Order Code RL30273

CRS Report for Congress

Encryption Export Controls

Updated January 11, 2001

(name redacted)
Legislative Attorney
American Law Division

Encryption Export Controls

Summary

Encryption exports are controlled under the Arms Export Control Act (AECA) and the Export Administration Act (EAA), the latter statute to expire August 20, 2001. The more stringent AECA controls, administered by the State Department, apply to encryption items classified as defense articles or services. Items not so classified are subject to regulation by the Department of Commerce (DOC) under the extended EAA authorities. DOC requires licenses for certain commodities and software, but allows other encryption items to be exported under license exceptions.

The U.S. Government has traditionally maintained that controls over strong encryption are necessary for national security, foreign policy, and law enforcement reasons. Industry has argued that federal regulatory policies insufficiently address rapid technological developments, prevent manufacturers from marketing products available abroad, and harm U.S. national interests by making strong U.S. encryption unobtainable by legitimate users worldwide. While most encryption was originally controlled under the AECA, in late 1996 the President transferred jurisdiction over nonmilitary items to DOC, which at the same time eased controls over commercial encryption that used a key recovery feature or was destined for financial institutions. In 1998 the Administration further relaxed controls over 56-bit technology generally and stronger encryption destined for U.S. subsidiaries, insurance companies, and other end-users, retreating from earlier key recovery requirements. Further modifications were announced in September 1999, allowing license exceptions for the export of encryption of any key length after a technical review to most end-users in all but terrorist countries; draft regulations were issued in late 1999. Following criticism by companies, privacy groups and Internet proponents, DOC expanded aspects of its original proposal and issued new regulations in January 2000. Regulations issued in October 2000 further streamlined controls over encryption exports to 23 countries including European Member states. Restrictive export licensing regulations have raised constitutional concerns, some arguing that they impose a prior restraint on speech in violation of the First Amendment. Federal courts have both upheld and dismissed First Amendment challenges to export controls, the outcome generally turning on whether the court viewed the encryption item and its export as essentially expressive or functional. Courts in California and Ohio have allowed challenges to proceed, holding that encryption source code is protected speech for First Amendment purposes.

Legislation introduced in the 106th Congress would have required increased liberalization of encryption export controls. **H.R. 850**, the Security and Freedom Through Encryption (SAFE) Act, was reported from the House Judiciary Committee, House Commerce Committee (as amended), and House International Relations Committee (as amended); significantly more restrictive versions of the bill had been reported by the House Armed Services Committee and House Permanent Select Committee on Intelligence (H.Rept. 106-117, Pts 1-5). **S. 798**, the Promote Reliable On-Line Transactions to Encourage Commerce and Trade (PROTECT) Act of 1999, was reported favorably and without amendment by the Senate Commerce Committee (S.Rept. 106-142). No further action was taken on these bills. This report will be updated periodically.

Contents

Encryption Export Controls

This report discusses encryption export controls, beginning with background on the development and use of encryption, and continuing with a description of export controls imposed under the Arms Export Control Act (AECA) and the Export Administration Act (EAA); a discussion of recent federal court rulings in First Amendment challenges to AECA and EAA regulations; and a summary of 106th Congress legislation aimed at liberalizing law and policy affecting encryption exports.

Background

Encryption is a means of scrambling data so that parties may send and receive private messages.[1] It may also be used for authentication (confirming the identity of the sender) and data integrity (ensuring that a message has not been changed in transit). Contemporary encryption is generally based on an algorithm paired with a "key" — usually a string of 40 to 128 bits — which together protect messages from computer-based descrambling by outsiders.

Keys may be secret or public. Under the former, both the sender and the recipient share an identical key. A public key system involves a related pair of keys, one of which is published in a public directory and the other remaining with the sender or recipient. Public key systems are useful for encrypting messages in large and open computer networks such as the Internet, where individual users may not have previous knowledge of one another. Key escrow or recovery systems make it possible for parties other than those who are party to an encrypted conversation or who encrypt data for storage to have access to the secure material. This capability is viewed favorably by law enforcement since key access enables authorities to decrypt so-called "real time" messages without the knowledge or consent of parties to a communication or to decrypt stored data for investigatory purposes. Key escrow or recovery systems may also be of general commercial benefit in the event a key is lost, stolen, or destroyed.

The development and use of strong computerized encryption in the United States was originally limited to the federal government for military and intelligence

---

[1] *See generally* "What Is Cryptography?" *in* Office of Technology Assessment, *Information Security and Privacy in Network Environments* 122 (Box 4-1)(September 1994)[hereinafter cited as OTA Report]. For additional background, *see* CRS Issue Brief IB96039, *Encryption Technology: Congressional Issues.*

applications.[2] Eventually, the increasing use of computers for commercial purposes led to a need for stronger commercial encryption as well. In 1971, IBM completed the development of a cipher code with a 128-bit key, turning it into a marketable product by 1974. At the same time, the federal government began to solicit bids for an encryption algorithm that could be used as a federal standard for storing and transmitting unclassified data – known as a data encryption standard (DES). IBM reportedly responded with a 56-bit key and other modifications after discussions with the National Security Agency (NSA), the federal entity responsible for communications intelligence, which had earlier taken considerable interest in its project. As stated in a Senate report, NSA "certified that ... [the revised IBM cipher] was, to the best of their knowledge, free of any statistical or mathematical weaknesses"[3] and recommended it for use as the new DES.

Critics suggested possible vulnerabilities in the shortened key and pointed out the inherent (and continuing) dilemma in the confrontation of governmental and business interests in the area. One author states that "[s]ince the DES would eventually be manufactured commercially and installed on a wide assortment of equipment sold abroad, the NSA would not want to cut its own throat by permitting the foreign proliferation of an unbreakable cipher. Yet weaknesses in the cipher would still allow the Agency to penetrate every communications link and data bank using the DES, American as well as foreign."[4]

While the current DES is based on a 56-bit key, the National Institute of Standards and Technology (NIST) in 1997 began to develop an Advanced Encryption Standard (AES) with a key length of from 128 to 256-bits.[5] In October 2000, NIST announced its choice for this new AES algorithm – the Rijndael – which will be proposed for incorporation in a new Draft Federal Information Processing Standard (FIPS). Following a public comment period and any subsequent revisions, the

---

[2]The discussion of the development of the data encryption standard in this and the following paragraph is drawn from J. Bamford, *The Puzzle Palace* 427-57 (Penguin 1983)[hereinafter cited as Bamford]; Staff of Senate Select Comm. on Intelligence, 95th Cong., 2d Sess., *Unclassified Summary: Involvement of NSA in the Development of the Data Encryption Standard* (1978)[hereinafter cited as Senate Report]; and *OTA Study*, *supra* note 1, at 122-23.

[3]Senate Report, *supra* note 2, at 4.

[4]Bamford, *supra* note 2, at 437.

[5]*See* 62 Fed. Reg. 48051 (1997). In recent testimony on 106th Congress encryption bills, industry witnesses have stated that the current worldwide standard is 128-bit encryption, described as the minimum strength now required by new Internet applications. Testimony of Ira Rubinstein, Senior Corporate Attorney, Microsoft Corporation, before the House Permanent Select Committee on Intelligence, June 9, 1999, *as reported by* Federal Document Clearing House, *available in* LEXIS, News Library, Curnws File; Testimony of D. James Bidzos, Vice Chair, Security Dynamics Inc., on Behalf of Americans for Computer Privacy, before the Senate Comm. on Commerce, Science and Transportation, June 10, 1999, at 4. The export of some encryption of 128 bits and higher is now allowed by the Commerce Department. *See* text at 7-8, *infra* and Testimony of William A. Reinsch, Under Secretary of Commerce for Export Administration, before the Senate Comm. on Commerce, Science and Transportation, June 10, 1999 [hereinafter cited as Reinsch Testimony] [http://www.bxa.doc.gov/Encryption/archive.htm].

Secretary of Commerce will decide whether to adopt the FIPS as an official government standard.[6]

With the growth of the global economy, the business community has continued to express a need for strong encryption for domestic use and cross-border communications and transactions. While there are no statutory restrictions on the domestic use of encryption, the computer industry argues that restrictive export controls have hampered U.S. technological development since it is impracticable to develop separate products for the domestic and foreign market; that export restrictions will hinder its long-term competitiveness, given the increasing availability of strong foreign cryptography and the projected increase in demand for such products due to the increasing popularity of electronic commerce; and that U.S. interests are harmed by making increasingly strong U.S. encryption unavailable to legitimate users worldwide.[7] At the same time the federal government argues that because of its national security and law enforcement responsibilities it should not facilitate the proliferation of encryption despite its foreign availability and the increasing capability of private computer users to invade encrypted systems.[8] The

---

[6]For additional information on the Rijndael algorithm and the draft Federal Information Processing Standard, see [http://www.nist.gov/aes].

[7]*See, e.g.*, Evans, "U.S. Export Control of Encryption Software: Efforts to Protect National Security Threaten the U.S. Software Industry's Ability to Compete in Foreign Markets," 19 N.C.J. Int'l Law & Com. Reg. 469 (1994). Restrictions on importation and use of encryption in foreign countries may also limit market access. *See, e.g.*, Baker, "Encryption: Shielding Cyberspace," J. of Commerce, July 25, 1995, at 6A. For recent statements of industry concerns, see, *e.g.*, Testimony of Christopher G. Caine, IBM Corporation, House Permanent Select Comm. on Intelligence, Hearing on H.R. 850, June 9, 1999, *as printed by* Federal Document Clearing House, *available in* LEXIS, News Library, Curnws File; Testimony of D. James Bidzos, Vice Chair, Security Dynamics Inc., on Behalf of Americans for Computer Privacy, before the Senate Comm. on Commerce, Science and Transportation, June 10, 1999, at 4.

A U.S. government study released in January 1996 found that U.S. firms faced competition in the security-specific software market in a number of foreign markets from encryption exporters such as the United Kingdom, Germany and Israel, but that, while export controls had limited U.S. market share in 14 countries, controls have had little or no impact in 7 others and had not prevented the U.S. companies from keeping pace with overall foreign market demand. Some smaller U.S. security-specific software firms, however, had found it infeasible to develop a product for domestic use and another for foreign consumption. U.S. Dept. of Commerce and Nat'l Security Agency, *A Study of the International Market for Computer Software with Encryption; prepared for the Interagency Working Group on Encryption and Telecommunications Policy* (1996)(Executive Summary). A recent assessment of foreign availability may be found in a June 1999 study issued by the Cyberspace Policy Institute, George Washington University, Washington. D.C. Hoffman *et al., Growing Development of Foreign Encryption Products in the Face of U.S. Export Regu*lations (June 10, 1999)[www.seas.gwu.edu/~cpi/library/papers.html].

[8]An overview of traditional governmental concerns may be found in 1975 congressional testimony by then-NSA Director Lt. Gen. Lew Allen, Jr. *See* "The National Security Agency and Fourth Amendment Rights" *in Intelligence Activities, Senate Resolution 21; Hearings Before the Senate Select Comm. to Study Government Operations with Respect to*

(continued...)

Administration has advocated the development of a key management infrastructure (KMI), in which third-parties would maintain an extra key to an encrypted system, as an indispensable element of worldwide use of public key encryption.[9] In response to such proposals, business, consumer, and privacy groups have expressed numerous concerns over the governmental role in determining who may hold escrowed keys and over who may obtain access to encrypted transactions and data. The Administration has since deemphasized the use of export controls to foster KMI development.

Current Export Controls over Encryption

Encryption had traditionally been treated as a munition subject to Cold War export restrictions imposed by the Coordinating Committee for Multilateral Export Controls (CoCom). Encryption currently appears both as a munition and a dual-use item on lists maintained by CoCom's successor, the 33-member Wassenaar Arrangement.[10] A Cryptography Note to the dual-use list added in December 1998 requires Wassenaar members to review exports of mass market hardware and encryption with a key length greater than 64 bits in light of their respective export control regimes; this policy replaces the earlier General Software Note, which did not restrict the export of mass market encryption software.[11]

Encryption is subject to U.S. export controls under both the Arms Export Control Act (AECA) and the Export Administration Act of 1979 (EAA). Section 38 of the AECA, 22 U.S.C. § 2778, authorizes the President to control the commercial

---

[8](...continued)
Intelligence, 94th Cong., 1st Sess., v. 5 at 15-24 (1976). For more a more recent discussion, see, for example, Department of Justice testimony before the Senate Commerce Committee during June 10, 1999, hearings on S. 798, the Promote Reliable On-Line Transactions to Encourage Commerce and Trade (PROTECT) Act (Statement of James K. Robinson, Assistant Attorney General, Criminal Division, Department of Justice.

[9]*See The Security and Freedom Through Encryption (SAFE) Act: Hearing on H.R. 695 Before the Subcomm. on Telecommunications, Trade and Consumer Protection of the House Commerce Comm.*, 105th Cong. 54-57 (1997)(prepared statement of William A. Reinsch, Under Secretary of Commerce for Export Administration); *H.R. 695, the Security and Freedom Through Encryption Act: Hearing Held June 30, 1997, House Comm. on National Security*, 105th Cong. 54-62 (1998)(written statement of William P. Crowell, Deputy Director, NSA).

[10]The Wassenaar Arrangement is considerably less strict than CoCom, focusing primarily on the transparency of national export control regimes and not granting veto power to individual members over organizational decisions. *See generally* R. Grimmett, *Military Technology and Conventional Weapons Export Controls: The Wassenaar Arrangement*, CRS Report 95-1196. For added information, see [http:// www.wassenaar.org].

[11]Reinsch Testimony, *supra* note 5. In March 1997, the Organization for Economic Cooperation and Development issued guidelines for national cryptography policies, advocating, among other things, market driven development of cryptographic methods, provision for controlled lawful access to plaintext or keys, privacy protections, clear statements of keyholder liability in contracts or legislation, and international coordination of policies in the area. The guidelines are available at [http://www.oecd.org/dsti/sti/it/secur/index.htm].

export of defense articles and services and to establish a United States Munitions List (USML) delineating these articles. The AECA is administered by the State Department through its Office of Defense Trade Controls (DTC), a sub-unit of the Department's Bureau of Politico-Military Affairs.[12] The Department implements the Act through the International Traffic in Arms Regulations (ITARS), set forth in 22 C.F.R. Parts 120 through 130. Arms exporters must register with the federal government and obtain licenses before items may be exported. The designation of items as defense articles and defense services for regulation under the AECA is not judicially reviewable.[13] Unlike the EAA, the AECA does not require foreign availability to be taken into account in licensing decisions. Section 38 provides the President with strong enforcement authorities and authorizes stringent criminal and civil penalties for those who violate the AECA and its implementing regulations. The NSA has played a role in the licensing process, advising as to the national security impact of an export and examining such factors as the sensitivity of a product and its end users; it has also provided technical advice in the determination of whether an item belongs on the USML.[14]

In implementing the AECA, the State Department may decide that a product is not defense-related and transfer jurisdiction over that item to the Bureau of Export Administration (BXA) of the Department of Commerce (DOC).[15] The Export Administration Act of 1979 (EAA), which was recently reauthorized until August 20, 2001, authorizes the Commerce Department to control exports for national security, foreign policy, and short supply reasons.[16] Items subject to EAA regulation are listed in the Commerce Control List (CCL), 15 C.F.R. § 799.1, Supp. No. 1.

Originally, virtually all encryption was classified as a defense article and regulated under the AECA.[17] In the early 1990's the Department of State had exempted from AECA control nine types of encryption (including smart cards and

---

[12]Further information regarding the Office of Defense Trade Controls may be found at the Office's Internet site: [http://www.pmdtc.org].

[13]Arms Export Control Act (AECA), § 38(h), 22 U.S.C. § 2778(h).

[14]*See* Rubinstein, "Export Controls on Encryption Software" *in Coping with U.S. Export Controls 1996*, at 317-18 (Practicing Law Institute 1996).

[15]An exporter may request the State Department to make a "commodity jursidiction" (CJ) determination if there is doubt as to whether an item is subject to the USML. A CJ request may also be made to the Department to consider redesignating an item currently covered by the USML, a process that may result in transferring the item to Commerce Department jurisdiction. 22 C.F.R. § 120.4.

[16]50 U.S.C. App. §§ 2401 *et seq.* (1994). In the interim between the expiration of the EAA in August 1994 and its reauthorization effective November 13, 2000 (Pub. L. No. 106-508), regulations issued under the Act were maintained under an executive order issued under the International Emergency Economic Powers Act (IEEPA). "Continuation of Export Controls," Executive Order 12924 of August 19, 1994, 59 Fed. Reg. 43437 (1994). IEEPA is set forth at 50 U.S.C. §§ 1701 *et seq.*

[17]Encryption is treated as "Auxiliary Military Equipment" and listed in Category XIII of the USML; technical data and defense services related to these items are regulated as well. 22 U.S.C. § 121.1, Categories XII(b) and XIII(k).

encryption for use in financial transactions) and transferred authority over these items to the Commerce Department.[18] Jurisdiction over encryption exports could also be transferred to DOC for mass market software under an expedited commodity jurisdiction procedure[19] and as a result of case-by-case review.[20] As a general policy, the State Department allowed exports of commercial encryption with 40-bit keys, although some software with DES could be exported to U.S.-controlled subsidiaries and financial institutions.[21]

The Clinton Administration announced a new encryption policy in October 1996, giving DOC jurisdiction over all commercial encryption, though subject to conditions many of which were similar to those imposed under the AECA (*e.g.*, EAA foreign availability provisions were inapplicable).[22] The President's Executive Order made approvals subject to an interagency review process and gave the Justice Department a vote in determining encryption export policy. Key recovery encryption of unlimited key length could be exported as could 56-bit non-recovery encryption if the manufacturer agreed to develop a recovery system within 2 years. In May 1997, DOC eased controls over encryption for financial purposes, announcing that, after a one-time review, it would approve exports of unlimited key length "specifically designed to support financial transactions" and, for 2 years, strong general purpose non-recovery encryption "when used for interbank and similar financial transactions" once producers agreed to develop a recoverable product.[23]

---

[18]Exempted items needed to perform one of the following functions and to be restricted to that function: (1) decryption of copy-protected software; (2) use in machines for banking or money transactions; (3) cryptographic processing using analog functions in certain broadcast and fax equipment; (4) personalized smart cards; (5) access control, such as in ATMs; (6) data authentication; (7) fixed data compression or coding techniques; (8) reception of limited-audience radio or television programs (decryption must be limited to video, audio or management functions; and (9) anti-virus software. 22 C.F.R. § 121.1, Category XIII(b)(1)(i)-(ix)(1995). Manufacturers of a category XIII(b)(1) item that remained under State Department jurisdiction could, however, apply for an export license to make multiple shipments of the item to end users in approved countries without having to obtain individuals licenses for each customer. 22 C.F.R. § 123.16(b)(1), § 124.15 (1995).

[19] 57 Fed. Reg. 32148 (1992). This aspect of the encryption export control regime has ben called the Software Publishers Association (SPA) Agreement. "U.S. Sets Procedures for Easing Controls on Exports of Encoding-Capable Software," 9 Int'l Trade Rep. 1246 (BNA 1992). Regarding commodity jurisdiction procedures, *see supra* note 13 and the Internet site of the Office of Defense Trade Controls [http://www.pmdtc.org].

[20]56 Fed. Reg. 42285 (1991); 57 Fed. Reg. 15227, 15229 (1992). In February 1996, the Department amended its regulations to allow U.S. citizens and lawful permanent residents to temporarily and conditionally export laptop computers with encryption for personal use. 61 Fed. Reg. 6111 (1996).

[21]*See* Rubenstein, *supra* note 14, at 324-25

[22]Exec. Order 12036 of November 15, 1996, 61 Fed. Reg. 58767 (1996); Memorandum on Encryption Export Policy, November 15, 1996, White House Press Release, November 15, 1996. *See also* 61 Fed. Reg. 68633 (1996)(AECA) and 61 Fed. Reg. 65462 (1996)(EAA).

[23]Bureau of Export Administration, "Encryption Exports Approved for Electronic (continued...)

In 1998, the Clinton Administration changed its key recovery policy, allowing the export of 56-bit encryption to all destinations except embargoed/terrorist countries under a license exception after a one-time agency review and without a commitment to produce a key recovery product. While a license exception continued to be available for encryption of unlimited key length that contained a key recovery feature, a requirement that the government pre-approve a key recovery agent was eliminated. In addition, the favorable export treatment previously granted financial institutions was extended to insurance companies, health and medical end-users, and, with some end-use restrictions, on-line merchants. Following a one-time agency review, U.S. companies could also export encryption of any key length for internal company proprietary use to their subsidiaries in all but embargoed destinations. Products of any key length for use by commercial entities in some 45 countries and, for companies headquartered in 22 countries (including the United States), their worldwide subsidiaries located anywhere but in embargoed destinations, were exportable after review. This policy also allowed the export of "recoverable" encryption, that is, encryption that allows access to plaintext by law enforcement and others, but does so without a key recovery feature. The Administration also announced plans to establish a technical support center run by the FBI to provide federal, state, and local law enforcement with the funds and expertise needed to deal with developments in encryption technology.[24]

Further relaxation of encryption export controls took place in September 1999, when the Clinton Administration announced that encryption items of any key length may now be exported under a license exception, after a technical review, to individuals, firms, and other non-government end-users in any country except for seven state supporters of terrorism.[25] After a technical review, retail encryption commodities and software of any key length will also be exportable under a license exception to any recipient in any country except for the same seven destinations. Post-export reporting will be required, however, for any export to a non-U.S. entity of any product over 64 bits. The Administration also announced that it would implement the updated Wassenaar controls, allowing 56-bit DES and equivalent products to be exported without a license to all users and destinations, except the seven terrorist countries, after a technical review. It would also make encryption items of 64-bits or less that meet the mass market requirements of the Wassenaar cryptographic note eligible for export without a license after a technical review. The Clinton Administration further announced that foreign nationals working in the United States will no longer need to obtain an export license in order to work on encryption

---

[23](...continued)
Commerce," Press Release, May 8, 1997, BXA-97-12 [http://www.bxa.doc.gov/Encryption/archive.htm].

[24]Regulations are set forth at 15 C.F.R. Parts 740, 742, 743, 772, 774 (1999). For additional details, *see* 63 Fed. Reg. 72156 (1998); White House briefing on new encryption policy, September 16, 1998 [http://www.pub.whitehouse.gov]. *See generally* Baker & Banker, "The New Encryption Export Policy: The U.S. Government Rethinks Key Recovery," *in Coping with U.S. Export Controls 1998,* 782 PLI/Comm 589, *available in* WESTLAW, JLR File.

[25]"Administration Updates Encryption Export Policy; Fact Sheet," September 16, 1999 [http://www.pub.whitehouse.gov]; "Administration Eases Encryption Curbs, Sends Congress Plan to Permit Key Recovery," 16 Int'l Trade Rep. 1510 (BNA 1999).

for U.S. firms. Following criticism by companies, privacy groups, and Internet proponents, the Administration postponed publication of the implementing regulations and expanded certain aspects of the earlier proposal in new rules that were issued January 14, 2000.[26] Among other things, DOC broadened the encryption license exception as it applies to source code; expanded the meaning of "retail" to include the provision of encryption through mail order, electronic, or telephone call transactions; and made the encryption license exception available for exports to government entities that are telecommunications companies and Internet service providers, so long as the export does not involve a non-retail product that will be used to provide services specific to government end-users.

Concurrent with the Clinton Administration's announcement was the President's proposal of the Cyberspace Electronic Security Act of 1999, which would set forth limitations on the government's use and disclosure of encryption keys obtained under court order, address the disclosure and use of stored recovery information by recovery agents for governmental purposes, and authorize appropriations for the FBI's Technical Support Center.[27]

On July 17, 2000, the Clinton Administration announced that it would further streamline controls for encryption exports to 23 countries, including European Union member states, removing distinctions between government and non-government end users and generally eliminating the 30-day waiting period following the exporter's submission of a classification request.[28] Implementing regulations were issued October 19, 2000.[29]

First Amendment Issues

Because AECA regulations treat the disclosure of encryption software and technical data to a foreign person as an export, strict AECA penalties could apply to individuals who discuss developments in advanced cryptography at domestic

---

[26] "Revisions to Encryption Items; Interim final rule; request for comments," 65 Fed. Reg. 2492 (2000); Department of Commerce, Bureau of Export Administration, "Administration Updates Encryption Export Policy; Fact Sheet," January 12, 2000; "U.S. Eases Tight Government Restrictions on Exports of Strong Encryption Items," 68 U.S.L.W. 2424 (BNA 2000).

[27] 145 Cong. Rec. H8390-91 (daily ed. Sept. 21, 1999). The legislation is contained in H.Doc. 106-123.

[28] "Assuring Security and Trust in Cyberspace," July 17, 2000 [http://www.pub.whitehouse.gov].

[29] "Revisions to Encryption Items; Final rule," 65 Fed. Reg. 62600 (2000). The new rule also revises and clarifies the January 14, 2000 regulations, "including changes in the treatment of products incorporating short-range wireless technologies, open cryptographic interfaces, beta test software, encryption source code, and U.S. content (*de minimis*) requirements." *Id.* Additionally, the rule "allows, for the first time, exporters to self-classify unilateral [sic] controlled encryption products" falling under certain export control classification numbers "upon notification to the Bureau of Export Administration." *Id.* For additional information on the new regulations, see [http://www.bxa.doc.gov/Encrption/Default.htm].

conferences attended by foreign persons and over computer networks with foreign participants without first obtaining an export license.[30] It has been argued that these aspects of the AECA — and now EAA — regulatory regime constitute a prior restraint of protected speech in violation of the First Amendment.[31] Federal district courts addressing this issue over the last three years have both upheld and dismissed First Amendment challenges to export licensing schemes for encryption. In the first circuit court opinion issued during this period, the Court of Appeals for the Ninth Circuit, on May 8, 1999, affirmed a lower court ruling striking Department of Commerce regulations as an unconstitutional prior restraint.[32]

---

[30]In late 1995, the Justice Department terminated a controversial criminal investigation of Philip Zimmerman, who had developed the public key encryption system known as Pretty Good Privacy and made it freely available in this country. "Data-Secrecy Export Case Dropped by U.S.," *N.Y.Times*, Jan. 12, 1996, at D1. The question of possible AECA violations arose after the program was reportedly transmitted overseas via the Internet by another.

Current Commerce Department regulations address the issue of "exporting" encryption data via computer systems by providing, at 15 C.F.R. § 734.2(b)(9), that the export of controlled encryption source code and object code software includes:

> downloading, or causing the downloading of, such software to locations (including electronic bulleting boards, Internet file transfer protocol, and World Wide Web sites) outside the U.S. (except Canada), or making such software available for transfer outside the United States (except Canada), over wire, cable, radio, electromagnetic, photo optical, photoelectric or other comparable communications facilities to persons outside the United States (except Canada), including transfers from electronic bulletin boards, Internet file transfer protocol and World Wide Web sites, unless the person takes precautions adequate to prevent unauthorized transfer of such code outside the United States or Canada.

The regulations further provide that these precautions must include "ensuring that the facility from which the software is available controls the access to and transfers of such software" and describe measures that will accomplish this.

[31]*See, e.g.*, Greenspoon, "U.S. Government Control over the Export of Scientific Research and Other Technical Data: Holes in the Sieve," 16 Mich. J. Int'l L. 583 (1995), and articles listed in Froomkin, "The Metaphor is the Key: Cryptography, the Clipper Chip and the Constitution," 143 U. Pa. L. Rev. 709, 748, n. 162 (1995).

First Amendment concerns had been raised in a 1981 Justice Department memorandum opinion prepared for the State Department with respect to ITAR technical data revisions. The opinion stated in summary that "insofar as ... [the proposed licensing requirement] could be applied to persons who have no connection with any foreign enterprise, who disseminate technical data in circumstances in which there is no more than a belief or a reasonable basis for believing that the data might be taken abroad by foreign nationals and used there in the manufacture of arms, the licensing requirement is presumptively unconstitutional as a prior restraint on speech protected by the First Amendment." 5 Op. Off. Legal Counsel 202 (1985).

[32]Earlier, a federal appeals court had held that the application of Mutual Security Act export controls to technical assistance and data relating to a tape wiring program was constitutionally permissible under the First Amendment. United States v. Edler, 579 F.2d 516 (9th Cir. 1978). The statute at issue authorized the President to control the "export and import of arms, ammunition, and implements of war, including technical data relating thereto" (22 U.S.C. §

(continued...)

Court challenges have generally involved restrictions on the export of software containing encryption source code — that is, computer programming language describing an encryption program or an algorithm. This original programming language must be combined or translated into object code, which enables a computer to read the encryption program.[33] Distinctions are generally raised between the expressive and functional nature of the software at issue, and between the act of exporting software containing encryption source code and the use of source code to communicate. In his 1996 Executive Order, the President expressly stated that "the export of encryption software, like the export of other encryption described in ... [the order], must be controlled because of such software's functional capacity, rather than because of any possible information value of such software."[34] At the same time, it is argued that, regardless of the functional capability of software, the source code it contains is a language by which cryptographers convey mathematical ideas to each other and, as such, merits the strongest First Amendment protection.

Bernstein Cases

In *Bernstein v. Dep't of State,* a California federal district court, ruling on a government motion to dismiss, held that source code constituted speech protected by the First Amendment.[35] The court later ruled that AECA licensing requirements were an unconstitutional prior restraint on such speech.[36] The plaintiff subsequently challenged the 1996 DOC regulations on First Amendment grounds, the court holding these unconstitutional as well and enjoining their application to the plaintiff.[37] The injunction was stayed pending appeal. The Court of Appeals for the Ninth Circuit, in a 2-1 ruling, affirmed the district court's decision May 9, 1999, allowing a facial First Amendment challenge to the Commerce Department regulations and holding that the regulations were in fact an impermissible prior restraint.[38] On September 30, 1999, the Ninth Circuit granted the United States its motion for a rehearing before the

---

[32](...continued)
1934(a)(1970)). The court construed the law and its accompanying regulations narrowly, finding that they prohibited "only the exportation of technical data significantly and directly related to specific items on the U.S. Munitions List." 579 F.2d at 521. The Mutual Security Act provision in force when the appealed export violation occurred was repealed in 1976 and replaced by § 38 of the Arms Export Control Act .

[33]Commerce Department export control regulations define "source code" as "a convenient expression of one or more processes that may be turned by a programming system into equipment executable object code." 15 C.F.R. Part 772. The regulations define "object code" as "an equipment executable form of a convenient expression of one or more processes ("source code" (or source language) that has been converted by a programming system." *Id.*

[34]Exec. Order 12036, *supra* note 23, §1(c).

[35]Bernstein v. Dep't of State, 922 F.Supp. 1426 (N.D.Cal. 1996).

[36]Bernstein v. Dep't of State, 945 F. Supp. 1279 (N.D.Cal. 1996).

[37]Bernstein v. Dep't of State, 974 F. Supp. 1288 (N.D.Cal. 1997).

[38]Bernstein v. U.S. Dep't of Justice *et al.*, 176 F.3d 1132 (9th Cir. 1999). A facial challenge would allow the plaintiff to avoid applying for a license before challenging the scheme and to champion the rights of those not before the court.

full court of appeals and withdrew the earlier opinion.[39] The case was later remanded to the original three-judge panel on January 26, 2000, for reconsideration in light of DOC's new encryption regulations.[40] Plaintiff since requested an advisory opinion from DOC and, in February 2000, the Department reportedly notified him in writing that, under the new regulations, he may post source code for his encryption software on his Internet Web site.[41]

The Ninth Circuit three-judge panel had reviewed the district court *Bernstein* ruling *de novo* and held that the two-prong test for facial challenges set forth by the Supreme Court in *Lakewood v. Plain Dealer Publishing Co*., 486 U.S. 750 (1988), was met. As explained by the court, a licensing scheme is always subject to a facial challenge if, as described in *Lakewood*, it "'gives a government official or agency substantial power to discriminate based on the content or viewpoint of speech by suppressing disfavored speech or disliked speakers,' and has 'a close enough nexus to expression, or to conduct commonly associated with expression, to pose a real and substantial threat of ... censorship risks.'" [42] The court held that the first requirement was satisfied because the constraint on official discretion contained in the standard used by the Commerce Department to deny export licenses under the Export Regulations (EAR) — namely, inconsistency with "U.S. national security and foreign policy interests"[43] — was, in the court's view, "little better than no constraint at all."[44] The court discounted government arguments that the scheme was content-neutral, finding that finding that the agency's "boundless discretion" (as it was later described by the court) made DOC's assurances that it would not discriminate on the basis of content irrelevant [45]

The second requirement for facial challenges was fulfilled because, in the court's view, the regulations evidenced a "close enough nexus to expression." The court determined at the outset that "encryption software, in its source code form and as employed by those in the field of cryptography, must be viewed as expressive for First Amendment purposes, and thus is entitled to the protections of the prior restraint doctrine."[46] The court dismissed the government's argument that, even admitting the expressive nature of source code, its functional aspect — that is, by being compiled into "object code," it can be used to control the operations of a computer without

---

[39]"Court to reconsider ruling on encryption controls," AP State & Local Wire, Sept. 30, 1999, *available in* LEXIS, News Library, Curnws File.

[40]"Ninth Circuit Remands Encryption Case in Light of Recently Revised Encryption Policy," 17 Int'l Trade Rep. 204 (BNA 2000).

[41]"U.S. Lets Scientist Post Source Code for Encryption Software on Web Site," Wall St. J., Feb. 25, 2000, at B6.

[42]176 F.3d at 1139, *quoting* 486 U.S. 750, 759 (1988).

[43]176 F.3d 1139, *quoting* 15 C.F.R. § 742.15(b), the regulation setting forth the Commerce Department's licensing policy for encryption items.

[44]176 F.3d at 1139.

[45]*Id.*

[46]*Id.* at 1141.

conveying information to the user — obviated First Amendment problems in this case.[47] It also dismissed the government's argument that because the regulations were "laws of general application" and did not narrowly and specifically target speech, prior restraint analysis did not apply. Again relying on *Lakewood*, the court held that the Commerce Department regulations "explicitly apply to expression and place scientific expression under the censor's eye on a regular basis," distinguishing them, for example, from a building permit requirement, which would give officials "only intermittent and unpredictable opportunities" to regulate speech.[48]

The court then held the regulations to be an impermissible prior restraint, finding none of the elements needed to uphold the validity of licensing schemes, as set forth by the Supreme Court in *Freedman v. Maryland*, 380 U.S. 541 (1965), to be present in this case. As summarized by the court, a licensing scheme that imposed a prior restraint on speech would survive under *Freedman* if: (1) any restraint on speech were for a specified period of time; (2) there was expeditious judicial review; and (3) the censor bore the burden of going to court to suppress the speech and bore the burden of proof in any such judicial proceeding.[49] The court found that the requisite procedural safeguards were lacking because neither the Executive Branch process for resolving inter-agency disputes over export license applications, nor the internal appeals process for license denials contained firm deadlines, and further, the licensing process did not afford judicial review to those whose export license applications were denied.[50]

With respect to the scope of declaratory relief, the government argued that the lower court's order was invalid since it applied not only to encryption source code, but also to encryption object code, commodities, and technology. Agreeing with the government that the EAR could be "conceptually severed into component parts covering commodities, software and technology," the court nonetheless decided that the "integrated structure"of the regulations did not permit it to sever the judicially uncontested portions of the regulations and let the lower court relief stand.[51]

The dissenting judge in *Bernstein* concluded that since the EAR was a law of general application directed at conduct, the plaintiff did not meet the requirements for a facial First Amendment challenge. The dissent emphasized that the majority and the district court had paid insufficient attention to the functional aspects of encryption.[52]

---

[47]*Id.* at 1142.

[48]*Id.*

[49]*Id.* at 1144.

[50]*Id.* at 1145-46.

[51]*Id.* at 1146-47. The court stated that it had "neither the power nor the capacity to engage in line by line revisions of the challenged regulations or to redefine terms within the regulations. ... To do so would be to improperly invade the province reserved to the Executive." *Id.* at 1147 (citations omitted).

[52]*Id.* In his separate opinion, the concurring judge stated that he recognized the validity of the dissent's view regarding the functional purpose of source code and the First Amendment

(continued...)

Even though source code could be used expressively, the dissent argued that it was "inherently a functional device" and that, for purposes of First Amendment analysis, it was nearer to conduct than to speech.[53] Referring to the Ninth Circuit's 1996 decision in *Roulette v. City of Seattle*, 97 F.3d 300, which had quoted *Lakewood*, the dissent stated that "such an approach ignores the basic tenet that facial challenges are inappropriate 'unless at a minimum,'" the challenged statute is, in *Lakewood's* words "directed narrowly and specifically at expression or conduct commonly associated with expression."[54] The dissent found that the conduct at issue here was the export of encryption source code, noting that "the overwhelming majority" of individuals do not use source code as means of expression but rather as a means of protecting their computer communications.[55] In such case, "[e]xport of encryption source code simply does not fall withing the bounds of conduct commonly associated with expression such as picketing or handbilling."[56] The dissent further maintained that the EAR regulate encryption technology generally, whether in the form of hardware or software, and as such were directed at preventing the functional capability of encryption to be exported without a license.[57] In the dissent's view, the fact that the regulations were not directed at expression was supported by the fact that the regulations did not prevent the print publication of scholarly articles containing source code.[58] While the dissenting judge found that the plaintiff did not meet the requirements for a facial challenge, he acknowledged that a First Amendment claim with regard to the regulations as applied may nonetheless succeed in this case.[59]

Karn v. Dep't of State

First Amendment issues also arose in *Karn v. Dep't of State*, a case brought in the U.S. District Court for the District of Columbia in which plaintiff challenged the State Department's disapproval of the export of a diskette containing source code for encryption algorithms, while allowing the export of a book containing the same.[60] Along with his First Amendment claim, the plaintiff sought judicial review of the State Department's initial designation of the diskette as a "defense article" for purposes of the AECA, and also challenged the regulation on Fifth Amendment due process grounds. While the court rejected the plaintiff's request for judicial review of the

---

[52](...continued)
implications of this approach, and noted that "[t]he importance of this case suggests that it may be appropriate for review by the United States Supreme Court." *Id.*

[53]*Id.* at 1148.

[54]*Id.* at 1149.

[55]*Id.*

[56]*Id.*

[57]*Id.*

[58]*Id.*

[59]*Id.* at 1149-50.

[60]Karn v. Dep't of State, 925 F.Supp. 1 (D.D.C. 1996).

agency's classification decisions,[61] it allowed him to pursue his constitutional claims, though it ultimately dismissed these as well.[62] With regard to First Amendment arguments, the court held that the diskette was content-neutral and met the First Amendment test applicable to governmental regulation of such items set forth by the Supreme Court in *United States v. O'Brien*. The court also rejected plaintiff's prior restraint argument against the Department's technical data regulations.[63]

In the court's view, the content-neutrality of the AECA regulations was clearly evidenced by the fact that the government was "not regulating the exports of the diskette because of the expressive content of the comments [interspersed through the source code] and or source code, but instead are regulating because of the belief that the combination of encryption source code on machine readable media will make it easier for foreign intelligence sources to encode their communications."[64] As summarized by the court, a challenged regulation will be upheld under *O'Brien* if "it is within the constitutional power of the government, it 'furthers an important or substantial government interest,' and 'the incidental restriction on alleged First Amendment freedoms is no greater than is essential to the furtherance of that interest.'"[65]

While the plaintiff did not expressly or impliedly dispute that the first two *O'Brien* conditions were satisfied, he argued that the third element was lacking

---

[61]The court rejected plaintiff's initial request for judicial review on the ground that the § 38(h) of the AECA, 22 U.S.C. § 2778(h), expressly precluded such review and that Administrative Procedure Act (APA) judicial review provisions allowing challenges to agency actions on the ground that they are "arbitrary and capricious" could not be invoked as a substitute. 925 F.Supp. at 4-8, 13.

[62]The court found that, by arguing that his Fifth Amendment substantive due process rights were violated by the Department's action, the plaintiff was in fact attempting to revive his earlier-rejected APA claim through another vehicle, an action that the court found "would render the judicial review preclusion in § 2778(h) absolutely meaningless." 925 F.Supp. at 13. The court held that AECA regulation bore a reasonable relationship to the government's stated purpose, as required by the Fifth Amendment substantive due process standard applicable in cases where, as here, there was no assertion that a fundamental right was being infringed. *Id*.

[63]The court held that the plaintiff's did not have standing to claim that AECA regulations governing the export of "technical data" were an "'unconstitutional system of vague prior restraints,'" given that the State Department did not apply these regulations to him and there was thus no causal connection between these provisions and the plaintiff's injury. 925 F.Supp. at 12-13. In this regard, the court noted that "[w]hile courts have departed from traditional rules of standing with respect to certain First Amendment claims, claims of facial overbreadth and vagueness are rarely entertained with respect to content-neutral regulations." *Id.* at 13. The court also found that the Department had in fact limited the application of its technical data regulations in response to *United States v. Edler Industries*, a 1978 Ninth Circuit decision in which the court found the regulatory definition of "technical data" to be susceptible of overbreadth, but interpreted the statute narrowly to avoid a finding of unconstitutionality. *Id.* Regarding *United States v. Edler, see supra* note 28.

[64]*Id.* at 10.

[65]*Id.* at 11, *quoting* O'Brien v. United States, 391 U.S. 367, 377 (1988).

because, as summarized by the court, "the cryptographic algorithms contained on the Karn diskette are 'already widely available in other countries [through the Internet and other sources] or are so "weak" that they can be broken by the [National Security Agency].'"[66] The court held that the regulation was in fact narrowly tailored to meet its goal. Noting that this argument also implicated the second *O'Brien* requirement, the court held that plaintiff's disagreement with the government essentially involved a foreign policy dispute and thus "not one into which this Court can or will delve."[67] In the court's view, classifying encryption items as defense articles reflected the President's foreign policy judgment that proliferation of encryption products was harmful to the United States, a judgment that existed despite any argued availability or capability of the regulated items.[68] The court also rejected the plaintiff's request for judicial balancing of First Amendment harms against national security interests and found that the plaintiff had not presented any arguments that the regulation was substantially broader than was necessary to prevent proliferation of encryption products.[69]

Following issuance of the opinion and the 1996 jurisdictional shift, the plaintiff sought and was denied an export license by the Department of Commerce. He subsequently pursued his case in the district court, which recently ordered an evidentiary hearing on his constitutional claims. The hearing is limited to the question whether, for the purposes of producing an operating encryption system, material differences existed between the plaintiff's diskette and the corresponding source codes appearing in printed form.[70]

Junger v. Daley

A result that conflicted with the *Bernstein* cases but comported with *Karn* was reached in the 1998 decision of the U.S. District Court for the Northern District of Ohio in *Junger v. Daley*, which rejected a First Amendment challenge to DOC regulations.[71] In April 2000, the U.S. Court of Appeals for the Sixth Circuit reversed, holding that computer source code was protected by the First Amendment, and remanded the case to the district court for consideration of the plaintiff's constitutional challenge.[72]

Plaintiff Junger was a law professor who wanted to post encryption programs on his Internet site, an action the DOC treated as a export. The Department had informed him that he would need export licenses for software programs, but that a chapter in one of his textbooks containing encryption code could be exported without

---

[66]925 F.Supp. at 11, *quoting* Plaint's Opp. 15-16.

[67]925 F.Supp. at 11.

[68]*Id.*

[69]*Id.* at 12.

[70]Karn v. Dep't of State, Civ. A. No. 95-1812-LFO (D.D.C. Feb. 18, 1999).

[71]Junger v. Daley, 8 F.Supp.2d 708 (N.D.Ohio 1998).

[72]Junger v. Daley, 209 F.3d 481 (6th Cir. 2000).

a license. The plaintiff did not apply for export licenses for these items, but instead brought a First Amendment challenge to the regulations, claiming a prior restraint on speech, vagueness and overbreadth, unconstitutional content discrimination, and infringement of rights to freedom of association and discussion.[73] The court found that source code was "inherently functional" and thus its export was not sufficiently communicative to constitute protected conduct under the First Amendment; rejected plaintiff's facial challenges to the DOC regulations on grounds of prior restraint, vagueness and overbreadth;[74] and sustained the regulations under the intermediate First Amendment scrutiny applicable to governmental restrictions deemed content-neutral set forth in *O'Brien.*[75]

On appeal, the Sixth Circuit concluded that "computer source code is an expressive means for the exchange of information and ideas about computer programming," held that source code thus merited First Amendment protection, and allowed the plaintiff to proceed with his facial challenge of the DOC regulations.[76] The court held out the possibility that intermediate First Amendment scrutiny might apply, stating that the functional capabilities of source code should be considered when analyzing the government's interest in regulating this form of speech, but also noted that in such a case "the government 'must demonstrate that the recited harms are real, not merely conjectural, and that the regulation will in fact alleviate these harms in a direct and material way.'"[77] While the court acknowledged that the government's national security interests might outweigh those of protected speech, and require its regulation, it stated that the record to date had not resolved the issue

---

[73]Because plaintiff's claims of infringement of academic freedom and freedom of association were not pursued in briefs, the court considered them waived. 8 F.Supp.2d at 723. The plaintiff also argued that the International Emergency Economic Powers Act (IEEPA), under which the President had extended expired export control authorities in 1994, did not authorize the regulation of encryption exports because encryption was "informational material," a category of goods that was statutorily excluded from regulation from IEEPA. The court held that this action was unreviewable because the IEEPA committed any regulation of exports under it to the President's discretion; moreover, the court noted, the President's decision to use IEEPA to regulate trade was consistently held unreviewable by courts. *Id.* at 723.

[74]Quoting the *Lakewood* standard used by *Bernstein* majority and referring to the *Roulette* refinement cited by the Bernstein dissent, the court stated that for a facial challenge to be allowed, the disputed measure must not merely affect expressive conduct, but must be "'directed narrowly and specifically at expression or conduct commonly associated with expression.'" *Id.* at 718. The court found these requirements to be lacking since the exportation of the software was not integral to expression and that the expressive elements of software exportation were not directly or narrowly targeted: all types of encryption devices were regulated and, moreover, academic discussion and descriptions of software in print media were allowed. *Id.* at 718-719.

[75] The court held that the *O'Brien* test was met because: (1) an important government interest existed in controlling the export of encryption for national security purposes; (2) the regulations were not designed to limit the free exchange of ideas, but were imposed because of the encryption's functionality; and (3) the regulations "were targeted at precisely the activity that threatens the government legitimate interests."

[76] 209 F.3d at 485.

[77] *Id., quoting* Turner Broadcasting System v. FCC, 512 U.S. 622, 644 (1994).

in this case.[78] The court allowed the plaintiff to proceed with his constitutional challenge, directing the district court to examine the new encryption regulations issued in January 2000 to examine whether the plaintiff could bring a facial challenge on First Amendment grounds.

106th Congress Legislative Proposals

Two bills introduced in the 106th Congress, **H.R. 850 and S. 798**, would have relaxed controls on encryption exports along with addressing other encryption issues. A third bill, **S. 854**, did not expressly address export issues, but had implications for the use of encryption abroad and for government approvals that are conditioned on the use of key escrow or key recovery systems.

H.R. 850, the Security and Freedom Through Encryption (SAFE) Act, introduced February 25 by Mr. Goodlatte and 204 (later 258) co-sponsors, expanded upon H.R. 695, a 105th Congress version of the SAFE Act that had been strongly supported by industry.[79] **S. 798**, the Promote Reliable On-Line Transactions to Encourage Commerce and Trade (PROTECT) Act, was introduced April 14, 1999, by Mr. McCain and 5 (later 7) co-sponsors. Mr. McCain had sponsored an encryption bill in the 105th Congress (S. 909) that sought to relax encryption export controls, but would have given the executive branch greater leeway to impose restrictions than would be possible under S. 798. The Clinton Administration had opposed the introduced version of H.R. 695, but generally favored H.R. 909. While both H.R. 850 and S. 798 were supported by industry, the Clinton Administration stated its opposition to each.[80]

H.R. 850 was reported by the House Judiciary Committee, the House Commerce Committee, the House International Relations Committee, the House Armed Service Committee, and the House Permanent Select Committee on Intelligence, resulting in differing versions of the bill, two of which would allow strict export controls on encryption. The House Rules Committee was to determine which version of the bill would be presented for floor action. S. 798 was ordered reported favorably and without amendment June 23 by the Senate Commerce Committee, the only committee to which the bill was referred.

No further action was taken on any of these bills.

---

[78]209 F.3d at 485.

[79]H.R. 695 was reported without amendment from the House Judiciary Committee and and the House International Relations Committees, but was made more restrictive by the House National Security Committee and the House Permanent Select Committee on Intelligence.

[80]"Administration Says SAFE Act Threatens Law Enforcement, Security," 16 Int'l Trade Rep. 417 (BNA 1999); "Administration Opposes Senate Encryption Export Bill, Calls Review Panel 'Unworkable,'" 16 Int'l Trade Rep. 1002 (BNA 1999).

H.R. 850, as Introduced and Reported

H.R. 850, as introduced, would have amended the Export Administration Act of 1979 to grant the Secretary of Commerce sole authority over nonmilitary encryption. After a one-time 15-day technical review (meaning a review to determine that the item works as represented), the Secretary could no longer have required an export license for a wide variety of encryption hardware and software, except pursuant to the Trading with the Enemy Act (TWEA) or IEEPA. The Secretary would also have been required, after a one-time 15-day technical review, to permit the export of strong encryption for nonmilitary end uses (1) in countries to which certain financially-related encryption could then be exported, unless there was substantial evidence that the item would be diverted to a military end use or an end use supporting international terrorism, modified for military or terrorist end use, or reexported without any U.S. authorization that might be required under the EAA, or (2) if he determined that comparable encryption was commercially available abroad from a foreign supplier without effective restrictions. The Secretary could not have reinstated export controls on encryption items that were decontrolled as of the date of enactment, but could have prohibited the export of specific encryption products to an individual or organization in a specific foreign country if there was substantial evidence that the item was destined for terrorist or military end-uses. In addition, the President would have been allowed to prohibit the export of encryption products to terrorist countries or as part of an embargo under the IEEPA, the Trading with the Enemy Act (TWEA) or the EAA.

Regarding the sale and use of encryption generally, the bill would have, among other things, made it lawful for any U.S. person in a foreign country to use any encryption, regardless of the encryption algorithm selected, encryption key length chosen, or implementation technique or medium used, excepting encryption activities undertaken in the commission of a felony under a U.S. criminal statute. A U.S. person would have included a U.S. citizen, a U.S. firm, and a foreign firm owned or controlled by U.S. citizens or firms. The bill would have also prohibited the Federal Government from requiring key escrow capabilities in encryption products or conditioning any approval on the existence of such capabilities.

The **House Judiciary Committee**, which did not address export issues, reported the bill April 27 (H.Rept. 106-117, Part 1). The **House Commerce Committee** reported the bill as amended July 2 (H.Rept. 106-117, Part 2). The Commerce Committee version added provisions that would have required the Assistant Secretary of Commerce for Communications and Information and the National Telecommunications and Information Administration (NTIA) to issue regulations within 90 days of enactment identifying which products under DOC jurisdiction were designed for improvement of network security, network reliability, or data security ("critical infrastructure protection products"). Regarding products so identified, it would have also delegated to these agencies by 2 years after enactment all authority regarding export determinations and technical reviews that the Act delegated to the Secretary. The amended version would have also expanded the 15-day technical review periods to 30 "working days"; required DOC to consult with the Secretaries of Defense and State, the Attorney General, and the Director of Central Intelligence before the licensing policies provided for in the bill took effect; allowed DOC to prohibit exports of strong encryption and specific encryption

products to end users in specific countries for the additional reasons of harm to U.S. national security, use in sexual exploitation of minors, or use in illegal activities involving organized crime; and provided that encryption products could be controlled for any reason other than their encryption capability and that nothing in the SAFE Act or its amendment of the EAA altered the ability of the Secretary of Commerce to control exports for reasons other than encryption.

This version also added provisions that would have created a National Electronic Technologies Center to assist law enforcement in developing and maintaining encryption capabilities; required the Secretary of Commerce to undertake export promotion activities for encryption products; directed the President to begin negotiating international agreements to facilitate encryption trade and provide for mutual recognition of countries' export controls (allowing the President to consider a country's refusal to negotiate when considering U.S. participation in any cooperation or assistance program with that country); and criminalized transfers of over 56-bit encryption products to the People's Liberation Army and other military end users in the People's Republic of China (PRC).

The **House Committee on International Relations** reported the bill as amended July 19, 1999 (H.Rept. 106-117, Part 3). This reported version would have, among other things, expanded the 15-day technical review periods to 30 "working days"; required DOC to consult with the Secretaries of Defense and State, the Attorney General, and the Director of Central Intelligence before the licensing policies provided for in the bill took effect; required the Secretary, before approving an encryption export or re-export to a major drug-transit country or major illicit drug-producing country, to consult with the Attorney General, the FBI Director, and the Administrator of the Drug Enforcement Administration regarding the impact of the export or re-export on the flow of illicit drugs into the United States (but would not have authorized the prohibition of an export or a license denial solely because the destination was one of these countries); and provided that nothing in the SAFE Act limited the President's authority under IEEPA, TWEA, or the EAA, to prohibit the export or reexport of over 56-bit encryption to any PRC military unit.

The amended bill would have also expanded the reasons for which the Secretary could make specific export denials by adding the facilitation of illicit drug imports into the United States, the manufacture of weapons of mass destruction or assistance in the proliferation of such weapons, and illegal activities involving sexual exploitation of minors; required the Secretary to consult with the Secretaries of Defense and State, the Attorney General, the FBI Director, the Administrator of the Drug Enforcement Administration, and the Director of Central Intelligence before making such decisions; and changed the evidentiary standard for such decisions from "substantial" to "credible. The committee version also provided that encryption products would be subject to export controls imposed for any reason other than their encryption capability (including export controls imposed on high performance computers) and that nothing in the SAFE Act or its amendment of the EAA altered the ability of the Secretary of Commerce to control exports for reasons other than encryption capabilities.

The **House Committee on Armed Services** reported a rewritten version of H.R. 850 on July 21 in the form of an amendment in the nature of a substitute (H.Rept.

106-117, Part 4).[81] The amendment, which did not address the domestic sale or use of encryption, would have renamed the bill the "Protection of National Security and Public Safety Act"; given the President sole authority to control the export of all dual-use encryption products; authorized the President to deny the export of any encryption product on the basis that its export is contrary to U.S. national security interests; and prohibited judicial review of any presidential or presidentially-delegated encryption export decision under the Act.

The amendment would have allowed the export of encryption under licenses and license exceptions depending on encryption strength. The President would have been required to notify Congress, within 180 days of enactment, of the maximum level of encryption strength that could be exported under a license exception without harm to U.S. national security interests. It would have made an encryption product that did not exceed this level eligible for an export license exception, provided (1) the product was submitted for a one-time technical review (with required information to be determined by the President); (2) the item did not require licensing under otherwise applicable regulations; (3) the item was not intended for a country, end user, or end use that was by regulation ineligible to receive the product and the encryption was otherwise qualified for export; and (4) the exporter, at the time the product was submitted for technical review, provided the names and addresses of its distribution chain partners. After his initial notification, the President would have been required to continue to inform Congress of the encryption strength for license exceptions every subsequent 180 days, and could no longer decrease this level.

A license would have been required for the export of any encryption products designed or manufactured within the United States with an encryption strength that exceeded the license-exception level. The license applicant would have needed to submit the product for technical review, to certify the intended end use and expected end user of the product, to provide information regarding a distribution chain partner if the export was being made to such an entity, and to submit any other information required by the President. The amendment would also have required post-export reporting by an exporter who had reason to believe that an exported product was diverted to unauthorized end uses or end users, and required all exporters and distribution chain partners of such exporters to submit a report to the Secretary specifying the particular product sold, the name and address of the end user of the product, and the intended end use of the product.

This committee amendment would have authorized the President to waive provisions regarding license exceptions if he determined that the waiver was necessary to protect U.S. national security interests and reported to Congress regarding any such waiver. It would also have authorized the President to waive the licensing requirement for stronger encryption for specific classes of end users identified as being eligible for receipt of encryption commodities and software under the current license exception for encryption in 15 C.F.R. § 740.17, and required him to report to Congress on any such waiver. The committee amendment would also have created a public-private Encryption Industry and Information Security Board to advise the

---

[81] Amendment in the Nature of a Substitute to H.R. 850 Offered by Mr. Weldon of Pennsylvania, Mr. Sisisky, and Mr. Andrews.

President on the foreign availability of encryption products and required the Secretary of Commerce to conduct a market share survey of foreign markets for encryption products at least once every 6 months.

The **House Permanent Select Committee on Intelligence** July 23 reported an amendment to H.R. 850 in the nature of a substitute, retitling the bill the Encryption for the National Interest Act (H.Rept. 106-117, Part 5). With regard to general export authorities, this version, similar to that reported by the House Armed Services Committee amendment, would have given the President sole authority to control the export of all dual-use encryption products; authorized the President to deny the export of any encryption product on the basis that its export was contrary to U.S. national security interests; and prohibited judicial review of any presidential or presidentially-delegated encryption export decision under the Act based on national security.

The amendment would also have required a system of export licenses and license exceptions. An encryption product of 64 bits or less would have been eligible for a license exception, provided (1) the product was submitted for a one-time technical review (a maximum 45-day process with required information to be determined by the President); (2) the item did not require licensing under otherwise applicable regulations; (3) the item was not intended for a country, end user, or end use that was by regulation ineligible to receive the product and the encryption was otherwise qualified for export; (4) the exporter, within 180 days after export, submitted a certification identifying the intended end use of the products and the name and address of the intended recipient, if available; (5) the exporter, within 180 days after export, provided the names and addresses of its distribution chain partners; and (6) the exporter, at the time the product was submitted for technical review, provided proof that its distribution chain partners had contractually agreed to abide by all U.S. laws and regulations involving the export or reexport of U.S.-origin encryption products. It would also have allowed license exceptions for the export of an encryption product whether or not the product contained a method of decrypting encrypted data.[82] The committee version would have required the President periodically to review the encryption strength that could be exported under the license exception without harm to U.S. national security, but would not have allowed him to reduce the level from 64 bits.

The amendment would have allowed the President to grant a license for the export of any encryption product designed or manufactured within the United States with an encryption strength that exceeded the license-exception level under the following conditions: (1) a requirement that the product contain a method of gaining timely access to plaintext or decryption information may not be imposed as a condition of the license; (2) the products must be submitted for technical review; (3) the exporter must submit a certification identifying the intended end use and the expected end user or class or end users of the product; (4) the exporter must provide proof that its distribution chain partners have contractually agreed to abide by all U.S.

---

[82]With regard to this provision (§ 302(d)), the Committee report states that "there is no requirement that recoverability features be included in the product for the section [on license exceptions] to apply."

laws and regulations involving the export and reexport of U.S.-origin encryption products; and (5) the exporter must submit the names and addresses of the distribution chain. The bill also provided for post-export reporting by the exporter of possible unauthorized diversions, pirating, and encryption sales by distribution chain partners. Notwithstanding the provision for licenses, the President would have been permitted to allow exports under a license exception for higher level encryption if the export was consistent with national security.

The amended version would also have required the President to provide for expedited review of commodity classification requests and export license applications involving encryption items; allowed the Secretary of Commerce, the Secretary of Defense and the Secretary of State to use their existing statutory authorities to carry out the export provisions of the bill; and granted the President judicially unreviewable authority to waive the bill's export requirements if he determined that the waiver was "necessary to advance the national security."

The committee amendment would have created a public-private Encryption Industry and Information Security Board to advise the President on a variety of issues involving encryption, including the benefits and risks of globally-distributed strong encryption, the advancement of international standards for encryption products, and availability and market share of foreign encryption and their threat to U.S. industry. It also contained a sense of the Congress provision exhorting the President to negotiate international agreements establishing binding export control requirements on strong nonrecoverable encryption products that safeguard the privacy of U.S. citizens, prevent economic espionage, and enhance U.S. information security needs, and allowed the President to consider a country's refusal to negotiate such agreements when considering U.S. participation in any cooperation or assistance program with that country.

In addition, this committee bill addressed the domestic use of encryption, government procurement, and liability limitations for persons disclosing or providing plaintext of encrypted data, decryption information, or technical assistance.

S. 798, as Introduced and Reported

S.. 798, as introduced April 14, 1999 and reported, would have granted the Secretary of Commerce sole authority over nonmilitary encryption exports, requiring him to exercise his authority in consultation with the Secretaries of Defense and State. It would have allowed the President to use his TWEA and IEEPA authorities (1) to prohibit the export of encryption to a country, corporation, or other entity determined to support terrorism or to pose an immediate threat to national security and (2) to impose a trade embargo with respect to a specific country, corporation or entity. The Secretary of Commerce could also have prohibited the export of particular encryption to particular foreign individuals or organizations if there was substantial evidence that the encryption might be used or modified for military or terrorist use. Export controls on encryption would also have been allowed if the control was imposed for reasons other than encryption capability.

The bill would have decontrolled encryption of up to 64 bits and required license exceptions for recoverable products, encryption destined for certain commercial end-

users and governments of NATO, OECD, and ASEAN countries, technology with interface mechanisms, and related technical assistance or data. Products would have been eligible for an exception after a one-time technical review; the request for the exception (including the review) was to be completed within 15 working days. The bill would also have permitted exports of stronger encryption under a license exception if the Secretary of Commerce determined that the product was exportable under the EAA or a new public-private Encryption Export Advisory Board determined (and the Secretary agreed) that such products were generally or publicly available, or a comparable product would soon be available abroad (subject to presidential override on national security grounds). While a decision by the Secretary to disapprove an availability finding by the advisory board would have been subject to judicial review, a presidential national security override would not have been. A technical review and 15-day processing period would also have applied to these items. In addition, DOC license approvals for over 64-bit encryption would have been grandfathered.

The bill would have directed the National Institute of Standards and Technology to adopt an Advanced Encryption Standard by January 1, 2002, after which time the Secretary of Commerce could no longer impose encryption export controls on items that incorporated the new standard or an equivalent. These goods would be exportable without restrictions, except for those restrictions permitted under the bill. The bill would also have prohibited the Secretary of Commerce from taking actions that had the effect of imposing government-designed encryption standards on the private sector by restricting encryption exports and from imposing any reporting requirements on encryption products that were not subject to export controls or license exceptions.

S. 798 also contained provisions regarding the domestic use of encryption, government procurement, the development of the Advanced Encryption Standard (in addition those described above), and the improvement of the government's technological capability.

S. 864, as Introduced

While not primarily focused on export controls, S. 854, the Electronic Rights for the 21st Century Act, introduced April 21 by Mr. Leahy and referred to the Senate Committee on the Judiciary, would have made it lawful for any U.S. 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 (§ 201(a)). It would also have generally prohibited government-mandated key escrow or key recovery by not allowing any U.S. agency, among other things, to "condition any approval" on certain requirements involving a decryption key, access to a decryption key, key recovery information, or other plaintext access capability (§ 201(b)).