to the foreign coun-
8 try.

9 “(3) REQUIREMENTS FOR ORDER.—A judge of
10 a court described in paragraph (1) may issue an
11 order described in paragraph (2) if the judge finds,
12 on the basis on an application made by the Attorney
13 General under this subsection, that—

14 “(A) the decryption key or decryption as-
15 sistance sought is necessary for the decryption
16 of a communication or information that the for-
17 eign country is authorized to intercept or seize
18 pursuant to the law of the foreign country;

19 “(B) the law of the foreign country pro-
20 vides for adequate protection against arbitrary
21 interference with respect to privacy rights; and

22 “(C) the decryption key or decryption as-
23 sistance is being sought in connection with a
24 criminal investigation for conduct that would
25 constitute a violation of a criminal law of the

1 United States if committed within the jurisdic-
 2 tion of the United States.

3 “(c) DEFINITION.—As used in this section, the term
 4 ‘official request’ has the meaning given that term in sec-
 5 tion 3506(c) of this title.”

6 (b) CLERICAL AMENDMENT.—The chapter analysis
 7 for part I of title 18, United States Code, is amended by
 8 inserting after the item relating to chapter 123 the follow-
 9 ing new item:

**“125. Encrypted wire or electronic communications and
 stored electronic information 2801”.**

10 **SEC. 7. INTELLIGENCE ACTIVITIES.**

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

14 (b) CERTAIN CONDUCT.—Nothing in this Act or the
 15 amendments made by this Act shall affect the conduct,
 16 by officers or employees of the United States Government
 17 in accordance with other applicable Federal law, under
 18 procedures approved by the Attorney General, of activities
 19 intended to—

20 (1) intercept encrypted or other official commu-
 21 nications of United States executive branch entities
 22 or United States Government contractors for com-
 23 munications security purposes;

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

6 (3) access an electronic communication system
7 used exclusively by a foreign power or agent of a for-
8 eign power as so defined.

○