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.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the ''Electronic Rights for the 21st Century Act''.

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

SEC. 2. PURPOSES.

The purposes of this Act are—

(1) to promote the privacy and constitutional rights of individuals and organizations in networked computer systems and other digital environments, protect the confidentiality of information and security of critical infrastructure systems relied on by individuals, businesses and government agencies, and properly balance the needs of law enforcement to have the access to electronic communications and information in appropriate circumstances;

(2) to encourage Americans to develop and deploy encryption technology and to promote the use of encryption by Americans to protect the security, confidentiality, and privacy of their lawful wire and electronic communications and stored electronic information; and

(3) to establish privacy standards and procedures by which investigative or law enforcement officers and foreign governments may obtain decryption assistance for encrypted communications and stored electronic information.

SEC. 3. FINDINGS.

Congress finds that—

(1) the digitization of information and the explosion in the growth of computing and electronic networking offers tremendous potential benefits to

the way Americans live, work, and are entertained, but also raises new threats to the privacy of the American people and the competitiveness of American businesses;

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

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

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

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

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

nances, and employees, to computers and computer networks unless the security and privacy of that information is assured;

(7) America's critical infrastructures, including its telecommunications system, banking and financial infrastructure, and power and transportation infrastructure, increasingly rely on vulnerable information systems, and will represent a growing risk to national security and public safety unless the security and privacy of those information systems is assured;

(8) encryption technology is an essential tool to promote and protect the privacy, security, confidentiality, integrity, and authenticity of wire and electronic communications and stored electronic information;

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

(10) Americans should be free to use lawfully whatever particular encryption techniques, technologies, programs, or products developed in the marketplace that best suits their needs in order to interact electronically with the government and others worldwide in a secure, private, and confidential manner;

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

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

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

(14) the Constitution of the United States permits lawful electronic surveillance and the use of other investigative tools by law enforcement officers and the seizure of stored electronic information only upon compliance with stringent standards and procedures designed to protect the right to privacy and other rights protected under the fourth amendment of the Constitution of the United States;

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

forcement officers obtain decryption assistance from persons—

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

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

(16) Americans are increasingly shopping online and purchasing books from online vendors, and expect that their choices of reading or viewing materials will be kept confidential;

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

(18) generally, under current law, telecommunications carriers may not disclose individually identifiable customer proprietary network information without their customers' approval, while providers of electronic communications services and remote computing services may make such disclosure to anyone other than a governmental entity and have no legal

obligation to notify their subscribers when they do so;

(19) subscribers of Internet services through facilities of cable operators must be given notice and an opportunity to prohibit disclosure before the cable operator may disclose any personally identifiable information, including name or address, about a subscriber to any other person, while providers of electronic communications services and remote computing services have no similar legal obligation to protect the privacy of their subscribers; and

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

SEC. 4. DEFINITIONS.

In this Act:

(1) AGENCY.—The term ''agency'', in the case of the United States Government, has the meaning given the term in section 6 of title 18, United States Code, and includes the United States Postal Service.

(2) ENCRYPT; ENCRYPTION.—The terms ''encrypt'' and ''encryption'' refer to the scrambling (and descrambling) of wire communications, elec-

tronic communications, or electronically stored information using mathematical formulas or algorithms in order to preserve the confidentiality, integrity, or authenticity of, and prevent unauthorized recipients from accessing or altering, such communications or information.

(3) ENCRYPTION PRODUCT.—The term ''encryption product'' means a computing device, computer hardware, computer software, or technology with encryption capabilities.

(4) KEY.—The term ''key'' means the variable information used in or produced by a mathematical formula, code, or algorithm, or any component thereof, used to encrypt or decrypt wire communications, electronic communications, or electronically stored information.

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

(6) STATE.—The term ''State'' includes a State of the United States, the District of Columbia, and any commonwealth, territory, or possession of the United States.

(7) UNITED STATES PERSON.—The term ''United States person'' means any—

(A) national of the United States; or

(B) legal entity that—

(i) is organized under the laws of the United States or any State; and

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

TITLE I—PRIVACY PROTECTION FOR COMMUNICATIONS AND ELECTRONIC INFORMATION

SEC. 101. ENHANCED PRIVACY PROTECTION FOR INFORMATION ON COMPUTER NETWORKS.

Section 2703(b) of title 18, United States Code, is amended by striking paragraph (1) and inserting the following new paragraph (1):

''(1) IN GENERAL.—A governmental entity may require a provider of remote computing service to disclose the contents of any electronic communication to which this paragraph is made applicable by paragraph (2)—

''(A) pursuant to a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant, a copy of which warrant shall be served on the subscriber or customer of such remote computing service before

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

''(B) pursuant to a Federal or State grand jury or trial subpoena, a copy of which subpoena shall be served on the subscriber or customer of such remote computing service under circumstances allowing the subscriber or customer a meaningful opportunity to challenge the subpoena.''.

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

(1) by indenting the paragraph 2 ems;

(2) by inserting ''APPLICABILITY.—'' after ''(2)''; and

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

SEC. 102. GOVERNMENT ACCESS TO LOCATION INFORMATION.

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

''(g) DISCLOSURE OF LOCATION INFORMATION TO GOVERNMENTAL ENTITIES.—

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

shall provide to a governmental entity information generated by and disclosing the current physical location of a subscriber's equipment only if the governmental entity obtains a court order issued upon a finding that there is probable cause to believe that the equipment has been used, is being used, or is about to be used to commit a felony offense.

''(2) DISCLOSURE UPON SUBSCRIBER OR USER CONSENT.—A provider of mobile electronic communication service may provide to a governmental entity information described in paragraph (1) with the consent of the subscriber or the user of the equipment concerned.''.

(b) CONFORMING AMENDMENT.—Subsection (c)(1)(B) of that section is amended by striking ''(b) of this section'' and inserting ''(b), or wireless location information covered by subsection (g)''.

SEC. 103. ENHANCED PRIVACY PROTECTION FOR TRANSACTIONAL INFORMATION OBTAINED FROM PEN REGISTERS AND TRAP AND TRACE DEVICES.

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

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

''(1) authorizing the installation and use of a pen register or a trap and trace device within the jurisdiction of the court if the court finds, based on the certification by the attorney for the government or the State law enforcement or investigative officer, that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation; and

''(2) directing that the use of the pen register or trap and trace device be conducted in such a way as to minimize the recording or decoding of any electronic or other impulses that are not related to the dialing and signaling information utilized in call processing by the service provider upon whom the order is served.''.

SEC. 104. PRIVACY PROTECTION FOR CONFERENCE CALLS.

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

''(13) The interception of wire or electronic communications pursuant to an order under this section must be terminated when the facility identified in the order authorizing such interception is no longer being used, unless the judge determines on the basis of facts submitted by the applicant that there is probable cause to believe that an individual continuing as a party to the communication

is committing, has committed, or is about to commit a particular offense enumerated in the order and there is probable cause to believe that particular communications concerning that offense will be obtained through such continuing interception.''.

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

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

''(1) to the dialing and signaling information utilized in call processing; or

''(2) in the case of a packet-switched network, to the addressing information.''.

SEC. 106. PRIVACY SAFEGUARDS FOR INFORMATION COLLECTED BY INTERNET REGISTRARS.

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

''(h) RECORDS CONCERNING DOMAIN NAME REGISTRATION SERVICE.—A provider of domain name registration service may disclose a record or other information pertaining to a subscriber or customer of such service—

''(1) to any person—

''(A) if the provider has provided the subscriber or customer, in a clear and conspicuous manner, the opportunity to prohibit such disclosure;

''(B) in the case of information that identifies the service provider hosting the website of the subscriber or customer; or

''(C) to the extent such disclosure is necessary incident to the provision of such service or for the protection of the rights or property of the provider of such service; or

''(2) without notice or consent of the subscriber or customer in response to a subpoena or warrant authorized by a Federal or State statute.''.

(b) DOMAIN NAME REGISTRATION SERVICE DEFINED.—Section 2711 of such title is amended—

(1) in paragraph (1), by striking ''and'' at the end;

(2) in paragraph (2), by striking the period at the end and inserting ''; and''; and

(3) by adding at the end the following:

''(3) the term 'domain name registration service' means a service to the public for the assignment and management of domain names and Internet Protocol addresses.''.

SEC. 107. REPORTS CONCERNING GOVERNMENTAL ACCESS TO ELECTRONIC COMMUNICATIONS.

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

''(i) REPORTS.—In April each year, the Attorney General shall transmit to Congress a full and complete report on—

''(1) the number and kind of warrants, orders, and subpoenas applied for by law enforcement agencies of the Department of Justice under this section;

''(2) the number of such applications granted or denied; and

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

''(A) the number and type of communications disclosed;

''(B) the approximate number and frequency of incriminating communications disclosed;

''(C) the offense specified in the application; and

''(D) the approximate number of persons whose communications were intercepted.''.

SEC. 108. ROVING WIRETAPS.

(a) SCOPE OF WIRETAPS.—Subsection (11)(b) of section 2518 of title 18, United States Code, is amended by striking clauses (ii) through (iv) and inserting the following new clauses:

''(ii) the application identifies the person believed to be committing the offense and whose communications are to be intercepted and the applicant makes a showing that—

''(I) the person changes facilities in a way that has the effect of thwarting interception from a specified facility; or

''(II) the person intends to thwart interception by changing facilities; and

''(iii) the judge finds that such showing has been adequately made.''.

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

(1) by inserting ''(a)'' after ''(12)''; and

(2) by adding at the end the following:

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

lieved to be committing the offense and named in the order is a party.''.

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

(a) USE OF CALL LOCATION AND CRASH NOTIFICATION INFORMATION.—Subsection (d) of section 222 of the Communications Act of 1934 (47 U.S.C. 222) is amended—

(1) by striking ''or'' at the end of paragraph (2);

(2) by striking the period at the end of paragraph (3) and inserting a semicolon; and

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

''(4) to provide call location information concerning the user of a commercial mobile service (as such term is defined in section 332(d))—

''(A) to a public safety answering point, emergency medical service provider or emergency dispatch provider, public safety official, fire service official, law enforcement official, hospital emergency facility, or trauma care facility in order to respond to the user's call for emergency services;

''(B) to inform the user's legal guardian or members of the user's immediate family of the user's location in an emergency situation that involves the risk of death or serious physical harm; or

''(C) to providers of information or database management services solely for purposes of assisting in the delivery of emergency services in response to an emergency; or

''(5) to transmit automatic crash notification information as part of the operation of an automatic crash notification system.''.

(b) CUSTOMER APPROVAL OF USE OF CALL LOCATION AND CRASH NOTIFICATION INFORMATION.—That section is further amended—

(1) by redesignating subsection (f) as subsection (h); and

(2) by inserting after subsection (e) the following new subsection (f):

''(f) CUSTOMER APPROVAL OF USE OF CALL LOCATION INFORMATION AND CRASH NOTIFICATION INFORMATION.—For purposes of subsection (c)(1), without the express prior authorization of the customer, a customer shall not be considered to have approved the use or disclosure of or access to—

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

''(2) automatic crash notification information to any person other than for use in the operation of an automatic crash notification system.''.

(c) USE OF LISTED AND UNLISTED SUBSCRIBER INFORMATION FOR EMERGENCY SERVICES.—That section is further amended by inserting after subsection (f), as amended by subsection (b) of this section, the following new subsection (g):

''(g) SUBSCRIBER LISTED AND UNLISTED INFORMATION FOR EMERGENCY SERVICES.—Notwithstanding subsections (b), (c), and (d), a telecommunications carrier that provides telephone exchange service shall provide information described in subsection (h)(3)(A) (including information pertaining to subscribers whose information is unlisted or unpublished) that is in its possession or control (including information pertaining to subscribers of other carriers) on a timely and unbundled basis, under nondiscriminatory and reasonable rates, terms, and conditions to providers of emergency services, and providers of emergency support services, solely for purposes of delivering or assisting in the delivery of emergency services.''.

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

(1) in paragraph (1)(A), by inserting ''location,'' after ''destination,''; and

(2) by adding at the end the following:

''(4) PUBLIC SAFETY ANSWERING POINT.—The term 'public safety answering point' means a facility that has been designated to receive emergency calls and route them to emergency service personnel.

''(5) EMERGENCY SERVICES.—The term 'emergency services' means 911 emergency services and emergency notification services.

''(6) EMERGENCY NOTIFICATION SERVICES.—The term 'emergency notification services' means services that notify the public of an emergency.

''(7) EMERGENCY SUPPORT SERVICES.—The term 'emergency support services' means information or data base management services used in support of emergency services.''.

SEC. 110. CONFIDENTIALITY OF SUBSCRIBER INFORMATION.

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

(1) in paragraph (1)(A), by inserting before the period at the end the following: ''only if such disclosure is—

''(i) necessary to initiate, render, bill, and collect for such service;

''(ii) necessary to protect the rights or property of the provider of such service;

''(iii) required by law;

''(iv) made at the request of the subscriber or customer; or

''(v) if the provider has provided the subscriber or customer, in a clear and conspicuous manner, with the opportunity to prohibit such disclosure.''; and

(2) by adding at the end the following:

''(3) Nothing in this subsection may be construed to prohibit a provider of electronic communication service or remote computing service from using, disclosing, or permitting access to aggregate subscriber information from which individual subscriber identities and characteristics have been removed.''.

TITLE II—PROMOTING USE OF ENCRYPTION

SEC. 201. FREEDOM TO USE ENCRYPTION.

(a) NO DOMESTIC ENCRYPTION CONTROLS.—It shall be lawful for any person within the United States, and for any United States person in a foreign country, to use, develop, manufacture, sell, distribute, or import any encryption product, regardless of the encryption algorithm selected, encryption key length chosen, existence of key recovery or other plaintext access capability, or implementation or medium used.

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

(1) IN GENERAL.—Except as provided in paragraph (3), no agency of the United States may require, compel, set standards for, condition any approval on, or condition the receipt of any benefit on, a requirement that a decryption key, access to a decryption key, key recovery information, or other plaintext access capability be—

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

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

(C) retained by the owner or user of an encryption key or any other person, other than for encryption products for the use of the Federal Government or a State government.

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

(3) EXCEPTIONS.—The prohibition in paragraph (1) does not apply to—

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

(B) the authority of any investigative or law enforcement officer, or any member of the intelligence community (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 401a)), acting under any law in effect on the date of enactment of this Act, to gain access to encrypted communications or information.

(c) USE OF ENCRYPTION FOR AUTHENTICATION OR INTEGRITY PURPOSES.—No agency of the United States shall establish any condition, tie, or link between encryption products, standards, and services used for confidentiality purposes and those used for authentication, integrity, or access control purposes.

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

To ensure that secure electronic access to the Federal Government is available to persons outside of and not operating under contract with agencies of the United States, the Federal Government may not purchase any encryption product with a key recovery or other plaintext access feature if such key recovery or plaintext access feature would interfere with use of the full encryption capabilities of the product when interoperating with other commercial encryption products.

SEC. 203. LAW ENFORCEMENT DECRYPTION ASSISTANCE.

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

"CHAPTER 124—ENCRYPTED WIRE OR ELECTRONIC COMMUNICATIONS AND STORED ELECTRONIC INFORMATION

"Sec.
"2801. Definitions.
"2802. Access to decryption assistance for communications.

''§ 2801. Definitions

''In this chapter:

''(1) DECRYPTION ASSISTANCE.—The term 'decryption assistance' means assistance that provides or facilitates access to the plaintext of an encrypted wire or electronic communication or stored electronic information, including the disclosure of a decryption key or the use of a decryption key to produce plaintext.

''(2) DECRYPTION KEY.—The term 'decryption key' means the variable information used in or produced by a mathematical formula, code, or algorithm, or any component thereof, used to decrypt a wire communication or electronic communication or stored electronic information that has been encrypted.

''(3) ENCRYPT; ENCRYPTION.—The terms 'encrypt' and 'encryption' refer to the scrambling (and descrambling) of wire communications, electronic communications, or electronically stored information using mathematical formulas or algorithms in order to preserve the confidentiality, integrity, or authenticity of, and prevent unauthorized recipients

from accessing or altering, such communications or information.

''(4) FOREIGN GOVERNMENT.—The term 'foreign government' has the meaning given the term in section 1116.

''(5) OFFICIAL REQUEST.—The term 'official request' has the meaning given the term in section 3506(c).

''(6) INCORPORATED DEFINITIONS.—Any term used in this chapter that is not defined in this chapter and that is defined in section 2510, has the meaning given the term in section 2510.

''§ 2802. Access to decryption assistance for communications

''(a) CRIMINAL INVESTIGATIONS.—

''(1) IN GENERAL.—An order authorizing the interception of a wire or electronic communication under section 2518 shall, upon request of the applicant, direct that a provider of wire or electronic communication service, or any other person possessing information capable of decrypting that communication, other than a person whose communications are the subject of the interception, shall promptly furnish the applicant with the necessary decryption assistance, if the court finds that the

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

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

''(A) contain a provision that the decryption assistance provided shall involve disclosure of a private decryption key only if no other form of decryption assistance is available and otherwise shall be limited to the minimum necessary to decrypt the communications intercepted pursuant to such order; and

''(B) terminate on the earlier of—

''(i) the date on which the authorized objective is attained; or

''(ii) 30 days after the date on which the order or extension, as applicable, is issued.

''(3) NOTICE.—If decryption assistance is provided pursuant to an order under this subsection, the court issuing the order shall cause to be served on the person whose communications are the subject of such decryption assistance, as part of the inventory required to be served pursuant to section

2518(8), notice of the receipt of the decryption assistance and a specific description of the decryption keys or other decryption assistance disclosed.

''(b) FOREIGN INTELLIGENCE INVESTIGATIONS.—

''(1) IN GENERAL.—An order authorizing the interception of a wire or electronic communication under section 105(b)(2) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1805(b)(2)) shall, upon request of the applicant, direct that a provider of wire or electronic communication service, or any other person possessing information capable of decrypting such communications, other than a person whose communications are the subject of the interception, shall promptly furnish the applicant with the necessary decryption assistance, if the court finds that the decryption assistance sought is necessary for the decryption of a communication intercepted pursuant to the order.

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

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

munications intercepted pursuant to such order; and

"(B) terminate on the earlier of—

"(i) the date on which the authorized objective is attained; or

"(ii) 30 days after the date on which the order or extension, as applicable, is issued.

"(c) GENERAL PROHIBITION ON DISCLOSURE.—Other than pursuant to an order under subsection (a) or (b), no person possessing information capable of decrypting a wire or electronic communication of another person shall disclose that information or provide decryption assistance to an investigative or law enforcement officer.

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

"(a) DECRYPTION ASSISTANCE.—No person may disclose a decryption key or provide decryption assistance pertaining to the contents of stored electronic communications or records, including those disclosed pursuant to section 2703, to a governmental entity, except—

"(1) pursuant to a warrant issued under the Federal Rules of Criminal Procedure or an equivalent State warrant, a copy of which warrant shall be

served on the person who created the electronic communication or record before or at the same time service is made on the keyholder;

''(2) pursuant to a subpoena, a copy of which subpoena shall be served on the person who created the electronic communication or record, under circumstances allowing the person meaningful opportunity to challenge the subpoena; or

''(3) upon the consent of the person who created the electronic communication or record.

''(b) DELAY OF NOTIFICATION.—In the case of communications disclosed pursuant to section 2703(a), service of the copy of the warrant or subpoena on the person who created the electronic communication or record may be delayed for a period of not to exceed 90 days upon request to the court by the governmental entity requiring the decryption assistance, if the court determines that there is reason to believe that notification of the existence of the court order or subpoena may have an adverse result described in section 2705(a)(2).

''§ 2804. Foreign government access to decryption assistance

''(a) IN GENERAL.—No investigative or law enforcement officer may—

''(1) release a decryption key to a foreign government or to a law enforcement agency of a foreign government; or

''(2) except as provided in subsection (b), provide decryption assistance to a foreign government or to a law enforcement agency of a foreign government.

''(b) CONDITIONS FOR COOPERATION WITH FOREIGN GOVERNMENT.—

''(1) APPLICATION FOR ORDER.—In any case in which the United States has entered into a treaty or convention with a foreign government to provide mutual assistance with respect to providing decryption assistance, the Attorney General (or the designee of the Attorney General) may, upon an official request to the United States from the foreign government, apply for an order described in paragraph (2) from the district court in which the person possessing information capable of decrypting the encrypted communication or stored electronic information at issue resides—

''(A) directing that person to release a decryption key or provide decryption assistance to the Attorney General (or the designee of the Attorney General); and

"(B) authorizing the Attorney General (or the designee of the Attorney General) to furnish the foreign government with the plaintext of the communication or information at issue.

"(2) CONTENTS OF ORDER.—An order described in this paragraph is an order directing the person possessing information capable of decrypting the communication or information at issue to—

"(A) release a decryption key to the Attorney General (or the designee of the Attorney General) so that the plaintext of the communication or information may be furnished to the foreign government; or

"(B) provide decryption assistance to the Attorney General (or the designee of the Attorney General) so that the plaintext of the communication or information may be furnished to the foreign government.

"(3) REQUIREMENTS FOR ORDER.—The court described in paragraph (1) may issue an order described in paragraph (2) if the court finds, on the basis of an application made by the Attorney General under this subsection, that—

"(A) the decryption key or decryption assistance sought is necessary for the decryption

of a communication or information that the foreign government is authorized to intercept or seize pursuant to the law of the foreign country;

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

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

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

''124. Encrypted wire or electronic communications and stored electronic information ..... 2801''.

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

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

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

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

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

"§ 2710. Wrongful disclosure of video tape rental or sale records and library loan and book sale records

''(a) DEFINITIONS.—In this section:

''(1) The term 'book seller' means any person, engaged in the business, in or affecting interstate or foreign commerce, of selling books, magazines, or other printed material, or any person or other entity to whom a disclosure is made under subparagraph (D) or (E) of subsection (b)(2), but only with respect to the information contained in the disclosure.

''(2) The term 'consumer' means any renter, purchaser, or subscriber of goods or services from a video tape service provider or book seller.

''(3) The term 'library' means an institution that operates as a public library or serves as a library for any university, school, or college.

''(4) The term 'ordinary course of business' means only debt collection activities, order fulfillment, request processing, and the transfer of ownership.

''(5) The term 'patron' means any individual who requests or receives—

''(A) services within a library; or

''(B) books or other materials on loan from a library.

''(6) The term 'personally identifiable information' includes the following:

''(A) Information that identifies a person as having requested or obtained specific video materials or services from a video tape service provider.

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

''(C) Information that identifies a person as having requested or obtained any materials or services from a library.

''(7) The term 'video tape service provider' means any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials, or any person or other entity to whom a disclosure is made under subparagraph (D) or (E) of subsection (b)(2), but

only with respect to the information contained in the disclosure.

''(b) VIDEO TAPE RENTAL AND SALE AND BOOK SALE RECORDS.—

''(1) IN GENERAL.—A video tape service provider or book seller who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider or seller, as the case may be, shall be liable to the aggrieved person for the relief provided in subsection (d).

''(2) DISCLOSURE.—A video tape service provider or book seller may disclose personally identifiable information concerning any consumer—

''(A) to the consumer;

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

''(C) to a law enforcement agency pursuant to a warrant issued under the Federal Rules of Criminal Procedure, an equivalent State warrant, or a court order issued in accordance with paragraph (4);

''(D) to any person if the disclosure is solely of the names and addresses of consumers and if—

''(i) the video tape service provider or book seller, as the case may be, has provided the consumer, in a clear and conspicuous manner, with the opportunity to prohibit such disclosure; and

''(ii) the disclosure does not identify the title, description, or subject matter of any video tapes or other audio visual material, or books, magazines, or other printed material, except that the subject matter of such materials may be disclosed if the disclosure is for the exclusive use of marketing goods and services directly to the consumer;

''(E) to any person if the disclosure is incident to the ordinary course of business of the video tape service provider or book seller; or

''(F) pursuant to a court order, in a civil proceeding upon a showing of compelling need for the information that cannot be accommodated by any other means, if—

''(i) the consumer is given reasonable notice, by the person seeking the disclosure, of the court proceeding relevant to the issuance of the court order; and

"(ii) the consumer is afforded the opportunity to appear and contest the claim of the person seeking the disclosure.

"(3) SAFEGUARDS.—If an order is granted pursuant to subparagraph (C) or (F) of paragraph (2), the court shall impose appropriate safeguards against unauthorized disclosure.

"(4) COURT ORDERS.—A court order authorizing disclosure under paragraph (2)(C) shall issue only with prior notice to the consumer and only if the law enforcement agency shows that there is probable cause to believe that a person has engaged, is engaging, or is about to engage in criminal activity and that the records or other information sought are material to the investigation of such activity. In the case of a State government authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this subsection, on a motion made promptly by the video tape service provider or the book seller, may quash or modify such order if the information or records requested are unreasonably voluminous in nature or if compliance with such order otherwise would cause an unreasonable burden on such provider or seller, as the case may be.

''(c) LIBRARY RECORDS.—

''(1) IN GENERAL.—Any library that knowingly discloses, to any person, personally identifiable information concerning any patron of the library shall be liable to the aggrieved person as provided in subsection (d).

''(2) DISCLOSURE.—A library may disclose personally identifiable information concerning any patron—

''(A) to the patron;

''(B) to any person with the informed written consent of the patron given at the time the disclosure is sought;

''(C) to a law enforcement agency pursuant to a warrant issued under the Federal Rules of Criminal Procedure, an equivalent State warrant, or a court order issued in accordance with paragraph (4);

''(D) to any person if the disclosure is solely of the names and addresses of patrons and if—

''(i) the library has provided the patron with a written statement that affords the patron the opportunity to prohibit such disclosure; and

"(ii) the disclosure does not reveal, directly or indirectly, the title, description, or subject matter of any library materials borrowed or services utilized by the patron;

"(E) to any authorized person if the disclosure is necessary for the retrieval of overdue library materials or the recoupment of compensation for damaged or lost library materials; or

"(F) pursuant to a court order, in a civil proceeding upon a showing of compelling need for the information that cannot be accommodated by any other means, if—

"(i) the patron is given reasonable notice, by the person seeking the disclosure, of the court proceeding relevant to the issuance of the court order; and

"(ii) the patron is afforded the opportunity to appear and contest the claim of the person seeking the disclosure.

"(3) SAFEGUARDS.—If an order is granted pursuant to subparagraph (C) or (F) of paragraph (2), the court shall impose appropriate safeguards against unauthorized disclosure.

"(4) COURT ORDERS.—A court order authorizing disclosure under paragraph (2)(C) shall issue

only with prior notice to the patron and only if the law enforcement agency shows that there is probable cause to believe that a person has engaged, is engaging or is about to engage in criminal activity and that the records or other information sought are material to the investigation of such activity. In the case of a State government authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this subsection, on a motion made promptly by the library, may quash or modify such order if the information or records requested are unreasonably voluminous in nature or if compliance with such order otherwise would cause an unreasonable burden on the library.''.

(b) CLERICAL AMENDMENT.—The item relating to section 2701 in the analysis for chapter 121 of title 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.''.

TITLE IV—PRIVACY PROTECTION FOR SATELLITE HOME VIEWERS

SEC. 401. PRIVACY PROTECTION FOR SUBSCRIBERS OF SATELLITE TELEVISION SERVICES FOR PRIVATE HOME VIEWING.

(a) IN GENERAL.—Section 631 of the Communications Act of 1934 (47 U.S.C. 551) is amended to read as follows:

"SEC. 631. PRIVACY OF SUBSCRIBER INFORMATION FOR SUBSCRIBERS OF CABLE SERVICE AND SATELLITE TELEVISION SERVICE.

''(a) NOTICE TO SUBSCRIBERS REGARDING PERSONALLY IDENTIFIABLE INFORMATION.—At the time of entering into an agreement to provide any cable service, satellite home viewing service, or other service to a subscriber, and not less often than annually thereafter, a cable operator, satellite carrier, or distributor shall provide notice in the form of a separate, written statement to such subscriber that clearly and conspicuously informs the subscriber of—

''(1) the nature of personally identifiable information collected or to be collected with respect to the subscriber as a result of the provision of such

service and the nature of the use of such information;

''(2) the nature, frequency, and purpose of any disclosure that may be made of such information, including an identification of the types of persons to whom the disclosure may be made;

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

''(4) the times and place at which the subscriber may have access to such information in accordance with subsection (d); and

''(5) the limitations provided by this section with respect to the collection and disclosure of information by the cable operator, satellite carrier, or distributor and the right of the subscriber under this section to enforce such limitations.

''(b) COLLECTION OF PERSONALLY IDENTIFIABLE INFORMATION.—

''(1) IN GENERAL.—Except as provided in paragraph (2), a cable operator, satellite carrier, or distributor shall not use its cable or satellite system to collect personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber.

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

''(A) obtain information necessary to render a cable or satellite service or other service provided by the cable operator, satellite carrier, or distributor to the subscriber; or

''(B) detect unauthorized reception of cable or satellite communications.

''(c) DISCLOSURE OF PERSONALLY IDENTIFIABLE INFORMATION.—

''(1) IN GENERAL.—Except as provided in paragraph (2), a cable operator, satellite carrier, or distributor may not disclose personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber and shall take such actions as are necessary to prevent unauthorized access to such information by a person other than the subscriber or the cable operator, satellite carrier, or distributor.

''(2) EXCEPTIONS.—A cable operator, satellite carrier, or distributor may disclose information described in paragraph (1) if the disclosure is—

"(A) necessary to render, or conduct a legitimate business activity related to, a cable or satellite service or other service provided by the cable operator, satellite carrier, or distributor to the subscriber;

"(B) subject to paragraph (3), made pursuant to a court order authorizing such disclosure, if the subscriber is notified of such order by the person to whom the order is directed; or

"(C) a disclosure of the names and addresses of subscribers to any other provider of cable or satellite service or other service, if—

"(i) the cable operator, satellite carrier, or distributor has provided the subscriber the opportunity to prohibit or limit such disclosure; and

"(ii) the disclosure does not reveal, directly or indirectly—

"(I) the extent of any viewing or other use by the subscriber of a cable or satellite service or other service provided by the cable operator, satellite carrier, or distributor; or

"(II) the nature of any transaction made by the subscriber over

the cable or satellite system of the cable operator, satellite carrier, or distributor.

''(3) COURT ORDERS.—A governmental entity may obtain personally identifiable information concerning a cable or satellite subscriber pursuant to a court order only if, in the court proceeding relevant to such court order—

''(A) such entity offers clear and convincing evidence that the subject of the information is reasonably suspected of engaging in criminal activity and that the information sought would be material evidence in the case; and

''(B) the subject of the information is afforded the opportunity to appear and contest such entity's claim.

''(d) SUBSCRIBER ACCESS TO INFORMATION.—A cable or satellite subscriber shall be provided access to all personally identifiable information regarding that subscriber that is collected and maintained by a cable operator, satellite carrier, or distributor. Such information shall be made available to the subscriber at reasonable times and at a convenient place designated by such cable operator, satellite carrier, or distributor. A cable or sat-

ellite subscriber shall be provided reasonable opportunity to correct any error in such information.

''(e) DESTRUCTION OF INFORMATION.—A cable operator, satellite carrier, or distributor shall destroy personally identifiable information if the information is no longer necessary for the purpose for which it was collected and there are no pending requests or orders for access to such information under subsection (d) or pursuant to a court order.

''(f) RELIEF.—

''(1) IN GENERAL.—Any person aggrieved by any act of a cable operator, satellite carrier, or distributor in violation of this section may bring a civil action in a district court of the United States.

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

''(A) actual damages but not less than liquidated damages computed at the rate of $100 a day for each day of violation or $1,000, whichever is greater;

''(B) punitive damages; and

''(C) reasonable attorneys' fees and other litigation costs reasonably incurred.

''(3) NO EFFECT ON OTHER REMEDIES.—The remedy provided by this subsection shall be in addition to any other remedy available under any provision of law to a cable or satellite subscriber.

''(g) DEFINITIONS.—In this section:

''(1) DISTRIBUTOR.—The term 'distributor' has the meaning given that term in section 119(d)(1) of title 17, United States Code.

''(2) CABLE OPERATOR.—

''(A) IN GENERAL.—The term 'cable operator' has the meaning given that term in section 602.

''(B) INCLUSION.—The term includes any person who—

''(i) is owned or controlled by, or under common ownership or control with, a cable operator; and

''(ii) provides any wire or radio communications service.

''(3) OTHER SERVICE.—The term 'other service' includes any wire, electronic, or radio communications service provided using any of the facilities of a cable operator, satellite carrier, or distributor that are used in the provision of cable service or satellite home viewing service.

''(4) PERSONALLY IDENTIFIABLE INFORMATION.—The term 'personally identifiable information' does not include any record of aggregate data that does not identify particular persons.

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

(b) NOTICE WITH RESPECT TO CERTAIN AGREEMENTS.—

(1) IN GENERAL.—Except as provided in paragraph (2), a cable operator, satellite carrier, or distributor who has entered into agreements referred to in section 631(a) of the Communications Act of 1934, as amended by subsection (a), before the date of enactment of this Act, shall provide any notice required under that section, as so amended, to subscribers under such agreements not later than 180 days after that date.

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

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

○