

105TH CONGRESS
2D SESSION

S. 2067

To protect the privacy and constitutional rights of Americans, to establish standards and procedures regarding law enforcement access to decryption assistance for encrypted communications and stored electronic information, to affirm the rights of Americans to use and sell encryption products, and for other purposes.

IN THE SENATE OF THE UNITED STATES

MAY 12, 1998

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

A BILL

To protect the privacy and constitutional rights of Americans, to establish standards and procedures regarding law enforcement access to decryption assistance for encrypted communications and stored electronic information, to affirm the rights of Americans to use and sell encryption products, 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,*

1 **SECTION 1. SHORT TITLE; TABLE OF CONTENTS.**

2 (a) SHORT TITLE.—This Act may be cited as the
3 “Encryption Protects the Rights of Individuals from Vio-
4 lation and Abuse in CYberspace (E–PRIVACY) Act”.

5 (b) TABLE OF CONTENTS.—The table of contents for
6 this Act is as follows:

- Sec. 1. Short title; table of contents.
- Sec. 2. Purposes.
- Sec. 3. Findings.
- Sec. 4. Definitions.

TITLE I—PRIVACY PROTECTION FOR COMMUNICATIONS AND
ELECTRONIC INFORMATION

- Sec. 101. Freedom to use encryption.
- Sec. 102. Purchase and use of encryption products by the Federal Government.
- Sec. 103. Enhanced privacy protection for information on computer networks.
- Sec. 104. Government access to location information.
- Sec. 105. Enhanced privacy protection for transactional information obtained
from pen registers or trap and trace devices.

TITLE II—LAW ENFORCEMENT ASSISTANCE

- Sec. 201. Encrypted wire or electronic communications and stored electronic
communications.

TITLE III—EXPORTS OF ENCRYPTION PRODUCTS

- Sec. 301. Commercial encryption products.
- Sec. 302. License exception for mass market products.
- Sec. 303. License exception for products without encryption capable of working
with encryption products.
- Sec. 304. License exception for product support and consulting services.
- Sec. 305. License exception when comparable foreign products available.
- Sec. 306. No export controls on encryption products used for nonconfidentiality
purposes.
- Sec. 307. Applicability of general export controls.
- Sec. 308. Foreign trade barriers to United States products.

7 **SEC. 2. PURPOSES.**

8 The purposes of this Act are—

- 9 (1) to ensure that Americans have the maxi-
10 mum possible choice in encryption methods to pro-
11 tect the security, confidentiality, and privacy of their

1 lawful wire and electronic communications and
2 stored electronic information;

3 (2) to promote the privacy and constitutional
4 rights of individuals and organizations in networked
5 computer systems and other digital environments,
6 protect the confidentiality of information and secu-
7 rity of critical infrastructure systems relied on by in-
8 dividuals, businesses and government agencies, and
9 properly balance the needs of law enforcement to
10 have the same access to electronic communications
11 and information as under current law; and

12 (3) to establish privacy standards and proce-
13 dures by which investigative or law enforcement offi-
14 cers may obtain decryption assistance for encrypted
15 communications and stored electronic information.

16 **SEC. 3. FINDINGS.**

17 Congress finds that—

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

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

5 (3) the rights of Americans to the privacy and
6 security of their communications and in the conduct-
7 ing of personal and business affairs should be pro-
8 moted and protected;

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

15 (5) individuals will not entrust their sensitive
16 personal, medical, financial, and other information
17 to computers and computer networks unless the se-
18 curity and privacy of that information is assured;

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

1 (7) America’s critical infrastructures, including
2 its telecommunications system, banking and finan-
3 cial infrastructure, and power and transportation in-
4 frastructure, increasingly rely on vulnerable informa-
5 tion systems, and will represent a growing risk to
6 national security and public safety unless the secu-
7 rity and privacy of those information systems is as-
8 sured;

9 (8) encryption technology is an essential tool to
10 promote and protect the privacy, security, confiden-
11 tiality, integrity, and authenticity of wire and elec-
12 tronic communications and stored electronic infor-
13 mation;

14 (9) encryption techniques, technology, pro-
15 grams, and products are widely available worldwide;

16 (10) Americans should be free to use lawfully
17 whatever particular encryption techniques, tech-
18 nologies, programs, or products developed in the
19 marketplace that best suits their needs in order to
20 interact electronically with the government and oth-
21 ers worldwide in a secure, private, and confidential
22 manner;

23 (11) government mandates for, or otherwise
24 compelled use of, third-party key recovery systems or
25 other systems that provide surreptitious access to

1 encrypted data threatens the security and privacy of
2 information systems;

3 (12) American companies should be free to
4 compete and sell encryption technology, programs,
5 and products, and to exchange encryption tech-
6 nology, programs, and products through the use of
7 the Internet, which is rapidly emerging as the pre-
8 ferred method of distribution of computer software
9 and related information;

10 (13) a national encryption policy is needed to
11 advance the development of the national and global
12 information infrastructure, and preserve the right to
13 privacy of Americans and the public safety and na-
14 tional security of the United States;

15 (14) Congress and the American people have
16 recognized the need to balance the right to privacy
17 and the protection of the public safety with national
18 security;

19 (15) the Constitution of the United States per-
20 mits lawful electronic surveillance by investigative or
21 law enforcement officers and the seizure of stored
22 electronic information only upon compliance with
23 stringent standards and procedures; and

24 (16) there is a need to clarify the standards
25 and procedures by which investigative or law en-

1 forcement officers obtain decryption assistance from
2 persons—

3 (A) who are voluntarily entrusted with the
4 means to decrypt wire and electronic commu-
5 nications and stored electronic information; or

6 (B) have information that enables the
7 decryption of such communications and infor-
8 mation.

9 **SEC. 4. DEFINITIONS.**

10 In this Act:

11 (1) **AGENCY.**—The term “agency” has the
12 meaning given the term in section 6 of title 18,
13 United States Code.

14 (2) **COMPUTER HARDWARE.**—The term “com-
15 puter hardware” includes computer systems, equip-
16 ment, application-specific assemblies, smart cards,
17 modules, and integrated circuits.

18 (3) **COMPUTING DEVICE.**—The term “comput-
19 ing device” means a device that incorporates 1 or
20 more microprocessor-based central processing units
21 that are capable of accepting, storing, processing, or
22 providing output of data.

23 (4) **ENCRYPT AND ENCRYPTION.**—The terms
24 “encrypt” and “encryption” refer to the scrambling
25 (and descrambling) of wire communications, elec-

1 tronic communications, or electronically stored infor-
2 mation, using mathematical formulas or algorithms
3 in order to preserve the confidentiality, integrity, or
4 authenticity of, and prevent unauthorized recipients
5 from accessing or altering, such communications or
6 information.

7 (5) ENCRYPTION PRODUCT.—The term
8 “encryption product”—

9 (A) means a computing device, computer
10 hardware, computer software, or technology,
11 with encryption capabilities; and

12 (B) includes any subsequent version of or
13 update to an encryption product, if the
14 encryption capabilities are not changed.

15 (6) EXPORTABLE.—The term “exportable”
16 means the ability to transfer, ship, or transmit to
17 foreign users.

18 (7) KEY.—The term “key” means the variable
19 information used in or produced by a mathematical
20 formula, code, or algorithm, or any component
21 thereof, used to encrypt or decrypt wire communica-
22 tions, electronic communications, or electronically
23 stored information.

1 (8) PERSON.—The term “person” has the
2 meaning given the term in section 2510(6) of title
3 18, United States Code.

4 (9) REMOTE COMPUTING SERVICE.—The term
5 “remote computing service” has the meaning given
6 the term in section 2711(2) of title 18, United
7 States Code.

8 (10) STATE.—The term “State” has the mean-
9 ing given the term in section 3156(a)(5) of title 18,
10 United States Code.

11 (11) TECHNICAL REVIEW.—The term “tech-
12 nical review” means a review by the Secretary, based
13 on information about a product’s encryption capa-
14 bilities supplied by the manufacturer, that an
15 encryption product works as represented.

16 (12) UNITED STATES PERSON.—The term
17 “United States person” means any—

18 (A) United States citizen; or

19 (B) any legal entity that—

20 (i) is organized under the laws of the
21 United States, or any State, the District of
22 Columbia, or any commonwealth, territory,
23 or possession of the United States; and

24 (ii) has its principal place of business
25 in the United States.

1 **TITLE I—PRIVACY PROTECTION**
2 **FOR COMMUNICATIONS AND**
3 **ELECTRONIC INFORMATION**

4 **SEC. 101. FREEDOM TO USE ENCRYPTION.**

5 (a) IN GENERAL.—Except as otherwise provided by
6 this Act and the amendments made by this Act, it shall
7 be lawful for any person within the United States, and
8 for any United States person in a foreign country, to use,
9 develop, manufacture, sell, distribute, or import any
10 encryption product, regardless of the encryption algorithm
11 selected, encryption key length chosen, existence of key re-
12 covery or other plaintext access capability, or implementa-
13 tion or medium used.

14 (b) PROHIBITION ON GOVERNMENT-COMPELLED
15 KEY ESCROW OR KEY RECOVERY ENCRYPTION.—

16 (1) IN GENERAL.—Except as provided in para-
17 graph (3), no agency of the United States nor any
18 State may require, compel, set standards for, condi-
19 tion any approval on, or condition the receipt of any
20 benefit on, a requirement that a decryption key, ac-
21 cess to a decryption key, key recovery information,
22 or other plaintext access capability be—

23 (A) given to any other person, including
24 any agency of the United States or a State, or
25 any entity in the private sector; or

1 (B) retained by any person using
2 encryption.

3 (2) USE OF PARTICULAR PRODUCTS.—No agen-
4 cy of the United States may require any person who
5 is not an employee or agent of the United States or
6 a State to use any key recovery or other plaintext
7 access features for communicating or transacting
8 business with any agency of the United States.

9 (3) EXCEPTION.—The prohibition in paragraph
10 (1) does not apply to encryption used by an agency
11 of the United States or a State, or the employees or
12 agents of such an agency, solely for the internal op-
13 erations and telecommunications systems of the
14 United States or the State.

15 (c) USE OF ENCRYPTION FOR AUTHENTICATION OR
16 INTEGRITY PURPOSES.—

17 (1) IN GENERAL.—The use, development, man-
18 ufacture, sale, distribution and import of encryption
19 products, standards, and services for purposes of as-
20 suring the confidentiality, authenticity, or integrity
21 or access control of electronic information shall be
22 voluntary and market driven.

23 (2) CONDITIONS.—No agency of the United
24 States or a State shall establish any condition, tie,
25 or link between encryption products, standards, and

1 services used for confidentiality, and those used for
2 authentication, integrity, or access control purposes.

3 **SEC. 102. PURCHASE AND USE OF ENCRYPTION PRODUCTS**

4 **BY THE FEDERAL GOVERNMENT.**

5 (a) PURCHASES.—An agency of the United States
6 may purchase encryption products for—

7 (1) the internal operations and telecommuni-
8 cations systems of the agency; or

9 (2) use by, among, and between that agency
10 and any other agency of the United States, the em-
11 ployees of the agency, or persons operating under
12 contract with the agency.

13 (b) INTEROPERABILITY.—To ensure that secure elec-
14 tronic access to the Government is available to persons
15 outside of and not operating under contract with agencies
16 of the United States, the United States shall purchase no
17 encryption product with a key recovery or other plaintext
18 access feature if such key recovery or plaintext access fea-
19 ture would interfere with use of the product's full
20 encryption capabilities when interoperating with other
21 commercial encryption products.

22 **SEC. 103. ENHANCED PRIVACY PROTECTION FOR INFORMA-**
23 **TION ON COMPUTER NETWORKS.**

24 Section 2703 of title 18, United States Code, is
25 amended by adding at the end the following:

1 “(g) ACCESS TO STORED ELECTRONIC INFORMA-
2 TION.—

3 “(1) DISCLOSURE.—

4 “(A) IN GENERAL.—Subject to subpara-
5 graph (B), a governmental entity may require
6 the disclosure by a provider of a remote com-
7 puting service of the contents of an electronic
8 record in networked electronic storage only if
9 the person who created the record is accorded
10 the same protections that would be available if
11 the record had remained in that person’s pos-
12 session.

13 “(B) NETWORKED ELECTRONIC STOR-
14 AGE.—In addition to the requirements of sub-
15 paragraph (A) and subject to paragraph (2), a
16 governmental entity may require the disclosure
17 of the contents of an electronic record in
18 networked electronic storage only—

19 “(i) pursuant to a warrant issued
20 under the Federal Rules of Criminal Pro-
21 cedure or equivalent State warrant, a copy
22 of which warrant shall be served on the
23 person who created the record prior to or
24 at the same time the warrant is served on

1 the provider of the remote computing serv-
2 ice;

3 “(ii) pursuant to a subpoena issued
4 under the Federal Rules of Criminal Pro-
5 cedure or equivalent State warrant, a copy
6 of which subpoena shall be served on the
7 person who created the record, under cir-
8 cumstances allowing that person a mean-
9 ingful opportunity to challenge the sub-
10 poena; or

11 “(iii) upon the consent of the person
12 who created the record.

13 “(2) DEFINITION.—In this subsection, an elec-
14 tronic record is in ‘networked electronic storage’ if—

15 “(A) it is not covered by subsection (a) of
16 this section;

17 “(B) the person holding the record is not
18 authorized to access the contents of such record
19 for any purposes other than in connection with
20 providing the service of storage; and

21 “(C) the person who created the record is
22 able to access and modify it remotely through
23 electronic means.”.

1 **SEC. 104. GOVERNMENT ACCESS TO LOCATION INFORMA-**
2 **TION.**

3 (a) COURT ORDER REQUIRED.—Section 2703 of title
4 18, United States Code, is amended by adding at the end
5 the following:

6 “(h) REQUIREMENTS FOR DISCLOSURE OF LOCA-
7 TION INFORMATION.—A provider of mobile electronic com-
8 munication service shall provide to a governmental entity
9 information generated by and disclosing, on a real time
10 basis, the physical location of a subscriber’s equipment
11 only if the governmental entity obtains a court order
12 issued upon a finding that there is probable cause to be-
13 lieve that an individual using or possessing the subscriber
14 equipment is committing, has committed, or is about to
15 commit a felony offense.”.

16 (b) CONFORMING AMENDMENT.—Section
17 2703(c)(1)(B) of title 18, United States Code, is amended
18 by inserting “or wireless location information covered by
19 subsection (g) of this section” after “(b) of this section”.

20 **SEC. 105. ENHANCED PRIVACY PROTECTION FOR TRANS-**
21 **ACTIONAL INFORMATION OBTAINED FROM**
22 **PEN REGISTERS OR TRAP AND TRACE DE-**
23 **VICES.**

24 Subsection 3123(a) of title 18, United States Code,
25 is amended to read as follows:

1 “(a) IN GENERAL.—Upon an application made under
2 section 3122, the court may enter an ex parte order—

3 “(1) authorizing the installation and use of a
4 pen register or a trap and trace device within the ju-
5 risdiction of the court if the court finds, based on
6 the certification by the attorney for the Government
7 or the State law enforcement or investigative officer,
8 that the information likely to be obtained by such in-
9 stallation and use is relevant to an ongoing criminal
10 investigation; and

11 “(2) directing that the use of the pen register
12 or trap and trace device be conducted in such a way
13 as to minimize the recording or decoding of any elec-
14 tronic or other impulses that are not related to the
15 dialing and signaling information utilized in call
16 processing.”.

17 **TITLE II—LAW ENFORCEMENT**
18 **ASSISTANCE**

19 **SEC. 201. ENCRYPTED WIRE OR ELECTRONIC COMMUNICA-**
20 **TIONS AND STORED ELECTRONIC COMMU-**
21 **NICATIONS.**

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

1 **“CHAPTER 124—ENCRYPTED WIRE OR**
 2 **ELECTRONIC COMMUNICATIONS AND**
 3 **STORED ELECTRONIC INFORMATION**

“Sec.

“2801. Definitions.

“2802. Unlawful use of encryption.

“2803. Access to decryption assistance for communications.

“2804. Access to decryption assistance for stored electronic communications or records.

“2805. Foreign government access to decryption assistance.

“2806. Establishment and operations of National Electronic Technologies Center.

4 **“§ 2801. Definitions**

5 “In this chapter:

6 “(1) DECRYPTION ASSISTANCE.—The term
 7 ‘decryption assistance’ means assistance that pro-
 8 vides or facilitates access to the plaintext of an
 9 encrypted wire or electronic communication or stored
 10 electronic information, including the disclosure of a
 11 decryption key or the use of a decryption key to
 12 produce plaintext.

13 “(2) DECRYPTION KEY.—The term ‘decryption
 14 key’ means the variable information used in or pro-
 15 duced by a mathematical formula, code, or algo-
 16 rithm, or any component thereof, used to decrypt a
 17 wire communication or electronic communication or
 18 stored electronic information that has been
 19 encrypted.

1 “(3) ENCRYPT; ENCRYPTION.—The terms
2 ‘encrypt’ and ‘encryption’ refer to the scrambling
3 (and descrambling) of wire communications, elec-
4 tronic communications, or electronically stored infor-
5 mation, using mathematical formulas or algorithms
6 in order to preserve the confidentiality, integrity, or
7 authenticity of, and prevent unauthorized recipients
8 from accessing or altering, such communications or
9 information.

10 “(4) FOREIGN GOVERNMENT.—The term ‘for-
11 eign government’ has the meaning given the term in
12 section 1116.

13 “(5) OFFICIAL REQUEST.—The term ‘official
14 request’ has the meaning given the term in section
15 3506(c).

16 “(6) INCORPORATED DEFINITIONS.—Any term
17 used in this chapter that is not defined in this chap-
18 ter and that is defined in section 2510, has the
19 meaning given the term in section 2510.

20 **“§ 2802. Unlawful use of encryption**

21 “Any person who, during the commission of a felony
22 under Federal law, knowingly and willfully encrypts any
23 incriminating communication or information relating to
24 that felony, with the intent to conceal that communication

1 or information for the purpose of avoiding detection by
2 a law enforcement agency or prosecutor—

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

6 “(2) in the case of a second or subsequent of-
7 fense under this section, shall be imprisoned not
8 more than 10 years, fined under this title, or both.

9 **“§ 2803. Access to decryption assistance for commu-
10 nications**

11 “(a) CRIMINAL INVESTIGATIONS.—

12 “(1) IN GENERAL.—An order authorizing the
13 interception of a wire or electronic communication
14 under section 2518 shall, upon request of the appli-
15 cant, direct that a provider of wire or electronic
16 communication service, or any other person possess-
17 ing information capable of decrypting that commu-
18 nication, other than a person whose communications
19 are the subject of the interception, shall promptly
20 furnish the applicant with the necessary decryption
21 assistance, if the court finds that the decryption as-
22 sistance sought is necessary for the decryption of a
23 communication intercepted pursuant to the order.

1 “(2) LIMITATIONS.—Each order described in
2 paragraph (1), and any extension of such an order,
3 shall—

4 “(A) contain a provision that the
5 decryption assistance provided shall involve dis-
6 closure of a private key only if no other form
7 of decryption assistance is available and other-
8 wise shall be limited to the minimum necessary
9 to decrypt the communications intercepted pur-
10 suant to this chapter; and

11 “(B) terminate on the earlier of—

12 “(i) the date on which the authorized
13 objective is attained; or

14 “(ii) 30 days after the date on which
15 the order or extension, as applicable, is
16 issued.

17 “(3) NOTICE.—If decryption assistance is pro-
18 vided pursuant to an order under this subsection,
19 the court issuing the order described in paragraph
20 (1)—

21 “(A) shall cause to be served on the person
22 whose communications are the subject of such
23 decryption assistance, as part of the inventory
24 required to be served pursuant to section
25 2518(8), notice of the receipt of the decryption

1 assistance and a specific description of the keys
2 or other assistance disclosed; and

3 “(B) upon the filing of a motion and for
4 good cause shown, shall make available to such
5 person, or to counsel for that person, for in-
6 spection, the intercepted communications to
7 which the decryption assistance related, except
8 that on an ex parte showing of good cause, the
9 serving of the inventory required by section
10 2518(8) may be postponed.

11 “(b) FOREIGN INTELLIGENCE INVESTIGATIONS.—

12 “(1) IN GENERAL.—An order authorizing the
13 interception of a wire or electronic communication
14 under section 105(b)(2) of the Foreign Intelligence
15 Surveillance Act of 1978 (50 U.S.C. 1805(b)(2))
16 shall, upon request of the applicant, direct that a
17 provider of wire or electronic communication service
18 or any other person possessing information capable
19 of decrypting such communications, other than a
20 person whose communications are the subject of the
21 interception, shall promptly furnish the applicant
22 with the necessary decryption assistance, if the court
23 finds that the decryption assistance sought is nec-
24 essary for the decryption of a communication inter-
25 cepted pursuant to the order.

1 “(2) LIMITATIONS.—Each order described in
2 paragraph (1), and any extension of such an order,
3 shall—

4 “(A) contain a provision that the
5 decryption assistance provided shall be limited
6 to the minimum necessary to decrypt the com-
7 munications intercepted pursuant to this chap-
8 ter; and

9 “(B) terminate on the earlier of—

10 “(i) the date on which the authorized
11 objective is attained; or

12 “(ii) 30 days after the date on which
13 the order or extension, as applicable, is
14 issued.

15 “(c) GENERAL PROHIBITION ON DISCLOSURE.—
16 Other than pursuant to an order under subsection (a) or
17 (b) of this section, no person possessing information capa-
18 ble of decrypting a wire or electronic communication of
19 another person shall disclose that information or provide
20 decryption assistance to an investigative or law enforce-
21 ment officer (as defined in section 2510(7)).

22 **“§ 2804. Access to decryption assistance for stored**
23 **electronic communications or records**

24 “(a) DECRYPTION ASSISTANCE.—No person may dis-
25 close a decryption key or provide decryption assistance

1 pertaining to the contents of stored electronic communica-
2 tions or records, including those disclosed pursuant to sec-
3 tion 2703, to a governmental entity, except—

4 “(1) pursuant to a warrant issued under the
5 Federal Rules of Criminal Procedure or an equiva-
6 lent State warrant, a copy of which warrant shall be
7 served on the person who created the electronic com-
8 munication prior to or at the same time service is
9 made on the keyholder;

10 “(2) pursuant to a subpoena, a copy of which
11 subpoena shall be served on the person who created
12 the electronic communication or record, under cir-
13 cumstances allowing the person meaningful oppor-
14 tunity to challenge the subpoena; or

15 “(3) upon the consent of the person who cre-
16 ated the electronic communication or record.

17 “(b) DELAY OF NOTIFICATION.—In the case of com-
18 munications disclosed pursuant to section 2703(a), service
19 of the copy of the warrant or subpoena on the person who
20 created the electronic communication under subsection (a)
21 may be delayed for a period of not to exceed 90 days upon
22 request to the court by the governmental entity requiring
23 the decryption assistance, if the court determines that
24 there is reason to believe that notification of the existence

1 of the court order or subpoena may have an adverse result
2 described in section 2705(a)(2).

3 **“§ 2805. Foreign government access to decryption as-**
4 **sistance**

5 “(a) IN GENERAL.—No investigative or law enforce-
6 ment officer may—

7 “(1) release a decryption key to a foreign gov-
8 ernment or to a law enforcement agency of a foreign
9 government; or

10 “(2) except as provided in subsection (b), pro-
11 vide decryption assistance to a foreign government
12 or to a law enforcement agency of a foreign govern-
13 ment.

14 “(b) CONDITIONS FOR COOPERATION WITH FOREIGN
15 GOVERNMENT.—

16 “(1) APPLICATION FOR AN ORDER.—In any
17 case in which the United States has entered into a
18 treaty or convention with a foreign government to
19 provide mutual assistance with respect to providing
20 decryption assistance, the Attorney General (or the
21 designee of the Attorney General) may, upon an offi-
22 cial request to the United States from the foreign
23 government, apply for an order described in para-
24 graph (2) from the district court in which the person

1 possessing information capable of decrypting the
2 communication or information at issue resides—

3 “(A) directing that person to release a
4 decryption key or provide decryption assistance
5 to the Attorney General (or the designee of the
6 Attorney General); and

7 “(B) authorizing the Attorney General (or
8 the designee of the Attorney General) to furnish
9 the foreign government with the plaintext of the
10 encrypted communication or stored electronic
11 information at issue.

12 “(2) CONTENTS OF ORDER.—An order is de-
13 scribed in this paragraph if it is an order directing
14 the person possessing information capable of
15 decrypting the communication or information at
16 issue to—

17 “(A) release a decryption key to the Attor-
18 ney General (or the designee of the Attorney
19 General) so that the plaintext of the commu-
20 nication or information may be furnished to the
21 foreign government; or

22 “(B) provide decryption assistance to the
23 Attorney General (or the designee of the Attor-
24 ney General) so that the plaintext of the com-

1 munication or information may be furnished to
2 the foreign government.

3 “(3) REQUIREMENTS FOR ORDER.—The court
4 described in paragraph (1) may issue an order de-
5 scribed in paragraph (2) if the court finds, on the
6 basis of an application made by the Attorney Gen-
7 eral under this subsection, that—

8 “(A) the decryption key or decryption as-
9 sistance sought is necessary for the decryption
10 of a communication or information that the for-
11 eign government is authorized to intercept or
12 seize pursuant to the law of that foreign coun-
13 try;

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

17 “(C) the decryption key or decryption as-
18 sistance is being sought in connection with a
19 criminal investigation for conduct that would
20 constitute a violation of a criminal law of the
21 United States if committed within the jurisdic-
22 tion of the United States.

1 **“§ 2806. Establishment and operations of National**
2 **Electronic Technologies Center**

3 “(a) NATIONAL ELECTRONIC TECHNOLOGIES CEN-
4 TER.—

5 “(1) ESTABLISHMENT.—There is established in
6 the Department of Justice a National Electronic
7 Technologies Center (referred to in this section as
8 the ‘NET Center’).

9 “(2) DIRECTOR.—The NET Center shall be ad-
10 ministered by a Director (referred to in this section
11 as the ‘Director’), who shall be appointed by the At-
12 torney General.

13 “(3) DUTIES.—The NET Center shall—

14 “(A) serve as a center for Federal, State,
15 and local law enforcement authorities for infor-
16 mation and assistance regarding decryption and
17 other access requirements;

18 “(B) serve as a center for industry and
19 government entities to exchange information
20 and methodology regarding information security
21 techniques and technologies;

22 “(C) support and share information and
23 methodology regarding information security
24 techniques and technologies with the Computer
25 Investigations and Infrastructure Threat As-
26 sessment Center (CITAC) and Field Computer

1 Investigations and Infrastructure Threat As-
2 sessment (CITA) Squads of the Federal Bureau
3 of Investigation;

4 “(D) examine encryption techniques and
5 methods to facilitate the ability of law enforce-
6 ment to gain efficient access to plaintext of
7 communications and electronic information;

8 “(E) conduct research to develop efficient
9 methods, and improve the efficiency of existing
10 methods, of accessing plaintext of communica-
11 tions and electronic information;

12 “(F) investigate and research new and
13 emerging techniques and technologies to facili-
14 tate access to communications and electronic in-
15 formation, including—

16 “(i) reverse-stenography;

17 “(ii) decompression of information
18 that previously has been compressed for
19 transmission; and

20 “(iii) demultiplexing;

21 “(G) investigate and research interception
22 and access techniques that preserve the privacy
23 and security of information not authorized to be
24 intercepted; and

1 “(H) obtain information regarding the
2 most current hardware, software, telecommuni-
3 cations, and other capabilities to understand
4 how to access digitized information transmitted
5 across networks.

6 “(4) EQUAL ACCESS.—State and local law en-
7 forcement agencies and authorities shall have access
8 to information, services, resources, and assistance
9 provided by the NET Center to the same extent that
10 Federal law enforcement agencies and authorities
11 have such access.

12 “(5) PERSONNEL.—The Director may appoint
13 such personnel as the Director considers appropriate
14 to carry out the duties of the NET Center.

15 “(6) ASSISTANCE OF OTHER FEDERAL AGEN-
16 CIES.—Upon the request of the Director of the NET
17 Center, the head of any department or agency of the
18 Federal Government may, to assist the NET Center
19 in carrying out its duties under this subsection—

20 “(A) detail, on a reimbursable basis, any of
21 the personnel of such department or agency to
22 the NET Center; and

23 “(B) provide to the NET Center facilities,
24 information, and other nonpersonnel resources.

1 “(7) PRIVATE INDUSTRY ASSISTANCE.—The
2 NET Center may accept, use, and dispose of gifts,
3 bequests, or devises of money, services, or property,
4 both real and personal, for the purpose of aiding or
5 facilitating the work of the Center. Gifts, bequests,
6 or devises of money and proceeds from sales of other
7 property received as gifts, bequests, or devises shall
8 be deposited in the Treasury and shall be available
9 for disbursement upon order of the Director of the
10 NET Center.

11 “(8) ADVISORY BOARD.—

12 “(A) ESTABLISHMENT.—There is estab-
13 lished in the NET Center an Advisory Board
14 for Excellence in Information Security (in this
15 paragraph referred to as the ‘Advisory Board’),
16 which shall be comprised of members who have
17 the qualifications described in subparagraph
18 (B) and who are appointed by the Attorney
19 General. The Attorney General shall appoint a
20 chairman of the Advisory Board.

21 “(B) QUALIFICATIONS.—Each member of
22 the Advisory Board shall have experience or ex-
23 pertise in the field of encryption, decryption,
24 electronic communication, information security,

1 electronic commerce, privacy protection, or law
2 enforcement.

3 “(C) DUTIES.—The duty of the Advisory
4 Board shall be to advise the NET Center and
5 the Federal Government regarding new and
6 emerging technologies relating to encryption
7 and decryption of communications and elec-
8 tronic information.

9 “(9) IMPLEMENTATION PLAN.—

10 “(A) IN GENERAL.—Not later than 2
11 months after the date of enactment of this
12 chapter, the Attorney General shall, in con-
13 sultation and cooperation with other appro-
14 priate Federal agencies and appropriate indus-
15 try participants, develop and cause to be pub-
16 lished in the Federal Register a plan for estab-
17 lishing the NET Center.

18 “(B) CONTENTS OF PLAN.—The plan pub-
19 lished under subparagraph (A) shall—

20 “(i) specify the physical location of
21 the NET Center and the equipment, soft-
22 ware, and personnel resources necessary to
23 carry out the duties of the NET Center
24 under this subsection;

1 (b) CONTROL BY SECRETARY OF COMMERCE.—Sub-
2 ject to the provisions of this title, and notwithstanding any
3 other provision of law, the Secretary of Commerce shall
4 have exclusive authority to control exports of encryption
5 products covered under subsection (a).

6 **SEC. 302. LICENSE EXCEPTION FOR MASS MARKET PROD-**
7 **UCTS.**

8 (a) EXPORT CONTROL RELIEF.—Subject to section
9 307, an encryption product that is generally available, or
10 incorporates or employs in any form, implementation, or
11 medium, an encryption product that is generally available,
12 shall be exportable without the need for an export license,
13 and without restrictions other than those permitted under
14 this Act, after a 1-time 15-day technical review by the Sec-
15 retary of Commerce.

16 (b) DEFINITIONS.—In this section, the term “gen-
17 erally available” means an encryption product that is—

18 (1) offered for sale, license, or transfer to any
19 person without restriction, whether or not for con-
20 sideration, including, but not limited to, over-the-
21 counter retail sales, mail order transactions, phone
22 order transactions, electronic distribution, or sale on
23 approval; and

24 (2) not designed, developed, or customized by
25 the manufacturer for specific purchasers except for

1 user or purchaser selection among installation or
2 configuration parameters.

3 (c) COMMERCE DEPARTMENT ASSURANCE.—

4 (1) IN GENERAL.—The manufacturer or ex-
5 porter of an encryption product may request written
6 assurance from the Secretary of Commerce that an
7 encryption product is considered generally available
8 for purposes of this section.

9 (2) RESPONSE.—Not later than 30 days after
10 receiving a request under paragraph (1), the Sec-
11 retary shall make a determination regarding whether
12 to issue a written assurance under that paragraph,
13 and shall notify the person making the request, in
14 writing, of that determination.

15 (3) EFFECT ON MANUFACTURERS AND EXPORT-
16 ERS.—A manufacturer or exporter who obtains a
17 written assurance under this subsection shall not be
18 held liable, responsible, or subject to sanctions for
19 failing to obtain an export license for the encryption
20 product at issue.

21 **SEC. 303. LICENSE EXCEPTION FOR PRODUCTS WITHOUT**
22 **ENCRYPTION CAPABLE OF WORKING WITH**
23 **ENCRYPTION PRODUCTS.**

24 Subject to section 307, any product that does not
25 itself provide encryption capabilities, but that incorporates

1 or employs in any form cryptographic application pro-
2 gramming interfaces or other interface mechanisms for
3 interaction with other encryption products covered by sec-
4 tion 301(a), shall be exportable without the need for an
5 export license, and without restrictions other than those
6 permitted under this Act, after a 1-time, 15-day technical
7 review by the Secretary of Commerce.

8 **SEC. 304. LICENSE EXCEPTION FOR PRODUCT SUPPORT**
9 **AND CONSULTING SERVICES.**

10 (a) **NO ADDITIONAL EXPORT CONTROLS IMPOSED IF**
11 **UNDERLYING PRODUCT COVERED BY LICENSE EXCEP-**
12 **TION.**—Technical assistance and technical data associated
13 with the installation and maintenance of encryption prod-
14 ucts covered by sections 302 and 303 shall be exportable
15 without the need for an export license, and without restric-
16 tions other than those permitted under this Act.

17 (b) **DEFINITIONS.**—In this section:

18 (1) **TECHNICAL ASSISTANCE.**—The term “tech-
19 nical assistance” means services, including instruc-
20 tion, skills training, working knowledge, and consult-
21 ing services, and the transfer of technical data.

22 (2) **TECHNICAL DATA.**—The term “technical
23 data” means information including blueprints, plans,
24 diagrams, models, formulae, tables, engineering de-
25 signs and specifications, manuals and instructions

1 written or recorded on other media or devices such
2 as disk, tape, or read-only memories.

3 **SEC. 305. LICENSE EXCEPTION WHEN COMPARABLE FOR-**
4 **EIGN PRODUCTS AVAILABLE.**

5 (a) FOREIGN AVAILABILITY STANDARD.—An
6 encryption product not qualifying under section 302 shall
7 be exportable without the need for an export license, and
8 without restrictions other than those permitted under this
9 Act, after a 1-time 15-day technical review by the Sec-
10 retary of Commerce, if an encryption product utilizing the
11 same or greater key length or otherwise providing com-
12 parable security to such encryption product is, or will be
13 within the next 18 months, commercially available outside
14 the United States from a foreign supplier.

15 (b) DETERMINATION OF FOREIGN AVAILABILITY.—

16 (1) ENCRYPTION EXPORT ADVISORY BOARD ES-
17 TABLISHED.—There is hereby established a board to
18 be known as the “Encryption Export Advisory
19 Board” (in this section referred to as the “Board”).

20 (2) MEMBERSHIP.—The Board shall be com-
21 prised of—

22 (A) the Under Secretary of Commerce for
23 Export Administration, who shall be Chairman;

24 (B) seven individuals appointed by the
25 President, of whom—

1 (i) one shall be a representative from
2 each of—

3 (I) the National Security Agency;

4 (II) the Central Intelligence
5 Agency; and

6 (III) the Office of the President;

7 and

8 (ii) four shall be individuals from the
9 private sector who have expertise in the de-
10 velopment, operation, or marketing of in-
11 formation technology products; and

12 (C) four individuals appointed by Congress
13 from among individuals in the private sector
14 who have expertise in the development, oper-
15 ation, or marketing of information technology
16 products, of whom—

17 (i) one shall be appointed by the Ma-
18 jority Leader of the Senate;

19 (ii) one shall be appointed by the Mi-
20 nority Leader of the Senate;

21 (iii) one shall be appointed by the
22 Speaker of the House of Representatives;
23 and

1 (iv) one shall be appointed by the Mi-
2 nority Leader of the House of Representa-
3 tives.

4 (3) MEETINGS.—

5 (A) IN GENERAL.—Subject to subpara-
6 graph (B), the Board shall meet at the call of
7 the Under Secretary of Commerce for Export
8 Administration.

9 (B) MEETINGS WHEN APPLICATIONS
10 PENDING.—If any application referred to in
11 paragraph (4)(A) is pending, the Board shall
12 meet not less than once every 30 days.

13 (4) DUTIES.—

14 (A) IN GENERAL.—Whenever an applica-
15 tion for a license exception for an encryption
16 product under this section is submitted to the
17 Secretary of Commerce, the Board shall deter-
18 mine whether a comparable encryption product
19 is commercially available outside the United
20 States from a foreign supplier as specified in
21 subsection (a).

22 (B) MAJORITY VOTE REQUIRED.—The
23 Board shall make a determination under this
24 paragraph upon a vote of the majority of the
25 members of the Board.

1 (C) DEADLINE.—The Board shall make a
2 determination with respect to an encryption
3 product under this paragraph not later than 30
4 days after receipt by the Secretary of an appli-
5 cation for a license exception under this sub-
6 section based on the encryption product.

7 (D) NOTICE OF DETERMINATIONS.—The
8 Board shall notify the Secretary of Commerce
9 of each determination under this paragraph.

10 (E) REPORTS TO PRESIDENT.—Not later
11 than 30 days after a meeting under this para-
12 graph, the Board shall submit to the President
13 a report on the meeting.

14 (F) APPLICABILITY OF FACAA.—The provi-
15 sions of the Federal Advisory Committee Act (5
16 U.S.C. App.) shall not apply to the Board or to
17 meetings held by the Board under this para-
18 graph.

19 (5) ACTION BY SECRETARY OF COMMERCE.—

20 (A) APPROVAL OR DISAPPROVAL.—The
21 Secretary of Commerce shall specifically ap-
22 prove or disapprove each determination of the
23 Board under paragraph (5) not later than 30
24 days of the submittal of such determination to
25 the Secretary under that paragraph.

1 (B) NOTIFICATION AND PUBLICATION OF
2 DECISION.—The Secretary of Commerce shall—

3 (i) notify the Board of each approval
4 or disapproval under this paragraph; and

5 (ii) publish a notice of the approval or
6 disapproval in the Federal Register.

7 (C) CONTENTS OF NOTICE.—Each notice
8 of a decision of disapproval by the Secretary of
9 Commerce under subparagraph (B) of a deter-
10 mination of the Board under paragraph (4)
11 that an encryption product is commercially
12 available outside the United States from a for-
13 eign supplier shall set forth an explanation in
14 detail of the reasons for the decision, including
15 why and how continued export control of the
16 encryption product which the determination
17 concerned will be effective in achieving its pur-
18 pose and the amount of lost sales and loss in
19 market share of United States encryption prod-
20 ucts as a result of the decision.

21 (6) JUDICIAL REVIEW.—Notwithstanding any
22 other provision of law, a decision of disapproval by
23 the Secretary of Commerce under paragraph (5) of
24 a determination of the Board under paragraph (4)
25 that an encryption product is commercially available

1 outside the United States from a foreign supplier
2 shall be subject to judicial review under the provi-
3 sions of subchapter II of chapter 5 of title 5, United
4 States Code (commonly referred to as the “Adminis-
5 trative Procedures Act”).

6 (c) INCLUSION OF COMPARABLE FOREIGN
7 ENCRYPTION PRODUCT IN A UNITED STATES PRODUCT
8 NOT BASIS FOR EXPORT CONTROLS.—A product that in-
9 corporates or employs a foreign encryption product, in the
10 way it was intended to be used and that the Board has
11 determined to be commercially available outside the
12 United States, shall be exportable without the need for
13 an export license and without restrictions other than those
14 permitted under this Act, after a 1-time 15-day technical
15 review by the Secretary of Commerce.

16 **SEC. 306. NO EXPORT CONTROLS ON ENCRYPTION PROD-**
17 **UCTS USED FOR NONCONFIDENTIALITY PUR-**
18 **POSES.**

19 (a) PROHIBITION ON NEW CONTROLS.—The Federal
20 Government shall not restrict the export of encryption
21 products used for nonconfidentiality purposes such as au-
22 thentication, integrity, digital signatures, nonrepudiation,
23 and copy protection.

24 (b) NO REINSTATEMENT OF CONTROLS ON PRE-
25 VIOUSLY DECONTROLLED PRODUCTS.—Those encryption

1 products previously decontrolled and not requiring an ex-
2 port license as of January 1, 1998, as a result of adminis-
3 trative decision or rulemaking shall not require an export
4 license.

5 **SEC. 307. APPLICABILITY OF GENERAL EXPORT CONTROLS.**

6 (a) SUBJECT TO TERRORIST AND EMBARGO CON-
7 TROLS.—Nothing in this Act shall be construed to limit
8 the authority of the President under the International
9 Emergency Economic Powers Act, the Trading with the
10 Enemy Act, or the Export Administration Act, to—

11 (1) prohibit the export of encryption products
12 to countries that have been determined to repeatedly
13 provide support for acts of international terrorism;
14 or

15 (2) impose an embargo on exports to, and im-
16 ports from, a specific country.

17 (b) SUBJECT TO SPECIFIC DENIALS FOR SPECIFIC
18 REASONS.—The Secretary of Commerce shall prohibit the
19 export of particular encryption products to an individual
20 or organization in a specific foreign country identified by
21 the Secretary if the Secretary determines that there is
22 substantial evidence that such encryption products will be
23 used for military or terrorist end-use, including acts
24 against the national security, public safety, or the integrity

1 of the transportation, communications, or other essential
2 systems of interstate commerce in the United States.

3 (c) OTHER EXPORT CONTROLS REMAIN APPLICA-
4 BLE.—(1) Encryption products shall remain subject to all
5 export controls imposed on such products for reasons
6 other than the existence of encryption capabilities.

7 (2) Nothing in this Act alters the Secretary’s ability
8 to control exports of products for reasons other than
9 encryption.

10 **SEC. 308. FOREIGN TRADE BARRIERS TO UNITED STATES**
11 **PRODUCTS.**

12 Not later than 180 days after the date of enactment
13 of this Act, the Secretary of Commerce, in consultation
14 with the United States Trade Representative, shall—

15 (1) identify foreign barriers to exports of
16 United States encryption products;

17 (2) initiate appropriate actions to address such
18 barriers; and

19 (3) submit to Congress a report on the actions
20 taken under this section.

○