

106TH CONGRESS
1ST SESSION

S. 854

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

IN THE SENATE OF THE UNITED STATES

APRIL 21, 1999

Mr. LEAHY 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 location information, decryption assistance for encrypted communications and stored electronic information, and other private information, to affirm the rights of Americans to use and sell encryption products as a tool for protecting their online privacy, 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 “Electronic Rights for the 21st Century Act”.

4 (b) TABLE OF CONTENTS.—The table of contents for
5 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. Enhanced privacy protection for information on computer networks.
- Sec. 102. Government access to location information.
- Sec. 103. Enhanced privacy protection for transactional information obtained from pen registers and trap and trace devices.
- Sec. 104. Privacy protection for conference calls.
- Sec. 105. Enhanced privacy protection for packet networks, including the Internet.
- Sec. 106. Privacy safeguards for information collected by Internet registrars.
- Sec. 107. Reports concerning governmental access to electronic communications.
- Sec. 108. Roving wiretaps.
- Sec. 109. Authority to provide customer location information for emergency purposes.
- Sec. 110. Confidentiality of subscriber information.

TITLE II—PROMOTING USE OF ENCRYPTION

- Sec. 201. Freedom to use encryption.
- Sec. 202. Purchase and use of encryption products by the Federal Government.
- Sec. 203. Law enforcement decryption assistance.

TITLE III—PRIVACY PROTECTION FOR LIBRARY LOAN AND BOOK
SALE RECORDS

- Sec. 301. Wrongful disclosure of library loan and book sale records.

TITLE IV—PRIVACY PROTECTION FOR SATELLITE HOME
VIEWERS

- Sec. 401. Privacy protection for subscribers of satellite television services for private home viewing.

6 **SEC. 2. PURPOSES.**

7 The purposes of this Act are—

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

10 (2) to encourage Americans to develop and de-
11 ploy encryption technology and to promote the use
12 of encryption by Americans to protect the security,
13 confidentiality, and privacy of their lawful wire and
14 electronic communications and stored electronic in-
15 formation; and

16 (3) to establish privacy standards and proce-
17 dures by which investigative or law enforcement offi-
18 cers and foreign governments may obtain decryption
19 assistance for encrypted communications and stored
20 electronic information.

21 **SEC. 3. FINDINGS.**

22 Congress finds that—

23 (1) the digitization of information and the ex-
24 plosion in the growth of computing and electronic
25 networking offers tremendous potential benefits to

1 the way Americans live, work, and are entertained,
2 but also raises new threats to the privacy of the
3 American people and the competitiveness of Amer-
4 ican businesses;

5 (2) a secure, private, and trusted national and
6 global information infrastructure is essential to pro-
7 mote economic growth, protect privacy, and meet the
8 needs of the American people and businesses;

9 (3) the rights of Americans to the privacy and
10 security of their communications and in the con-
11 ducting of personal and business affairs should be
12 promoted and protected;

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

19 (5) individuals will not entrust their sensitive
20 personal, medical, financial, and other information
21 to computers and computer networks unless the se-
22 curity and privacy of that information is assured;

23 (6) businesses will not entrust their proprietary
24 and sensitive corporate information, including infor-
25 mation about products, processes, customers, fi-

1 nances, and employees, to computers and computer
2 networks unless the security and privacy of that in-
3 formation is assured;

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

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

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

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

1 (11) government mandates for, or otherwise
2 compelled use of, third-party key recovery systems or
3 other systems that provide surreptitious access to
4 encrypted data threatens the security and privacy of
5 information systems;

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

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

15 (14) the Constitution of the United States per-
16 mits lawful electronic surveillance and the use of
17 other investigative tools by law enforcement officers
18 and the seizure of stored electronic information only
19 upon compliance with stringent standards and proce-
20 dures designed to protect the right to privacy and
21 other rights protected under the fourth amendment
22 of the Constitution of the United States;

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

1 enforcement 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 (16) Americans are increasingly shopping online
10 and purchasing books from online vendors, and ex-
11 pect that their choices of reading or viewing mate-
12 rials will be kept confidential;

13 (17) protecting the confidentiality and privacy
14 of the books, other written materials, and movies
15 that a person chooses to read or view should be pro-
16 tected to ensure the free exercise of first amendment
17 rights regardless of medium;

18 (18) generally, under current law, telecommuni-
19 cations carriers may not disclose individually identi-
20 fiable customer proprietary network information
21 without their customers' approval, while providers of
22 electronic communications services and remote com-
23 puting services may make such disclosure to anyone
24 other than a governmental entity and have no legal

1 obligation to notify their subscribers when they do
2 so;

3 (19) subscribers of Internet services through fa-
4 cilities of cable operators must be given notice and
5 an opportunity to prohibit disclosure before the cable
6 operator may disclose any personally identifiable in-
7 formation, including name or address, about a sub-
8 scriber to any other person, while providers of elec-
9 tronic communications services and remote com-
10 puting services have no similar legal obligation to
11 protect the privacy of their subscribers; and

12 (20) given the convergence among wireless, wire
13 line, cable, broadcast, and satellite services, privacy
14 safeguards should be applied more uniformly across
15 different media in order to provide a level competi-
16 tive playing field and consistent privacy protections.

17 **SEC. 4. DEFINITIONS.**

18 In this Act:

19 (1) **AGENCY.**—The term “agency”, in the case
20 of the United States Government, has the meaning
21 given the term in section 6 of title 18, United States
22 Code, and includes the United States Postal Service.

23 (2) **ENCRYPT; 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 (3) ENCRYPTION PRODUCT.—The term
8 “encryption product” means a computing device,
9 computer hardware, computer software, or tech-
10 nology with encryption capabilities.

11 (4) KEY.—The term “key” means the variable
12 information used in or produced by a mathematical
13 formula, code, or algorithm, or any component
14 thereof, used to encrypt or decrypt wire communica-
15 tions, electronic communications, or electronically
16 stored information.

17 (5) PERSON.—The term “person” has the
18 meaning given the term in section 2510(6) of title
19 18, United States Code.

20 (6) STATE.—The term “State” includes a State
21 of the United States, the District of Columbia, and
22 any commonwealth, territory, or possession of the
23 United States.

24 (7) UNITED STATES PERSON.—The term
25 “United States person” means any—

- 1 (A) national of the United States; or
 2 (B) legal entity that—
 3 (i) is organized under the laws of the
 4 United States or any State; and
 5 (ii) has its principal place of business
 6 in the United States.

7 **TITLE I—PRIVACY PROTECTION**
 8 **FOR COMMUNICATIONS AND**
 9 **ELECTRONIC INFORMATION**

10 **SEC. 101. ENHANCED PRIVACY PROTECTION FOR INFORMA-**
 11 **TION ON COMPUTER NETWORKS.**

12 Section 2703(b) of title 18, United States Code, is
 13 amended by striking paragraph (1) and inserting the fol-
 14 lowing new paragraph (1):

15 “(1) IN GENERAL.—A governmental entity may
 16 require a provider of remote computing service to
 17 disclose the contents of any electronic communica-
 18 tion to which this paragraph is made applicable by
 19 paragraph (2)—

20 “(A) pursuant to a warrant issued under
 21 the Federal Rules of Criminal Procedure or
 22 equivalent State warrant, a copy of which war-
 23 rant shall be served on the subscriber or cus-
 24 tomer of such remote computing service before

1 or at the same time the warrant is served on
2 the provider of the remote computing service; or

3 “(B) pursuant to a Federal or State grand
4 jury or trial subpoena, a copy of which sub-
5 poena shall be served on the subscriber or cus-
6 tomer of such remote computing service under
7 circumstances allowing the subscriber or cus-
8 tomer a meaningful opportunity to challenge
9 the subpoena.”.

10 (b) CONFORMING AMENDMENTS.—Paragraph (2) of
11 that section is amended—

12 (1) by indenting the paragraph 2 ems;

13 (2) by inserting “APPLICABILITY.—” after
14 “(2)”; and

15 (3) by indenting subparagraphs (A) and (B) 4
16 ems.

17 **SEC. 102. GOVERNMENT ACCESS TO LOCATION INFORMA-**
18 **TION.**

19 (a) COURT ORDER REQUIRED.—Section 2703 of title
20 18, United States Code, is amended by adding at the end
21 the following:

22 “(g) DISCLOSURE OF LOCATION INFORMATION TO
23 GOVERNMENTAL ENTITIES.—

24 “(1) DISCLOSURE UPON COURT ORDER.—A
25 provider of mobile electronic communication service

1 shall provide to a governmental entity information
 2 generated by and disclosing the current physical lo-
 3 cation of a subscriber’s equipment only if the gov-
 4 ernmental entity obtains a court order issued upon
 5 a finding that there is probable cause to believe that
 6 the equipment has been used, is being used, or is
 7 about to be used to commit a felony offense.

8 “(2) DISCLOSURE UPON SUBSCRIBER OR USER
 9 CONSENT.—A provider of mobile electronic commu-
 10 nication service may provide to a governmental enti-
 11 ty information described in paragraph (1) with the
 12 consent of the subscriber or the user of the equip-
 13 ment concerned.”.

14 (b) CONFORMING AMENDMENT.—Subsection
 15 (c)(1)(B) of that section is amended by striking “(b) of
 16 this section” and inserting “(b), or wireless location infor-
 17 mation covered by subsection (g)”.

18 **SEC. 103. ENHANCED PRIVACY PROTECTION FOR TRANS-**
 19 **ACTIONAL INFORMATION OBTAINED FROM**
 20 **PEN REGISTERS AND TRAP AND TRACE DE-**
 21 **VICES.**

22 Section 3123(a) of title 18, United States Code, is
 23 amended to read as follows:

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

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

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

16 **SEC. 104. PRIVACY PROTECTION FOR CONFERENCE CALLS.**

17 Section 2518 of title 18, United States Code, is
18 amended by adding at the end the following:

19 “(13) The interception of wire or electronic commu-
20 nications pursuant to an order under this section must
21 be terminated when the facility identified in the order au-
22 thorizing such interception is no longer being used, unless
23 the judge determines on the basis of facts submitted by
24 the applicant that there is probable cause to believe that
25 an individual continuing as a party to the communication

1 is committing, has committed, or is about to commit a
 2 particular offense enumerated in the order and there is
 3 probable cause to believe that particular communications
 4 concerning that offense will be obtained through such con-
 5 tinuing interception.”.

6 **SEC. 105. ENHANCED PRIVACY PROTECTION FOR PACKET**
 7 **NETWORKS, INCLUDING THE INTERNET.**

8 Section 3121(c) of title 18, United States Code, is
 9 amended by striking “other impulses” and all that follows
 10 and inserting “other impulses—

11 “(1) to the dialing and signaling information
 12 utilized in call processing; or

13 “(2) in the case of a packet-switched network,
 14 to the addressing information.”.

15 **SEC. 106. PRIVACY SAFEGUARDS FOR INFORMATION COL-**
 16 **LECTED BY INTERNET REGISTRARS.**

17 (a) IN GENERAL.—Section 2703 of title 18, United
 18 States Code, as amended by section 102(a) of this Act,
 19 is further amended by adding at the end the following:

20 “(h) RECORDS CONCERNING DOMAIN NAME REG-
 21 ISTRATION SERVICE.—A provider of domain name reg-
 22 istration service may disclose a record or other informa-
 23 tion pertaining to a subscriber or customer of such
 24 service—

25 “(1) to any person—

1 “(A) if the provider has provided the sub-
2 scriber or customer, in a clear and conspicuous
3 manner, the opportunity to prohibit such disclo-
4 sure;

5 “(B) in the case of information that identi-
6 fies the service provider hosting the website of
7 the subscriber or customer; or

8 “(C) to the extent such disclosure is nec-
9 essary incident to the provision of such service
10 or for the protection of the rights or property
11 of the provider of such service; or

12 “(2) without notice or consent of the subscriber
13 or customer in response to a subpoena or warrant
14 authorized by a Federal or State statute.”.

15 (b) DOMAIN NAME REGISTRATION SERVICE DE-
16 FINED.—Section 2711 of such title is amended—

17 (1) in paragraph (1), by striking “and” at the
18 end;

19 (2) in paragraph (2), by striking the period at
20 the end and inserting “; and”; and

21 (3) by adding at the end the following:

22 “(3) the term ‘domain name registration serv-
23 ice’ means a service to the public for the assignment
24 and management of domain names and Internet
25 Protocol addresses.”.

1 **SEC. 107. REPORTS CONCERNING GOVERNMENTAL ACCESS**
2 **TO ELECTRONIC COMMUNICATIONS.**

3 Section 2703 of title 18, United States Code, as
4 amended by section 106(a) of this Act, is further amended
5 by adding at the end the following:

6 “(i) **REPORTS.**—In April each year, the Attorney
7 General shall transmit to Congress a full and complete re-
8 port on—

9 “(1) the number and kind of warrants, orders,
10 and subpoenas applied for by law enforcement agen-
11 cies of the Department of Justice under this section;

12 “(2) the number of such applications granted or
13 denied; and

14 “(3) with respect to each warrant, order, or
15 subpoena issued under this section—

16 “(A) the number and type of communica-
17 tions disclosed;

18 “(B) the approximate number and fre-
19 quency of incriminating communications dis-
20 closed;

21 “(C) the offense specified in the applica-
22 tion; and

23 “(D) the approximate number of persons
24 whose communications were intercepted.”.

1 **SEC. 108. ROVING WIRETAPS.**

2 (a) SCOPE OF WIRETAPS.—Subsection (11)(b) of sec-
3 tion 2518 of title 18, United States Code, is amended by
4 striking clauses (ii) through (iv) and inserting the fol-
5 lowing new clauses:

6 “(ii) the application identifies the person
7 believed to be committing the offense and whose
8 communications are to be intercepted and the
9 applicant makes a showing that—

10 “(I) the person changes facilities in a
11 way that has the effect of thwarting inter-
12 ception from a specified facility; or

13 “(II) the person intends to thwart
14 interception by changing facilities; and

15 “(iii) the judge finds that such showing
16 has been adequately made.”.

17 (b) LIMITATION.—Subsection (12) of that section is
18 amended—

19 (1) by inserting “(a)” after “(12)”; and

20 (2) by adding at the end the following:

21 “(b) Each order and extension thereof to which the
22 requirements of subsections (1)(b)(ii) and (3)(D) of this
23 section do not apply by reason of subsection (11) of this
24 section shall provide that the authorization to intercept
25 only applies to communications to which the person be-

1 lieved to be committing the offense and named in the order
2 is a party.”.

3 **SEC. 109. AUTHORITY TO PROVIDE CUSTOMER LOCATION**
4 **INFORMATION FOR EMERGENCY PURPOSES.**

5 (a) USE OF CALL LOCATION AND CRASH NOTIFICA-
6 TION INFORMATION.—Subsection (d) of section 222 of the
7 Communications Act of 1934 (47 U.S.C. 222) is
8 amended—

9 (1) by striking “or” at the end of paragraph
10 (2);

11 (2) by striking the period at the end of para-
12 graph (3) and inserting a semicolon; and

13 (3) by adding at the end the following new
14 paragraphs:

15 “(4) to provide call location information con-
16 cerning the user of a commercial mobile service (as
17 such term is defined in section 332(d))—

18 “(A) to a public safety answering point,
19 emergency medical service provider or emer-
20 gency dispatch provider, public safety official,
21 fire service official, law enforcement official,
22 hospital emergency facility, or trauma care fa-
23 cility in order to respond to the user’s call for
24 emergency services;

1 “(B) to inform the user’s legal guardian or
2 members of the user’s immediate family of the
3 user’s location in an emergency situation that
4 involves the risk of death or serious physical
5 harm; or

6 “(C) to providers of information or data-
7 base management services solely for purposes of
8 assisting in the delivery of emergency services
9 in response to an emergency; or

10 “(5) to transmit automatic crash notification
11 information as part of the operation of an automatic
12 crash notification system.”.

13 (b) CUSTOMER APPROVAL OF USE OF CALL LOCA-
14 TION AND CRASH NOTIFICATION INFORMATION.—That
15 section is further amended—

16 (1) by redesignating subsection (f) as sub-
17 section (h); and

18 (2) by inserting after subsection (e) the fol-
19 lowing new subsection (f):

20 “(f) CUSTOMER APPROVAL OF USE OF CALL LOCA-
21 TION INFORMATION AND CRASH NOTIFICATION INFORMA-
22 TION.—For purposes of subsection (e)(1), without the ex-
23 press prior authorization of the customer, a customer shall
24 not be considered to have approved the use or disclosure
25 of or access to—

1 “(1) call location information concerning the
2 user of a commercial mobile service (as such term is
3 defined in section 332(d)), other than in accordance
4 with subsection (d)(4); or

5 “(2) automatic crash notification information to
6 any person other than for use in the operation of an
7 automatic crash notification system.”.

8 (c) USE OF LISTED AND UNLISTED SUBSCRIBER IN-
9 FORMATION FOR EMERGENCY SERVICES.—That section is
10 further amended by inserting after subsection (f), as
11 amended by subsection (b) of this section, the following
12 new subsection (g):

13 “(g) SUBSCRIBER LISTED AND UNLISTED INFORMA-
14 TION FOR EMERGENCY SERVICES.—Notwithstanding sub-
15 sections (b), (c), and (d), a telecommunications carrier
16 that provides telephone exchange service shall provide in-
17 formation described in subsection (h)(3)(A) (including in-
18 formation pertaining to subscribers whose information is
19 unlisted or unpublished) that is in its possession or control
20 (including information pertaining to subscribers of other
21 carriers) on a timely and unbundled basis, under non-
22 discriminatory and reasonable rates, terms, and conditions
23 to providers of emergency services, and providers of emer-
24 gency support services, solely for purposes of delivering
25 or assisting in the delivery of emergency services.”.

1 (d) DEFINITIONS.—Subsection (h) of that section, as
2 redesignated by subsection (b)(1) of this section, is
3 amended—

4 (1) in paragraph (1)(A), by inserting “loca-
5 tion,” after “destination,”; and

6 (2) by adding at the end the following:

7 “(4) PUBLIC SAFETY ANSWERING POINT.—The
8 term ‘public safety answering point’ means a facility
9 that has been designated to receive emergency calls
10 and route them to emergency service personnel.

11 “(5) EMERGENCY SERVICES.—The term ‘emer-
12 gency services’ means 911 emergency services and
13 emergency notification services.

14 “(6) EMERGENCY NOTIFICATION SERVICES.—
15 The term ‘emergency notification services’ means
16 services that notify the public of an emergency.

17 “(7) EMERGENCY SUPPORT SERVICES.—The
18 term ‘emergency support services’ means informa-
19 tion or data base management services used in sup-
20 port of emergency services.”.

21 **SEC. 110. CONFIDENTIALITY OF SUBSCRIBER INFORMA-**
22 **TION.**

23 Section 2703(c) of title 18, United States Code, is
24 amended—

1 (1) in paragraph (1)(A), by inserting before the
2 period at the end the following: “only if such disclo-
3 sure is—

4 “(i) necessary to initiate, render, bill, and col-
5 lect for such service;

6 “(ii) necessary to protect the rights or property
7 of the provider of such service;

8 “(iii) required by law;

9 “(iv) made at the request of the subscriber or
10 customer; or

11 “(v) if the provider has provided the subscriber
12 or customer, in a clear and conspicuous manner,
13 with the opportunity to prohibit such disclosure.”;
14 and

15 (2) by adding at the end the following:

16 “(3) Nothing in this subsection may be construed to
17 prohibit a provider of electronic communication service or
18 remote computing service from using, disclosing, or per-
19 mitting access to aggregate subscriber information from
20 which individual subscriber identities and characteristics
21 have been removed.”.

1 **TITLE II—PROMOTING USE OF**
2 **ENCRYPTION**

3 **SEC. 201. FREEDOM TO USE ENCRYPTION.**

4 (a) **NO DOMESTIC ENCRYPTION CONTROLS.**—It shall
5 be lawful for any person within the United States, and
6 for any United States person in a foreign country, to use,
7 develop, manufacture, sell, distribute, or import any
8 encryption product, regardless of the encryption algorithm
9 selected, encryption key length chosen, existence of key re-
10 covery or other plaintext access capability, or implementa-
11 tion or medium used.

12 (b) **PROHIBITION ON GOVERNMENT-COMPELLED**
13 **KEY ESCROW OR KEY RECOVERY.**—

14 (1) **IN GENERAL.**—Except as provided in para-
15 graph (3), no agency of the United States may re-
16 quire, compel, set standards for, condition any ap-
17 proval on, or condition the receipt of any benefit on,
18 a requirement that a decryption key, access to a
19 decryption key, key recovery information, or other
20 plaintext access capability be—

21 (A) required to be built into computer
22 hardware or software for any purpose;

23 (B) 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 (C) retained by the owner or user of an
2 encryption key or any other person, other than
3 for encryption products for the use of the Fed-
4 eral Government or a State government.

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

11 (3) EXCEPTIONS.—The prohibition in para-
12 graph (1) does not apply to—

13 (A) encryption used by an agency of the
14 United States, or the employees or agents of
15 such agency, solely for the internal operations
16 and telecommunications systems of the United
17 States Government; or

18 (B) the authority of any investigative or
19 law enforcement officer, or any member of the
20 intelligence community (as defined in section 3
21 of the National Security Act of 1947 (50
22 U.S.C. 401a)), acting under any law in effect
23 on the date of enactment of this Act, to gain
24 access to encrypted communications or informa-
25 tion.

1 (c) USE OF ENCRYPTION FOR AUTHENTICATION OR
 2 INTEGRITY PURPOSES.—No agency of the United States
 3 shall establish any condition, tie, or link between
 4 encryption products, standards, and services used for con-
 5 fidentiality purposes and those used for authentication, in-
 6 tegrity, or access control purposes.

7 **SEC. 202. PURCHASE AND USE OF ENCRYPTION PRODUCTS**
 8 **BY THE FEDERAL GOVERNMENT.**

9 To ensure that secure electronic access to the Federal
 10 Government is available to persons outside of and not op-
 11 erating under contract with agencies of the United States,
 12 the Federal Government may not purchase any encryption
 13 product with a key recovery or other plaintext access fea-
 14 ture if such key recovery or plaintext access feature would
 15 interfere with use of the full encryption capabilities of the
 16 product when interoperating with other commercial
 17 encryption products.

18 **SEC. 203. LAW ENFORCEMENT DECRYPTION ASSISTANCE.**

19 (a) IN GENERAL.—Part I of title 18, United States
 20 Code, is amended by adding at the end the following:

21 **“CHAPTER 124—ENCRYPTED WIRE OR**
 22 **ELECTRONIC COMMUNICATIONS AND**
 23 **STORED ELECTRONIC INFORMATION**

“Sec.

“2801. Definitions.

“2802. Access to decryption assistance for communications.

“2803. Access to decryption assistance for stored electronic communications or records.

“2804. Foreign government access to decryption assistance.

1 **“§ 2801. Definitions**

2 “In this chapter:

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

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

17 “(3) ENCRYPT; ENCRYPTION.—The terms
18 ‘encrypt’ and ‘encryption’ refer to the scrambling
19 (and descrambling) of wire communications, elec-
20 tronic communications, or electronically stored infor-
21 mation using mathematical formulas or algorithms
22 in order to preserve the confidentiality, integrity, or
23 authenticity of, and prevent unauthorized recipients

1 from accessing or altering, such communications or
2 information.

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

6 “(5) OFFICIAL REQUEST.—The term ‘official
7 request’ has the meaning given the term in section
8 3506(e).

9 “(6) INCORPORATED DEFINITIONS.—Any term
10 used in this chapter that is not defined in this chap-
11 ter and that is defined in section 2510, has the
12 meaning given the term in section 2510.

13 **“§ 2802. Access to decryption assistance for commu-
14 nications**

15 “(a) CRIMINAL INVESTIGATIONS.—

16 “(1) IN GENERAL.—An order authorizing the
17 interception of a wire or electronic communication
18 under section 2518 shall, upon request of the appli-
19 cant, direct that a provider of wire or electronic
20 communication service, or any other person pos-
21 sessed information capable of decrypting that com-
22 munication, other than a person whose communica-
23 tions are the subject of the interception, shall
24 promptly furnish the applicant with the necessary
25 decryption assistance, if the court finds that the

1 decryption assistance sought is necessary for the
2 decryption of a communication intercepted pursuant
3 to the order.

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

7 “(A) contain a provision that the
8 decryption assistance provided shall involve dis-
9 closure of a private decryption key only if no
10 other form of decryption assistance is available
11 and otherwise shall be limited to the minimum
12 necessary to decrypt the communications inter-
13 cepted pursuant to such order; and

14 “(B) terminate on the earlier of—

15 “(i) the date on which the authorized
16 objective is attained; or

17 “(ii) 30 days after the date on which
18 the order or extension, as applicable, is
19 issued.

20 “(3) NOTICE.—If decryption assistance is pro-
21 vided pursuant to an order under this subsection,
22 the court issuing the order shall cause to be served
23 on the person whose communications are the subject
24 of such decryption assistance, as part of the inven-
25 tory required to be served pursuant to section

1 2518(8), notice of the receipt of the decryption as-
2 sistance and a specific description of the decryption
3 keys or other decryption assistance disclosed.

4 “(b) FOREIGN INTELLIGENCE INVESTIGATIONS.—

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

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

22 “(A) contain a provision that the
23 decryption assistance provided shall be limited
24 to the minimum necessary to decrypt the com-

1 communications intercepted pursuant to such order;
2 and

3 “(B) terminate on the earlier of—

4 “(i) the date on which the authorized
5 objective is attained; or

6 “(ii) 30 days after the date on which
7 the order or extension, as applicable, is
8 issued.

9 “(c) GENERAL PROHIBITION ON DISCLOSURE.—

10 Other than pursuant to an order under subsection (a) or
11 (b), no person possessing information capable of
12 decrypting a wire or electronic communication of another
13 person shall disclose that information or provide
14 decryption assistance to an investigative or law enforce-
15 ment officer.

16 **“§ 2803. Access to decryption assistance for stored**
17 **electronic communications or records**

18 “(a) DECRYPTION ASSISTANCE.—No person may dis-
19 close a decryption key or provide decryption assistance
20 pertaining to the contents of stored electronic communica-
21 tions or records, including those disclosed pursuant to sec-
22 tion 2703, to a governmental entity, except—

23 “(1) pursuant to a warrant issued under the
24 Federal Rules of Criminal Procedure or an equiva-
25 lent State warrant, a copy of which warrant shall be

1 served on the person who created the electronic com-
2 munication or record before or at the same time
3 service is made on the keyholder;

4 “(2) pursuant to a subpoena, a copy of which
5 subpoena shall be served on the person who created
6 the electronic communication or record, under cir-
7 cumstances allowing the person meaningful oppor-
8 tunity to challenge the subpoena; or

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

11 “(b) DELAY OF NOTIFICATION.—In the case of com-
12 munications disclosed pursuant to section 2703(a), service
13 of the copy of the warrant or subpoena on the person who
14 created the electronic communication or record may be de-
15 layed for a period of not to exceed 90 days upon request
16 to the court by the governmental entity requiring the
17 decryption assistance, if the court determines that there
18 is reason to believe that notification of the existence of
19 the court order or subpoena may have an adverse result
20 described in section 2705(a)(2).

21 **“§ 2804. Foreign government access to decryption as-**
22 **sistance**

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

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

4 “(2) except as provided in subsection (b), pro-
5 vide decryption assistance to a foreign government
6 or to a law enforcement agency of a foreign govern-
7 ment.

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

10 “(1) APPLICATION FOR ORDER.—In any case in
11 which the United States has entered into a treaty or
12 convention with a foreign government to provide mu-
13 tual assistance with respect to providing decryption
14 assistance, the Attorney General (or the designee of
15 the Attorney General) may, upon an official request
16 to the United States from the foreign government,
17 apply for an order described in paragraph (2) from
18 the district court in which the person possessing in-
19 formation capable of decrypting the encrypted com-
20 munication or stored electronic information at issue
21 resides—

22 “(A) directing that person to release a
23 decryption key or provide decryption assistance
24 to the Attorney General (or the designee of the
25 Attorney General); and

1 “(B) authorizing the Attorney General (or
2 the designee of the Attorney General) to furnish
3 the foreign government with the plaintext of the
4 communication or information at issue.

5 “(2) CONTENTS OF ORDER.—An order de-
6 scribed in this paragraph is an order directing the
7 person possessing information capable of decrypting
8 the communication or information at issue to—

9 “(A) release a decryption key to the Attor-
10 ney General (or the designee of the Attorney
11 General) so that the plaintext of the commu-
12 nication or information may be furnished to the
13 foreign government; or

14 “(B) provide decryption assistance to the
15 Attorney General (or the designee of the Attor-
16 ney General) so that the plaintext of the com-
17 munication or information may be furnished to
18 the foreign government.

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

24 “(A) the decryption key or decryption as-
25 sistance sought is necessary for the decryption

1 of a communication or information that the for-
 2 eign government is authorized to intercept or
 3 seize pursuant to the law of the foreign country;

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

7 “(C) the decryption key or decryption as-
 8 sistance is being sought in connection with a
 9 criminal investigation for conduct that would
 10 constitute a violation of a criminal law of the
 11 United States if committed within the jurisdic-
 12 tion of the United States.”.

13 (b) CLERICAL AMENDMENT.—The analysis for part
 14 I of title 18, United States Code, is amended by adding
 15 at the end the following:

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

16 **TITLE III—PRIVACY PROTEC-**
 17 **TION FOR LIBRARY LOAN**
 18 **AND BOOK SALE RECORDS**

19 **SEC. 301. WRONGFUL DISCLOSURE OF LIBRARY LOAN AND**
 20 **BOOK SALE RECORDS.**

21 (a) IN GENERAL.—Section 2710 of title 18, United
 22 States Code, is amended—

23 (1) by redesignating subsections (c) through (f)
 24 as subsections (d) through (g), respectively; and

1 (2) by striking the section designation and all
2 that follows through the end of subsection (b) and
3 inserting the following:

4 **“§ 2710. Wrongful disclosure of video tape rental or**
5 **sale records and library loan and book**
6 **sale records**

7 “(a) DEFINITIONS.—In this section:

8 “(1) The term ‘book seller’ means any person,
9 engaged in the business, in or affecting interstate or
10 foreign commerce, of selling books, magazines, or
11 other printed material, or any person or other entity
12 to whom a disclosure is made under subparagraph
13 (D) or (E) of subsection (b)(2), but only with re-
14 spect to the information contained in the disclosure.

15 “(2) The term ‘consumer’ means any renter,
16 purchaser, or subscriber of goods or services from a
17 video tape service provider or book seller.

18 “(3) The term ‘library’ means an institution
19 that operates as a public library or serves as a li-
20 brary for any university, school, or college.

21 “(4) The term ‘ordinary course of business’
22 means only debt collection activities, order fulfill-
23 ment, request processing, and the transfer of owner-
24 ship.

1 “(5) The term ‘patron’ means any individual
2 who requests or receives—

3 “(A) services within a library; or

4 “(B) books or other materials on loan from
5 a library.

6 “(6) The term ‘personally identifiable informa-
7 tion’ includes the following:

8 “(A) Information that identifies a person
9 as having requested or obtained specific video
10 materials or services from a video tape service
11 provider.

12 “(B) Information that identifies a person
13 as having requested or obtained specific books,
14 magazines, or other printed material from a
15 book seller.

16 “(C) Information that identifies a person
17 as having requested or obtained any materials
18 or services from a library.

19 “(7) The term ‘video tape service provider’
20 means any person, engaged in the business, in or af-
21 fecting interstate or foreign commerce, of rental,
22 sale, or delivery of prerecorded video cassette tapes
23 or similar audio visual materials, or any person or
24 other entity to whom a disclosure is made under
25 subparagraph (D) or (E) of subsection (b)(2), but

1 only with respect to the information contained in the
2 disclosure.

3 “(b) VIDEO TAPE RENTAL AND SALE AND BOOK
4 SALE RECORDS.—

5 “(1) IN GENERAL.—A video tape service pro-
6 vider or book seller who knowingly discloses, to any
7 person, personally identifiable information con-
8 cerning any consumer of such provider or seller, as
9 the case may be, shall be liable to the aggrieved per-
10 son for the relief provided in subsection (d).

11 “(2) DISCLOSURE.—A video tape service pro-
12 vider or book seller may disclose personally identifi-
13 able information concerning any consumer—

14 “(A) to the consumer;

15 “(B) to any person with the informed,
16 written consent of the consumer given at the
17 time the disclosure is sought;

18 “(C) to a law enforcement agency pursuant
19 to a warrant issued under the Federal Rules of
20 Criminal Procedure, an equivalent State war-
21 rant, or a court order issued in accordance with
22 paragraph (4);

23 “(D) to any person if the disclosure is sole-
24 ly of the names and addresses of consumers
25 and if—

1 “(i) the video tape service provider or
2 book seller, as the case may be, has pro-
3 vided the consumer, in a clear and con-
4 spicuous manner, with the opportunity to
5 prohibit such disclosure; and

6 “(ii) the disclosure does not identify
7 the title, description, or subject matter of
8 any video tapes or other audio visual mate-
9 rial, or books, magazines, or other printed
10 material, except that the subject matter of
11 such materials may be disclosed if the dis-
12 closure is for the exclusive use of mar-
13 keting goods and services directly to the
14 consumer;

15 “(E) to any person if the disclosure is inci-
16 dent to the ordinary course of business of the
17 video tape service provider or book seller; or

18 “(F) pursuant to a court order, in a civil
19 proceeding upon a showing of compelling need
20 for the information that cannot be accommo-
21 dated by any other means, if—

22 “(i) the consumer is given reasonable
23 notice, by the person seeking the disclo-
24 sure, of the court proceeding relevant to
25 the issuance of the court order; and

1 “(ii) the consumer is afforded the op-
2 portunity to appear and contest the claim
3 of the person seeking the disclosure.

4 “(3) SAFEGUARDS.—If an order is granted pur-
5 suant to subparagraph (C) or (F) of paragraph (2),
6 the court shall impose appropriate safeguards
7 against unauthorized disclosure.

8 “(4) COURT ORDERS.—A court order author-
9 izing disclosure under paragraph (2)(C) shall issue
10 only with prior notice to the consumer and only if
11 the law enforcement agency shows that there is
12 probable cause to believe that a person has engaged,
13 is engaging, or is about to engage in criminal activ-
14 ity and that the records or other information sought
15 are material to the investigation of such activity. In
16 the case of a State government authority, such a
17 court order shall not issue if prohibited by the law
18 of such State. A court issuing an order pursuant to
19 this subsection, on a motion made promptly by the
20 video tape service provider or the book seller, may
21 quash or modify such order if the information or
22 records requested are unreasonably voluminous in
23 nature or if compliance with such order otherwise
24 would cause an unreasonable burden on such pro-
25 vider or seller, as the case may be.

1 “(c) LIBRARY RECORDS.—

2 “(1) IN GENERAL.—Any library that knowingly
3 discloses, to any person, personally identifiable infor-
4 mation concerning any patron of the library shall be
5 liable to the aggrieved person as provided in sub-
6 section (d).

7 “(2) DISCLOSURE.—A library may disclose per-
8 sonally identifiable information concerning any
9 patron—

10 “(A) to the patron;

11 “(B) to any person with the informed writ-
12 ten consent of the patron given at the time the
13 disclosure is sought;

14 “(C) to a law enforcement agency pursuant
15 to a warrant issued under the Federal Rules of
16 Criminal Procedure, an equivalent State war-
17 rant, or a court order issued in accordance with
18 paragraph (4);

19 “(D) to any person if the disclosure is sole-
20 ly of the names and addresses of patrons and
21 if—

22 “(i) the library has provided the pa-
23 tron with a written statement that affords
24 the patron the opportunity to prohibit such
25 disclosure; and

1 “(ii) the disclosure does not reveal, di-
2 rectly or indirectly, the title, description, or
3 subject matter of any library materials
4 borrowed or services utilized by the patron;

5 “(E) to any authorized person if the disclo-
6 sure is necessary for the retrieval of overdue li-
7 brary materials or the recoupment of compensa-
8 tion for damaged or lost library materials; or

9 “(F) pursuant to a court order, in a civil
10 proceeding upon a showing of compelling need
11 for the information that cannot be accommo-
12 dated by any other means, if—

13 “(i) the patron is given reasonable no-
14 tice, by the person seeking the disclosure,
15 of the court proceeding relevant to the
16 issuance of the court order; and

17 “(ii) the patron is afforded the oppor-
18 tunity to appear and contest the claim of
19 the person seeking the disclosure.

20 “(3) SAFEGUARDS.—If an order is granted pur-
21 suant to subparagraph (C) or (F) of paragraph (2),
22 the court shall impose appropriate safeguards
23 against unauthorized disclosure.

24 “(4) COURT ORDERS.—A court order author-
25 izing disclosure under paragraph (2)(C) shall issue

1 only with prior notice to the patron and only if the
2 law enforcement agency shows that there is probable
3 cause to believe that a person has engaged, is engag-
4 ing or is about to engage in criminal activity and
5 that the records or other information sought are ma-
6 terial to the investigation of such activity. In the
7 case of a State government authority, such a court
8 order shall not issue if prohibited by the law of such
9 State. A court issuing an order pursuant to this sub-
10 section, on a motion made promptly by the library,
11 may quash or modify such order if the information
12 or records requested are unreasonably voluminous in
13 nature or if compliance with such order otherwise
14 would cause an unreasonable burden on the li-
15 brary.”.

16 (b) CLERICAL AMENDMENT.—The item relating to
17 section 2701 in the analysis for chapter 121 of title 18,
18 United States Code, is amended to read as follows:

“2710. Wrongful disclosure of video tape rental or sale records and library loan
and book sale records.”.

1 **TITLE IV—PRIVACY PROTEC-**
2 **TION FOR SATELLITE HOME**
3 **VIEWERS**

4 **SEC. 401. PRIVACY PROTECTION FOR SUBSCRIBERS OF**
5 **SATELLITE TELEVISION SERVICES FOR PRI-**
6 **VATE HOME VIEWING.**

7 (a) IN GENERAL.—Section 631 of the Communica-
8 tions Act of 1934 (47 U.S.C. 551) is amended to read
9 as follows:

10 **“SEC. 631. PRIVACY OF SUBSCRIBER INFORMATION FOR**
11 **SUBSCRIBERS OF CABLE SERVICE AND SAT-**
12 **ELLITE TELEVISION SERVICE.**

13 “(a) NOTICE TO SUBSCRIBERS REGARDING PERSON-
14 ALLY IDENTIFIABLE INFORMATION.—At the time of en-
15 tering into an agreement to provide any cable service, sat-
16 ellite home viewing service, or other service to a sub-
17 scriber, and not less often than annually thereafter, a
18 cable operator, satellite carrier, or distributor shall provide
19 notice in the form of a separate, written statement to such
20 subscriber that clearly and conspicuously informs the sub-
21 scriber of—

22 “(1) the nature of personally identifiable infor-
23 mation collected or to be collected with respect to
24 the subscriber as a result of the provision of such

1 service and the nature of the use of such informa-
2 tion;

3 “(2) the nature, frequency, and purpose of any
4 disclosure that may be made of such information, in-
5 cluding an identification of the types of persons to
6 whom the disclosure may be made;

7 “(3) the period during which such information
8 will be maintained by the cable operator, satellite
9 carrier, or distributor;

10 “(4) the times and place at which the sub-
11 scriber may have access to such information in ac-
12 cordance with subsection (d); and

13 “(5) the limitations provided by this section
14 with respect to the collection and disclosure of infor-
15 mation by the cable operator, satellite carrier, or dis-
16 tributor and the right of the subscriber under this
17 section to enforce such limitations.

18 “(b) COLLECTION OF PERSONALLY IDENTIFIABLE
19 INFORMATION.—

20 “(1) IN GENERAL.—Except as provided in para-
21 graph (2), a cable operator, satellite carrier, or dis-
22 tributor shall not use its cable or satellite system to
23 collect personally identifiable information concerning
24 any subscriber without the prior written or electronic
25 consent of the subscriber.

1 “(2) EXCEPTION.—A cable operator, satellite
2 carrier, or distributor may use its cable or satellite
3 system to collect information described in paragraph
4 (1) in order to—

5 “(A) obtain information necessary to
6 render a cable or satellite service or other serv-
7 ice provided by the cable operator, satellite car-
8 rier, or distributor to the subscriber; or

9 “(B) detect unauthorized reception of cable
10 or satellite communications.

11 “(c) DISCLOSURE OF PERSONALLY IDENTIFIABLE
12 INFORMATION.—

13 “(1) IN GENERAL.—Except as provided in para-
14 graph (2), a cable operator, satellite carrier, or dis-
15 tributor may not disclose personally identifiable in-
16 formation concerning any subscriber without the
17 prior written or electronic consent of the subscriber
18 and shall take such actions as are necessary to pre-
19 vent unauthorized access to such information by a
20 person other than the subscriber or the cable oper-
21 ator, satellite carrier, or distributor.

22 “(2) EXCEPTIONS.—A cable operator, satellite
23 carrier, or distributor may disclose information de-
24 scribed in paragraph (1) if the disclosure is—

1 “(A) necessary to render, or conduct a le-
2 gitimate business activity related to, a cable or
3 satellite service or other service provided by the
4 cable operator, satellite carrier, or distributor to
5 the subscriber;

6 “(B) subject to paragraph (3), made pur-
7 suant to a court order authorizing such disclo-
8 sure, if the subscriber is notified of such order
9 by the person to whom the order is directed; or

10 “(C) a disclosure of the names and ad-
11 dresses of subscribers to any other provider of
12 cable or satellite service or other service, if—

13 “(i) the cable operator, satellite car-
14 rier, or distributor has provided the sub-
15 scriber the opportunity to prohibit or limit
16 such disclosure; and

17 “(ii) the disclosure does not reveal, di-
18 rectly or indirectly—

19 “(I) the extent of any viewing or
20 other use by the subscriber of a cable
21 or satellite service or other service
22 provided by the cable operator, sat-
23 ellite carrier, or distributor; or

24 “(II) the nature of any trans-
25 action made by the subscriber over

1 the cable or satellite system of the
2 cable operator, satellite carrier, or dis-
3 tributor.

4 “(3) COURT ORDERS.—A governmental entity
5 may obtain personally identifiable information con-
6 cerning a cable or satellite subscriber pursuant to a
7 court order only if, in the court proceeding relevant
8 to such court order—

9 “(A) such entity offers clear and con-
10 vincing evidence that the subject of the infor-
11 mation is reasonably suspected of engaging in
12 criminal activity and that the information
13 sought would be material evidence in the case;
14 and

15 “(B) the subject of the information is af-
16 forded the opportunity to appear and contest
17 such entity’s claim.

18 “(d) SUBSCRIBER ACCESS TO INFORMATION.—A
19 cable or satellite subscriber shall be provided access to all
20 personally identifiable information regarding that sub-
21 scriber that is collected and maintained by a cable oper-
22 ator, satellite carrier, or distributor. Such information
23 shall be made available to the subscriber at reasonable
24 times and at a convenient place designated by such cable
25 operator, satellite carrier, or distributor. A cable or sat-

1 elite subscriber shall be provided reasonable opportunity
2 to correct any error in such information.

3 “(e) DESTRUCTION OF INFORMATION.—A cable oper-
4 ator, satellite carrier, or distributor shall destroy person-
5 ally identifiable information if the information is no longer
6 necessary for the purpose for which it was collected and
7 there are no pending requests or orders for access to such
8 information under subsection (d) or pursuant to a court
9 order.

10 “(f) RELIEF.—

11 “(1) IN GENERAL.—Any person aggrieved by
12 any act of a cable operator, satellite carrier, or dis-
13 tributor in violation of this section may bring a civil
14 action in a district court of the United States.

15 “(2) DAMAGES AND COSTS.—In any action
16 brought under paragraph (1), the court may award
17 a prevailing plaintiff—

18 “(A) actual damages but not less than liq-
19 uidated damages computed at the rate of \$100
20 a day for each day of violation or \$1,000,
21 whichever is greater;

22 “(B) punitive damages; and

23 “(C) reasonable attorneys’ fees and other
24 litigation costs reasonably incurred.

1 “(3) NO EFFECT ON OTHER REMEDIES.—The
2 remedy provided by this subsection shall be in addi-
3 tion to any other remedy available under any provi-
4 sion of law to a cable or satellite subscriber.

5 “(g) DEFINITIONS.—In this section:

6 “(1) DISTRIBUTOR.—The term ‘distributor’ has
7 the meaning given that term in section 119(d)(1) of
8 title 17, United States Code.

9 “(2) CABLE OPERATOR.—

10 “(A) IN GENERAL.—The term ‘cable oper-
11 ator’ has the meaning given that term in sec-
12 tion 602.

13 “(B) INCLUSION.—The term includes any
14 person who—

15 “(i) is owned or controlled by, or
16 under common ownership or control with,
17 a cable operator; and

18 “(ii) provides any wire or radio com-
19 munications service.

20 “(3) OTHER SERVICE.—The term ‘other serv-
21 ice’ includes any wire, electronic, or radio commu-
22 nications service provided using any of the facilities
23 of a cable operator, satellite carrier, or distributor
24 that are used in the provision of cable service or sat-
25 ellite home viewing service.

1 “(4) PERSONALLY IDENTIFIABLE INFORMA-
2 TION.—The term ‘personally identifiable informa-
3 tion’ does not include any record of aggregate data
4 that does not identify particular persons.

5 “(5) SATELLITE CARRIER.—The term ‘satellite
6 carrier’ has the meaning given that term in section
7 119(d)(6) of title 17, United States Code.”.

8 (b) NOTICE WITH RESPECT TO CERTAIN AGREE-
9 MENTS.—

10 (1) IN GENERAL.—Except as provided in para-
11 graph (2), a cable operator, satellite carrier, or dis-
12 tributor who has entered into agreements referred to
13 in section 631(a) of the Communications Act of
14 1934, as amended by subsection (a), before the date
15 of enactment of this Act, shall provide any notice re-
16 quired under that section, as so amended, to sub-
17 scribers under such agreements not later than 180
18 days after that date.

19 (2) EXCEPTION.—Paragraph (1) shall not
20 apply with respect to any agreement under which a
21 cable operator, satellite carrier, or distributor was
22 providing notice under section 631(a) of the Com-
23 munications Act of 1934, as in effect on the day be-

1 fore the date of enactment of this Act, as of such
2 date.

○