

104TH CONGRESS  
2D SESSION

# S. 1587

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

---

## IN THE SENATE OF THE UNITED STATES

MARCH 5, 1996

Mr. LEAHY (for himself, Mr. BURNS, Mr. DOLE, Mr. PRESSLER, and Mrs. MURRAY) 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 escrowed 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 1996”.

6 **SEC. 2. PURPOSE.**

7 It is the purpose of this Act—

8 (1) to ensure that Americans are able to have  
9 the maximum possible choice in encryption methods

1 to protect the security, confidentiality, and privacy  
2 of their lawful wire or electronic communications;  
3 and

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

10 **SEC. 3. FINDINGS.**

11 The Congress finds that—

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

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

23 (3) the rights of Americans to the privacy and  
24 security of their communications and in conducting

1 their personal and business affairs should be pre-  
2 served and protected;

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

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

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

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

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

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

7           (10) American companies should be free to  
8 compete and to sell encryption technology, programs,  
9 and products;

10           (11) there is a need to develop a national  
11 encryption policy that advances the development of  
12 the national and global information infrastructure,  
13 and preserves Americans' right to privacy and the  
14 Nation's public safety and national security;

15           (12) there is a need to clarify the legal rights  
16 and responsibilities of key holders who are volun-  
17 tarily entrusted with the means to decrypt wire or  
18 electronic communications;

19           (13) the Congress and the American people  
20 have recognized the need to balance the right to pri-  
21 vacy and the protection of the public safety and na-  
22 tional security;

23           (14) the Congress has permitted lawful elec-  
24 tronic surveillance by investigative or law enforce-

1       ment officers only upon compliance with stringent  
2       statutory standards and procedures; and

3               (15) there is a need to clarify the standards  
4       and procedures by which investigative or law en-  
5       forcement officers obtain assistance from key holders  
6       who are voluntarily entrusted with the means to  
7       decrypt wire or electronic communications, including  
8       such communications in electronic storage.

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

10       (a) **LAWFUL USE OF ENCRYPTION.**—It shall be law-  
11       ful for any person within any State of the United States,  
12       the District of Columbia, the Commonwealth of Puerto  
13       Rico, and any territory or possession of the United States,  
14       and by United States persons in a foreign country to use  
15       any encryption, regardless of encryption algorithm se-  
16       lected, encryption key length chosen, or implementation  
17       technique or medium used except as provided in this Act  
18       and the amendments made by this Act or in any other  
19       law.

20       (b) **GENERAL CONSTRUCTION.**—Nothing in this Act  
21       or the amendments made by this Act shall be construed  
22       to—

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



1 preserve the confidentiality, integrity or authenticity  
2 and prevent unauthorized recipients from accessing  
3 or altering such communications;

4 “(3) the term ‘key holder’ means a person lo-  
5 cated within the United States (which may, but is  
6 not required to, be a Federal agency) who is volun-  
7 tarily entrusted by another independent person with  
8 the means to decrypt that person’s wire or electronic  
9 communications for the purpose of subsequent  
10 decryption of such communications;

11 “(4) the term ‘decryption key’ means the vari-  
12 able information used in a mathematical formula,  
13 code, or algorithm, or any component thereof, used  
14 to decrypt wire or electronic communications that  
15 have been encrypted; and

16 “(5) the term ‘decryption assistance’ means  
17 providing access, to the extent possible, to the plain  
18 text of encrypted wire or electronic communications.

19 **“§ 2802. Prohibited acts by key holders**

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

1       “(b) AUTHORIZED RELEASE OF KEY.—A key holder  
2 shall only release a decryption key in its possession or con-  
3 trol or provide decryption assistance—

4           “(1) with the lawful consent of the person  
5 whose key is being held or managed by the key hold-  
6 er;

7           “(2) as may be necessarily incident to the hold-  
8 ing or management of the key by the key holder; or

9           “(3) to investigative or law enforcement officers  
10 authorized by law to intercept wire or electronic  
11 communications under chapter 119, to obtain access  
12 to stored wire and electronic communications and  
13 transactional records under chapter 121, or to con-  
14 duct electronic surveillance, as defined in section  
15 101 of the Foreign Intelligence Surveillance Act of  
16 1978 (50 U.S.C. 1801), upon compliance with sub-  
17 section (c) of this section.

18       “(c) REQUIREMENTS FOR RELEASE OF DECRYPTION  
19 KEY OR PROVISION OF DECRYPTION ASSISTANCE TO IN-  
20 VESTIGATIVE OR LAW ENFORCEMENT OFFICER.—

21           “(1) CONTENTS OF WIRE AND ELECTRONIC  
22 COMMUNICATIONS.—A key holder is authorized to  
23 release a decryption key or provide decryption assist-  
24 ance to an investigative or law enforcement officer

1 authorized by law to conduct electronic surveillance  
2 under chapter 119, only if—

3 “(A) the key holder is given—

4 “(i) a court order signed by a judge of  
5 competent jurisdiction directing such re-  
6 lease or assistance; or

7 “(ii) a certification in writing by a  
8 person specified in section 2518(7) or the  
9 Attorney General stating that—

10 “(I) no warrant or court order is  
11 required by law;

12 “(II) all requirements under sec-  
13 tion 2518(7) have been met; and

14 “(III) the specified release or as-  
15 sistance is required;

16 “(B) the order or certification under para-  
17 graph (A)—

18 “(i) specifies the decryption key or  
19 decryption assistance which is being  
20 sought; and

21 “(ii) identifies the termination date of  
22 the period for which release or assistance  
23 has been authorized; and

24 “(C) in compliance with an order or certifi-  
25 cation under subparagraph (A), the key holder

1           shall provide only such key release or  
2           decryption assistance as is necessary for access  
3           to communications covered by subparagraph  
4           (B).

5           “(2) STORED WIRE AND ELECTRONIC COMMU-  
6           NICATIONS.—(A) A key holder is authorized to re-  
7           lease a decryption key or provide decryption assist-  
8           ance to an investigative or law enforcement officer  
9           authorized by law to obtain access to stored wire  
10          and electronic communications and transactional  
11          records under chapter 121, only if the key holder is  
12          directed to give such assistance pursuant to the  
13          same lawful process (court warrant, order, subpoena,  
14          or certification) used to obtain access to the stored  
15          wire and electronic communications and trans-  
16          actional records.

17          “(B) The notification required under section  
18          2703(b) shall, in the event that encrypted wire or  
19          electronic communications were obtained from elec-  
20          tronic storage, include notice of the fact that a key  
21          to such communications was or was not released or  
22          decryption assistance was or was not provided by a  
23          key holder.

24          “(C) In compliance with the lawful process  
25          under subparagraph (A), the key holder shall pro-

1       vide only such key release or decryption assistance  
2       as is necessary for access to the communications  
3       covered by such lawful process.

4               “(3) USE OF KEY.—(A) An investigative or law  
5       enforcement officer to whom a key has been released  
6       under this subsection may use the key only in the  
7       manner and for the purpose and duration that is ex-  
8       pressly provided for in the court order or other pro-  
9       vision of law authorizing such release and use, not  
10      to exceed the duration of the electronic surveillance  
11      for which the key was released.

12              “(B) On or before completion of the authorized  
13      release period, the investigative or law enforcement  
14      officer to whom a key has been released shall de-  
15      stroy and not retain the released key.

16              “(C) The inventory required to be served pursu-  
17      ant to section 2518(8)(d) on persons named in the  
18      order or the application under section 2518(7)(b),  
19      and such other parties to intercepted communica-  
20      tions as the judge may determine, in the interest of  
21      justice, shall, in the event that encrypted wire or  
22      electronic communications were intercepted, include  
23      notice of the fact that during the period of the order  
24      or extensions thereof a key to, or decryption assist-  
25      ance for, any encrypted wire or electronic commu-

1       nications of the person or party intercepted was or  
2       was not provided by a key holder.

3           “(4) NONDISCLOSURE OF RELEASE.—No key  
4       holder, officer, employee, or agent thereof shall dis-  
5       close the key release or provision of decryption as-  
6       sistance pursuant to subsection (b), except as may  
7       otherwise be required by legal process and then only  
8       after prior notification to the Attorney General or to  
9       the principal prosecuting attorney of a State or any  
10      political subdivision of a State, as may be appro-  
11      priate.

12       “(d) RECORDS OR OTHER INFORMATION HELD BY  
13      KEY HOLDERS.—A key holder, shall not disclose a record  
14      or other information (not including the key) pertaining to  
15      any person whose key is being held or managed by the  
16      key holder, except—

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

20           “(2) to an investigative or law enforcement offi-  
21       cer pursuant to a subpoena authorized under Fed-  
22       eral or State law, court order, or lawful process.

23      An investigative or law enforcement officer receiving a  
24      record or information under paragraph (2) is not required  
25      to provide notice to the person to whom the record or in-

1 formation pertains. Any disclosure in violation of this sub-  
2 section shall render the person committing the violation  
3 liable for the civil damages provided for in subsection (f).

4 “(e) CRIMINAL PENALTIES.—The punishment for an  
5 offense under subsection (a) of this section is—

6 “(1) if the offense is committed for a tortious,  
7 malicious, or illegal purpose, or for purposes of di-  
8 rect or indirect commercial advantage or private  
9 commercial gain—

10 “(A) a fine under this title or imprison-  
11 ment for not more than 1 year, or both, in the  
12 case of a first offense under this subparagraph;  
13 or

14 “(B) a fine under this title or imprison-  
15 ment for not more than 2 years, or both, for  
16 any second or subsequent offense; and

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

21 “(f) CIVIL DAMAGES.—

22 “(1) IN GENERAL.—Any person aggrieved by  
23 any act of a person in violation of subsections (a) or  
24 (d) may in a civil action recover from such person  
25 appropriate relief.

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

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

5                   “(B) damages under paragraph (3) and  
6                   punitive damages in appropriate cases; and

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

9           “(3) COMPUTATION OF DAMAGES.—The court  
10           may assess as damages whichever is the greater of—

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

14                   “(B) statutory damages in the amount of  
15                   \$5,000.

16           “(4) LIMITATION.—A civil action under this  
17           subsection shall not be commenced later than 2  
18           years after the date upon which the plaintiff first  
19           knew or should have known of the violation.

20           “(g) DEFENSE.—It shall be a complete defense  
21           against any civil or criminal action brought under this  
22           chapter that the defendant acted in good faith reliance  
23           upon a court warrant or order, grand jury or trial sub-  
24           poena, or statutory authorization.

1 **“§ 2803. Reporting requirements**

2       “(a) IN GENERAL.—In reporting to the Administra-  
3 tive Office of the United States Courts as required under  
4 section 2519(2) of this title, the Attorney General, an As-  
5 sistant Attorney General specially designated by the Attor-  
6 ney General, the principal prosecuting attorney of a State,  
7 or the principal prosecuting attorney of any political sub-  
8 division of a State, shall report on the number of orders  
9 and extensions served on key holders to obtain access to  
10 decryption keys or decryption assistance.

11       “(b) REQUIREMENTS.—The Director of the Adminis-  
12 trative Office of the United States Courts shall include  
13 as part of the report transmitted to the Congress under  
14 section 2519(3) of this title, the number of orders and  
15 extensions served on key holders to obtain access to  
16 decryption keys or decryption assistance and the offenses  
17 for which the orders were obtained.

18 **“§ 2804. Unlawful use of encryption to obstruct jus-**  
19 **tice**

20       “Whoever willfully endeavors by means of encryption  
21 to obstruct, impede, or prevent the communication of in-  
22 formation in furtherance of a felony which may be pros-  
23 ecuted in a court of the United States, to an investigative  
24 or law enforcement officer shall—

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

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

7   **“§ 2805. Freedom to sell encryption products**

8           “(a) IN GENERAL.—It shall be lawful for any person  
9           within any State of the United States, the District of Co-  
10          lumbia, the Commonwealth of Puerto Rico, and any terri-  
11          tory or possession of the United States, to sell in interstate  
12          commerce any encryption, regardless of encryption algo-  
13          rithm selected, encryption key length chosen, or implemen-  
14          tation technique or medium used.

15          “(b) CONTROL OF EXPORTS BY SECRETARY OF COM-  
16          MERCE.—

17                 “(1) GENERAL RULE.—Notwithstanding any  
18                 other law, subject to paragraphs (2), (3), and (4),  
19                 the Secretary of Commerce shall have exclusive au-  
20                 thority to control exports of all computer hardware,  
21                 software, and technology for information security  
22                 (including encryption), except computer hardware,  
23                 software, and technology that is specifically designed  
24                 or modified for military use, including command,  
25                 control, and intelligence applications.

1           “(2) ITEMS NOT REQUIRING LICENSES.—No  
2           validated license may be required, except pursuant  
3           to the Trading With The Enemy Act or the Inter-  
4           national Emergency Economic Powers Act (IEEPA)  
5           (but only to the extent that the authority of the  
6           IEEPA is not exercised to extend controls imposed  
7           under the Export Administration Act of 1979), for  
8           the export or reexport of—

9                   “(A) any software, including software with  
10                  encryption capabilities, that is—

11                           “(i) generally available, as is, and de-  
12                           signed for installation by the purchaser; or

13                           “(ii) in the public domain or publicly  
14                           available because it is generally accessible  
15                           to the interested public in any form; or

16                   “(B) any computing device solely because  
17                  it incorporates or employs in any form software  
18                  (including software with encryption capabilities)  
19                  exempted from any requirement for a validated  
20                  license under subparagraph (A).

21           “(3) SOFTWARE WITH ENCRYPTION CAPABILI-  
22           TIES.—The Secretary of Commerce shall authorize  
23           the export or reexport of software with encryption  
24           capabilities for nonmilitary end-uses in any country  
25           to which exports of software of similar capability are

1 permitted for use by financial institutions not con-  
2 trolled in fact by United States persons, unless there  
3 is substantial evidence that such software will be—

4 “(A) diverted to a military end-use or an  
5 end-use supporting international terrorism;

6 “(B) modified for military or terrorist end-  
7 use; or

8 “(C) reexported without requisite United  
9 States authorization.

10 “(4) **HARDWARE WITH ENCRYPTION CAPABILI-**  
11 **TIES.**—The Secretary shall authorize the export or  
12 reexport of computer hardware with encryption ca-  
13 pabilities if the Secretary determines that a product  
14 offering comparable security is commercially avail-  
15 able from a foreign supplier without effective restric-  
16 tions outside the United States.

17 “(5) **DEFINITIONS.**—As used in this sub-  
18 section—

19 “(A) the term ‘generally available’ means,  
20 in the case of software (including software with  
21 encryption capabilities), software that is widely  
22 offered for sale, license, or transfer including,  
23 but not limited to, over-the-counter retail sales,  
24 mail order transactions, phone order trans-

1 actions, electronic distribution, or sale on ap-  
2 proval;

3 “(B) the term ‘as is’ means, in the case of  
4 software (including software with encryption ca-  
5 pabilities), a software program that is not de-  
6 signed, developed, or tailored by the software  
7 company for specific purchasers, except that  
8 such purchasers may supply certain installation  
9 parameters needed by the software program to  
10 function properly with the purchaser’s system  
11 and may customize the software program by  
12 choosing among options contained in the soft-  
13 ware program;

14 “(C) the term ‘is designed for installation  
15 by the purchaser’ means, in the case of soft-  
16 ware (including software with encryption capa-  
17 bilities)—

18 “(i) the software company intends for  
19 the purchaser (including any licensee or  
20 transferee), who may not be the actual  
21 program user, to install the software pro-  
22 gram on a computing device and has sup-  
23 plied the necessary instructions to do so,  
24 except that the company may also provide  
25 telephone help-line services for software in-

1           stallation, electronic transmission, or basic  
2           operations; and

3           “(ii) that the software program is de-  
4           signed for installation by the purchaser  
5           without further substantial support by the  
6           supplier;

7           “(D) the term ‘computing device’ means a  
8           device which incorporates one or more  
9           microprocessor-based central processing units  
10          that can accept, store, process, or provide out-  
11          put of data; and

12          “(E) the term ‘computer hardware’, when  
13          used in conjunction with information security,  
14          includes, but is not limited to, computer sys-  
15          tems, equipment, application-specific assem-  
16          blies, modules, and integrated circuits.”.

17          (b) TECHNICAL AMENDMENT.—The table of chapters  
18          for part I of title 18, United States Code, is amended by  
19          inserting after the item relating to chapter 33, the follow-  
20          ing new item:

**“122. Encrypted wire and electronic communications ..... 2801”.**

21          **SEC. 6. INTELLIGENCE ACTIVITIES.**

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

1           (b) CERTAIN CONDUCT.—Nothing in this Act or the  
2 amendments made by this Act shall affect the conduct,  
3 by officers or employees of the United States Government  
4 in accordance with other applicable Federal law, under  
5 procedures approved by the Attorney General, or activities  
6 intended to—

7           (1) intercept encrypted or other official commu-  
8 nications of United States executive branch entities  
9 or United States Government contractors for com-  
10 munications security purposes;

11           (2) intercept radio communications transmitted  
12 between or among foreign powers or agents of a for-  
13 eign power as defined by the Foreign Intelligence  
14 Surveillance Act of 1978; or

15           (3) access an electronic communication system  
16 used exclusively by a foreign power or agent of a for-  
17 eign power as defined by the Foreign Intelligence  
18 Surveillance Act of 1978.

○

S 1587 IS—2