HEINONLINE

Citation: 6 Bernard D. Reams Jr. Law of E-SIGN A Legislative of the Electronic Signatures in Global and National Act Public Law No. 106-229 2000 1 2002

Content downloaded/printed from HeinOnline (http://heinonline.org) Sun Apr 21 22:59:59 2013

-- Your use of this HeinOnline PDF indicates your acceptance of HeinOnline's Terms and Conditions of the license agreement available at http://heinonline.org/HOL/License

-- The search text of this PDF is generated from uncorrected OCR text.

105TH CONGRESS
2D SESSION

S. 2067

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

IN THE SENATE OF THE UNITED STATES

MAY 12, 1998

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

---

A BILL

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

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

HeinOnline -- 6 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 1 2002

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "Encryption Protects the Rights of Individuals from Violation and Abuse in CYberspace (E–PRIVACY) 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 ensure that Americans have the maximum possible choice in encryption methods to protect the security, confidentiality, and privacy of their

HeinOnline -- 6 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 2 2002

lawful wire and electronic communications and stored electronic information;

(2) 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 same access to electronic communications and information as under current law; and

(3) to establish privacy standards and procedures by which investigative or law enforcement officers 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 American citizens and the competitiveness of American businesses;

HeinOnline -- 6 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 3 2002

(2) a secure, private, and trusted national and global information infrastructure is essential to promote economic growth, protect privacy, and meet the needs of American citizens 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, finances, and employees, to computers and computer networks unless the security and privacy of that information is assured;

HeinOnline -- 6 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 4 2002

(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

HeinOnline -- 6 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 5 2002

encrypted data threatens the security and privacy of information systems;

(12) American companies should be free to compete and sell encryption technology, programs, and products, and to exchange encryption technology, programs, and products through the use of the Internet, which is rapidly emerging as the preferred method of distribution of computer software and related information;

(13) 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;

(14) 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;

(15) the Constitution of the United States permits lawful electronic surveillance by investigative or law enforcement officers and the seizure of stored electronic information only upon compliance with stringent standards and procedures; and

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

HeinOnline -- 6 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 6 2002

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.

SEC. 4. DEFINITIONS.

In this Act:

(1) AGENCY.—The term "agency" has the meaning given the term in section 6 of title 18, United States Code.

(2) COMPUTER HARDWARE.—The term "computer hardware" includes computer systems, equipment, application-specific assemblies, smart cards, modules, and integrated circuits.

(3) COMPUTING DEVICE.—The term "computing device" means a device that incorporates 1 or more microprocessor-based central processing units that are capable of accepting, storing, processing, or providing output of data.

(4) ENCRYPT AND ENCRYPTION.—The terms "encrypt" and "encryption" refer to the scrambling (and descrambling) of wire communications, elec-

HeinOnline -- 6 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 7 2002

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.

(5) ENCRYPTION PRODUCT.—The term "encryption product"—

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

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

(6) EXPORTABLE.—The term "exportable" means the ability to transfer, ship, or transmit to foreign users.

(7) 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.

HeinOnline -- 6 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 8 2002

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

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

(10) STATE.—The term "State" has the meaning given the term in section 3156(a)(5) of title 18, United States Code.

(11) TECHNICAL REVIEW.—The term "technical review" means a review by the Secretary, based on information about a product's encryption capabilities supplied by the manufacturer, that an encryption product works as represented.

(12) UNITED STATES PERSON.—The term "United States person" means any—

(A) United States citizen; or

(B) any legal entity that—

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

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

HeinOnline -- 6 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 9 2002

TITLE I—PRIVACY PROTECTION FOR COMMUNICATIONS AND ELECTRONIC INFORMATION

SEC. 101. FREEDOM TO USE ENCRYPTION.

(a) IN GENERAL.—Except as otherwise provided by this Act and the amendments made by this Act, 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 ENCRYPTION.—

(1) IN GENERAL.—Except as provided in paragraph (3), no agency of the United States nor any State 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) given to any other person, including any agency of the United States or a State, or any entity in the private sector; or

HeinOnline -- 6 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 10 2002

(B) retained by any person using encryption.

(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) EXCEPTION.—The prohibition in paragraph (1) does not apply to encryption used by an agency of the United States or a State, or the employees or agents of such an agency, solely for the internal operations and telecommunications systems of the United States or the State.

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

(1) IN GENERAL.—The use, development, manufacture, sale, distribution and import of encryption products, standards, and services for purposes of assuring the confidentiality, authenticity, or integrity or access control of electronic information shall be voluntary and market driven.

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

HeinOnline -- 6 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 11 2002

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

SEC. 102. PURCHASE AND USE OF ENCRYPTION PRODUCTS BY THE FEDERAL GOVERNMENT.

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

(1) the internal operations and telecommunications systems of the agency; or

(2) use by, among, and between that agency and any other agency of the United States, the employees of the agency, or persons operating under contract with the agency.

(b) INTEROPERABILITY.—To ensure that secure electronic access to the Government is available to persons outside of and not operating under contract with agencies of the United States, the United States shall purchase no 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 product's full encryption capabilities when interoperating with other commercial encryption products.

SEC. 103. ENHANCED PRIVACY PROTECTION FOR INFORMATION ON COMPUTER NETWORKS.

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

HeinOnline -- 6 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 12 2002

"(g) ACCESS TO STORED ELECTRONIC INFORMATION.—

"(1) DISCLOSURE.—

"(A) IN GENERAL.—Subject to subparagraph (B), a governmental entity may require the disclosure by a provider of a remote computing service of the contents of an electronic record in networked electronic storage only if the person who created the record is accorded the same protections that would be available if the record had remained in that person's possession.

"(B) NETWORKED ELECTRONIC STORAGE.—In addition to the requirements of subparagraph (A) and subject to paragraph (2), a governmental entity may require the disclosure of the contents of an electronic record in networked electronic storage only—

"(i) 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 person who created the record prior to or at the same time the warrant is served on

HeinOnline -- 6 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 13 2002

the provider of the remote computing service;

"(ii) pursuant to a subpoena issued under the Federal Rules of Criminal Procedure or equivalent State warrant, a copy of which subpoena shall be served on the person who created the record, under circumstances allowing that person a meaningful opportunity to challenge the subpoena; or

"(iii) upon the consent of the person who created the record.

"(2) DEFINITION.—In this subsection, an electronic record is in 'networked electronic storage' if—

"(A) it is not covered by subsection (a) of this section;

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

"(C) the person who created the record is able to access and modify it remotely through electronic means.".

HeinOnline -- 6 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 14 2002

SEC. 104. 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:

"(h) REQUIREMENTS FOR DISCLOSURE OF LOCATION INFORMATION.—A provider of mobile electronic communication service shall provide to a governmental entity information generated by and disclosing, on a real time basis, the 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 an individual using or possessing the subscriber equipment is committing, has committed, or is about to commit a felony offense.".

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

SEC. 105. ENHANCED PRIVACY PROTECTION FOR TRANSACTIONAL INFORMATION OBTAINED FROM PEN REGISTERS OR TRAP AND TRACE DEVICES.

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

HeinOnline -- 6 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 15 2002

"(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.".

TITLE II—LAW ENFORCEMENT ASSISTANCE

SEC. 201. ENCRYPTED WIRE OR ELECTRONIC COMMUNICATIONS AND STORED ELECTRONIC COMMUNICATIONS.

(a) IN GENERAL.—Part I of title 18, United States Code, is amended by inserting after chapter 123 the following:

HeinOnline -- 6 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 16 2002

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

"§ 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.

HeinOnline -- 6 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 17 2002

"(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. Unlawful use of encryption

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

HeinOnline -- 6 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 18 2002

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

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

"(2) in the case of a second or subsequent offense under this section, shall be imprisoned not more than 10 years, fined under this title, or both.

"§ 2803. 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.

HeinOnline -- 6 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 19 2002

"(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 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 this chapter; 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 described in paragraph (1)—

"(A) 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

HeinOnline -- 6 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 20 2002

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

"(B) upon the filing of a motion and for good cause shown, shall make available to such person, or to counsel for that person, for inspection, the intercepted communications to which the decryption assistance related, except that on an ex parte showing of good cause, the serving of the inventory required by section 2518(8) may be postponed.

"(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.

HeinOnline -- 6 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 21 2002

"(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 communications intercepted pursuant to this chapter; 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) of this section, 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 (as defined in section 2510(7)).

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

"(a) DECRYPTION ASSISTANCE.—No person may disclose a decryption key or provide decryption assistance

HeinOnline -- 6 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 22 2002

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 prior to 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 under subsection (a) 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

HeinOnline -- 6 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 23 2002

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

"§ 2805. 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 AN 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

HeinOnline -- 6 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 24 2002

possessing information capable of decrypting the communication or 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 encrypted communication or stored electronic information at issue.

"(2) CONTENTS OF ORDER.—An order is described in this paragraph if it 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 com-

HeinOnline -- 6 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 25 2002

munication 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 that 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.

HeinOnline -- 6 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 26 2002

"§ 2806. Establishment and operations of National Electronic Technologies Center

"(a) NATIONAL ELECTRONIC TECHNOLOGIES CENTER.—

"(1) ESTABLISHMENT.—There is established in the Department of Justice a National Electronic Technologies Center (referred to in this section as the 'NET Center').

"(2) DIRECTOR.—The NET Center shall be administered by a Director (referred to in this section as the 'Director'), who shall be appointed by the Attorney General.

"(3) DUTIES.—The NET Center shall—

"(A) serve as a center for Federal, State, and local law enforcement authorities for information and assistance regarding decryption and other access requirements;

"(B) serve as a center for industry and government entities to exchange information and methodology regarding information security techniques and technologies;

"(C) support and share information and methodology regarding information security techniques and technologies with the Computer Investigations and Infrastructure Threat Assessment Center (CITAC) and Field Computer

HeinOnline -- 6 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 27 2002

Investigations and Infrastructure Threat Assessment (CITA) Squads of the Federal Bureau of Investigation;

"(D) examine encryption techniques and methods to facilitate the ability of law enforcement to gain efficient access to plaintext of communications and electronic information;

"(E) conduct research to develop efficient methods, and improve the efficiency of existing methods, of accessing plaintext of communications and electronic information;

"(F) investigate and research new and emerging techniques and technologies to facilitate access to communications and electronic information, including—

"(i) reverse-stenography;

"(ii) decompression of information that previously has been compressed for transmission; and

"(iii) demultiplexing;

"(G) investigate and research interception and access techniques that preserve the privacy and security of information not authorized to be intercepted; and

HeinOnline -- 6 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 28 2002

"(H) obtain information regarding the most current hardware, software, telecommunications, and other capabilities to understand how to access digitized information transmitted across networks.

"(4) EQUAL ACCESS.—State and local law enforcement agencies and authorities shall have access to information, services, resources, and assistance provided by the NET Center to the same extent that Federal law enforcement agencies and authorities have such access.

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

"(6) ASSISTANCE OF OTHER FEDERAL AGENCIES.—Upon the request of the Director of the NET Center, the head of any department or agency of the Federal Government may, to assist the NET Center in carrying out its duties under this subsection—

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

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

HeinOnline -- 6 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 29 2002

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

"(8) ADVISORY BOARD.—

"(A) ESTABLISHMENT.—There is established in the NET Center an Advisory Board for Excellence in Information Security (in this paragraph referred to as the 'Advisory Board'), which shall be comprised of members who have the qualifications described in subparagraph (B) and who are appointed by the Attorney General. The Attorney General shall appoint a chairman of the Advisory Board.

"(B) QUALIFICATIONS.—Each member of the Advisory Board shall have experience or expertise in the field of encryption, decryption, electronic communication, information security,

HeinOnline -- 6 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 30 2002

electronic commerce, privacy protection, or law enforcement.

"(C) DUTIES.—The duty of the Advisory Board shall be to advise the NET Center and the Federal Government regarding new and emerging technologies relating to encryption and decryption of communications and electronic information.

"(9) IMPLEMENTATION PLAN.—

"(A) IN GENERAL.—Not later than 2 months after the date of enactment of this chapter, the Attorney General shall, in consultation and cooperation with other appropriate Federal agencies and appropriate industry participants, develop and cause to be published in the Federal Register a plan for establishing the NET Center.

"(B) CONTENTS OF PLAN.—The plan published under subparagraph (A) shall—

"(i) specify the physical location of the NET Center and the equipment, software, and personnel resources necessary to carry out the duties of the NET Center under this subsection;

HeinOnline -- 6 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 31 2002

"(ii) assess the amount of funding necessary to establish and operate the NET Center; and

"(iii) identify sources of probable funding for the NET Center, including any sources of in-kind contributions from private industry.

"(b) AUTHORIZATION.—There are authorized to be appropriated such sums as may be necessary for the establishment and operation of the NET Center.".

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

TITLE III—EXPORTS OF ENCRYPTION PRODUCTS

SEC. 301. COMMERCIAL ENCRYPTION PRODUCTS.

(a) PROVISIONS APPLICABLE TO COMMERCIAL PRODUCTS.—The provisions of this title apply to all encryption products, regardless of the encryption algorithm selected, encryption key length chosen, exclusion of key recovery or other plaintext access capability, or implementation or medium used, except those specifically designed or modified for military use, including command, control, and intelligence applications.

HeinOnline -- 6 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 32 2002

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

SEC. 302. LICENSE EXCEPTION FOR MASS MARKET PRODUCTS.

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

(b) DEFINITIONS.—In this section, the term "generally available" means an encryption product that is—

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

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

HeinOnline -- 6 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 33 2002

user or purchaser selection among installation or configuration parameters.

(c) COMMERCE DEPARTMENT ASSURANCE.—

(1) IN GENERAL.—The manufacturer or exporter of an encryption product may request written assurance from the Secretary of Commerce that an encryption product is considered generally available for purposes of this section.

(2) RESPONSE.—Not later than 30 days after receiving a request under paragraph (1), the Secretary shall make a determination regarding whether to issue a written assurance under that paragraph, and shall notify the person making the request, in writing, of that determination.

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

SEC. 303. LICENSE EXCEPTION FOR PRODUCTS WITHOUT ENCRYPTION CAPABLE OF WORKING WITH ENCRYPTION PRODUCTS.

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

HeinOnline -- 6 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 34 2002

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

SEC. 304. LICENSE EXCEPTION FOR PRODUCT SUPPORT AND CONSULTING SERVICES.

(a) NO ADDITIONAL EXPORT CONTROLS IMPOSED IF UNDERLYING PRODUCT COVERED BY LICENSE EXCEPTION.—Technical assistance and technical data associated with the installation and maintenance of encryption products covered by sections 302 and 303 shall be exportable without the need for an export license, and without restrictions other than those permitted under this Act.

(b) DEFINITIONS.—In this section:

(1) TECHNICAL ASSISTANCE.—The term "technical assistance" means services, including instruction, skills training, working knowledge, and consulting services, and the transfer of technical data.

(2) TECHNICAL DATA.—The term "technical data" means information including blueprints, plans, diagrams, models, formulae, tables, engineering designs and specifications, manuals and instructions

HeinOnline -- 6 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 35 2002

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

SEC. 305. LICENSE EXCEPTION WHEN COMPARABLE FOREIGN PRODUCTS AVAILABLE.

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

(b) DETERMINATION OF FOREIGN AVAILABILITY.—

(1) ENCRYPTION EXPORT ADVISORY BOARD ESTABLISHED.—There is hereby established a board to be known as the "Encryption Export Advisory Board" (in this section referred to as the "Board").

(2) MEMBERSHIP.—The Board shall be comprised of—

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

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

HeinOnline -- 6 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 36 2002

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

(I) the National Security Agency;

(II) the Central Intelligence Agency; and

(III) the Office of the President; and

(ii) four shall be individuals from the private sector who have expertise in the development, operation, or marketing of information technology products; and

(C) four individuals appointed by Congress from among individuals in the private sector who have expertise in the development, operation, or marketing of information technology products, of whom—

(i) one shall be appointed by the Majority Leader of the Senate;

(ii) one shall be appointed by the Minority Leader of the Senate;

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

HeinOnline -- 6 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 37 2002

(iv) one shall be appointed by the Minority Leader of the House of Representatives.

(3) MEETINGS.—

(A) IN GENERAL.—Subject to subparagraph (B), the Board shall meet at the call of the Under Secretary of Commerce for Export Administration.

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

(4) DUTIES.—

(A) IN GENERAL.—Whenever an application for a license exception for an encryption product under this section is submitted to the Secretary of Commerce, the Board shall determine whether a comparable encryption product is commercially available outside the United States from a foreign supplier as specified in subsection (a).

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

HeinOnline -- 6 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 38 2002

(C) DEADLINE.—The Board shall make a determination with respect to an encryption product under this paragraph not later than 30 days after receipt by the Secretary of an application for a license exception under this subsection based on the encryption product.

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

(E) REPORTS TO PRESIDENT.—Not later than 30 days after a meeting under this paragraph, the Board shall submit to the President a report on the meeting.

(F) APPLICABILITY OF FACA.—The provisions of the Federal Advisory Committee Act (5 U.S.C. App.) shall not apply to the Board or to meetings held by the Board under this paragraph.

(5) ACTION BY SECRETARY OF COMMERCE.—

(A) APPROVAL OR DISAPPROVAL.—The Secretary of Commerce shall specifically approve or disapprove each determination of the Board under paragraph (5) not later than 30 days of the submittal of such determination to the Secretary under that paragraph.

HeinOnline -- 6 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 39 2002

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

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

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

(C) CONTENTS OF NOTICE.—Each notice of a decision of disapproval by the Secretary of Commerce under subparagraph (B) of a determination of the Board under paragraph (4) that an encryption product is commercially available outside the United States from a foreign supplier shall set forth an explanation in detail of the reasons for the decision, including why and how continued export control of the encryption product which the determination concerned will be effective in achieving its purpose and the amount of lost sales and loss in market share of United States encryption products as a result of the decision.

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

HeinOnline -- 6 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 40 2002

outside the United States from a foreign supplier shall be subject to judicial review under the provisions of subchapter II of chapter 5 of title 5, United States Code (commonly referred to as the "Administrative Procedures Act").

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

SEC. 306. NO EXPORT CONTROLS ON ENCRYPTION PRODUCTS USED FOR NONCONFIDENTIALITY PURPOSES.

(a) PROHIBITION ON NEW CONTROLS.—The Federal Government shall not restrict the export of encryption products used for nonconfidentiality purposes such as authentication, integrity, digital signatures, nonrepudiation, and copy protection.

(b) NO REINSTATEMENT OF CONTROLS ON PREVIOUSLY DECONTROLLED PRODUCTS.—Those encryption

HeinOnline -- 6 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 41 2002

products previously decontrolled and not requiring an export license as of January 1, 1998, as a result of administrative decision or rulemaking shall not require an export license.

SEC. 307. APPLICABILITY OF GENERAL EXPORT CONTROLS.

(a) SUBJECT TO TERRORIST AND EMBARGO CONTROLS.—Nothing in this Act shall be construed to limit the authority of the President under the International Emergency Economic Powers Act, the Trading with the Enemy Act, or the Export Administration Act, to—

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

(2) impose an embargo on exports to, and imports from, a specific country.

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

HeinOnline -- 6 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 42 2002

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

(c) OTHER EXPORT CONTROLS REMAIN APPLICABLE.—(1) Encryption products shall remain subject to all export controls imposed on such products for reasons other than the existence of encryption capabilities.

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

SEC. 308. FOREIGN TRADE BARRIERS TO UNITED STATES PRODUCTS.

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

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

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

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

O

HeinOnline -- 6 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 43 2002

HeinOnline -- 6 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 44 2002

Document No. 153

HeinOnline -- 6 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) [i] 2002

HeinOnline -- 6 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) [ii] 2002