DEMYSTIFYING U.S. ENCRYPTION EXPORT CONTROLS

JAMES B. ALTMAN*
WILLIAM MCGLONE**

TABLE OF CONTENTS

* S.B., Physics, *Massachusetts Institute of Technology* (1971); M.S., Physics, *Massachusetts Institute of Technology* (1975); J.D., *Boalt Hall, University of California, Berkeley* (1978); Member of the law firm of Miller & Chevalier, Chartered.

** A.B., History, *Harvard University* (1982); J.D., *Georgetown University Law Center* (1987); Member of the law firm of Miller & Chevalier, Chartered.

Messrs. Altman and McGlone are members of Miller & Chevalier's International Practice Group. Their practice includes counseling U.S. and foreign clients on compliance with U.S. export control laws.

INTRODUCTION

For nearly half a century, the U.S. government has maintained strict controls on exports of cryptographic products and technology.[1] With the coming of the "information age"—and the accompanying explosive need for and development of information security products—these controls have become increasingly visible and contentious.[2] Where only a handful of products and companies were affected by these controls just ten years ago, today virtually every high-technology company and multinational business is caught, to some degree, by encryption export controls.

U.S. controls on exports of cryptographic products and technology are highly complex, restrictive, and controversial. American exporters routinely complain that encryption export controls place them at a severe competitive disadvantage, citing as evidence a burdensome licensing process and the loss of business to foreign competitors that purportedly are subject to less stringent export regulation. At the other end of the spectrum, the law enforcement and national security communities insist that strict export controls are an essential tool in the battle against the growing threat of international crime and terrorism.

Thus, the encryption export control debate is being driven by complex and seemingly irreconcilable policy objectives, including privacy and First Amendment concerns, commercial efforts to protect proprietary business information, and, of course, law enforcement and national security concerns. The purpose of this Essay is neither to criticize nor to endorse U.S. controls on encryption exports. Rather, this Essay attempts to add to the legal and policy debate by offering practical insights on the export control framework and the policy tensions underlying the controls.

[1] *See infra* notes 8-40 and accompanying text (discussing U.S. cryptographic export regulations); *see also* Kenneth J. Pierce, *Public Cryptography, Arms Export Controls, and the First Amendment: A Need for Legislation,* 17 CORNELL INT'L L.J. 197, 201-02 (stating that National Security Agency ("NSA") was established in 1952 largely to control cryptologic services). In 1975, the NSA attempted to stop all federal grants for cryptology research. *See id.* at 203. The NSA now controls all grants to cryptology research. *See id.* at 204.

[2] *See generally* Lance J. Hoffman et al., *Cryptography Policy,* 37 COMMUNICATIONS OF THE ACM 109 (1994); Jill M. Ryan, Note, *Freedom to Speak Unintelligibly: The First Amendment Implications of Government-Controlled Encryption,* 4 WM. & MARY BILL RTS. J. 1165, 1167 (1996) (stating that encryption software is essential to protect mass amounts of personal, financial, and business related data transmitted through insecure channels); Peter H. Lewis, *Between a Hacker and a Hard Place: Data-Security Export Law Puts Businesses in a Bind,* N.Y. TIMES, Apr. 10, 1995, at D1.

Part I identifies the growing commercial needs for strong encryption in the ever-shrinking global marketplace. Part II discusses the scope, structure, and effect of current U.S. encryption export controls and licensing requirements. Part III surveys a number of initiatives—legal, political, and commercial—intended to liberalize encryption export controls. Finally, Part IV considers the competing policy concerns that will continue to shape litigation and the debate about the future course of encryption export controls.

I. INFORMATION SECURITY NEEDS AND COMPETITIVE PRESSURES ON U.S. INDUSTRY

It is axiomatic that secure electronic communication is essential to compete in today's international marketplace. As U.S. companies continue to expand their business operations around the world, they often need to exchange sensitive information with foreign branches, joint venture partners, subsidiaries, subcontractors, product suppliers, and customers. They must be able to communicate securely about those activities, often on a real-time basis. These business realities require more extensive and increasingly sophisticated electronic communication—by fax, telephone, videophone, computer network, etc. For this mode of business operation to remain viable, however, companies must be confident that the communications will remain secure and confidential.

Today's level of information security is, if anything, the tip of the proverbial iceberg. Until recently, most companies used relatively rudimentary cryptography for a limited number of purposes.[3] That is no longer satisfactory. U.S. and foreign companies now are in the process of moving to a much broader use of more powerful cryptography—either as a result of customer demand, for their own commercial protection, or both.[4] These companies include software develop-

[3] At its most fundamental level, encryption is the scrambling of information—whether in the form of data, text, or video signals. In general, encryption is accomplished with a "key." Although not necessarily true, for our purposes, it is sufficient to assume that the "security" of an encryption algorithm depends essentially on its key length. *See* BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY: PROTOCOLS, ALGORITHMS, AND SOURCE CODE IN C, at xix (2d ed. 1996) (providing introduction to encryption and describing various uses for information security); RSA Laboratories, *FAQ* 3.0 (visited Jan. 29, 1997) <http://www.rsa.com/rsalabs/faq/faq_toc.html> (on file with *The American University Law Review*).

[4] *See* Kenneth W. Dam & Herbert S. Lin, *National Cryptography Policy for the Information Age*, ISSUES IN SCI. & TECH., Summer 1996, at 33; A. Michael Froomkin, *The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709, 718 (1995) (noting that with new advances in communications technology, many businesses are concerned about data security).

ers producing security products that use encryption;[5] businesses and financial institutions that increasingly need to offer strong encryption capabilities in their software;[6] and telecommunications equipment and service providers that seek to encrypt transmissions or to offer encryption capabilities to their customers.[7]

II. U.S. EXPORT LICENSING REQUIREMENTS[8]

Over the years, we have observed a number of misconceptions about the scope and reach of encryption export controls. All of the following statements are at least partially inaccurate:

- No products with encryption capabilities may be exported.
- Products with encryption routines with 40-bit keys or less are not subject to licensing requirements.
- Products with encryption routines exceeding 40-bit key-lengths are not exportable under any circumstances.
- Products using the DES algorithm cannot be exported.
- Other countries do not control exports of encryption.

[5] *See* SCHNEIER, *supra* note 3, at 561-94 (outlining real-world applications of secured information and explaining encryption hardware and software).

[6] *See, e.g.*, *id.* at 584-85 (describing security-oriented software program that secures electronic mail).

[7] *See id.* at 594-95. One example of a telecommunications company offering encryption-capable hardware to its customers is AT&T and its Telephone Security Device ("TSD") Clipper Phone. *See id.* To prevent interception of a communication by a third party, the TSD generates a unique signal that only the TSD at the other end of the line can decipher. *See id.*

[8] As this Essay was going to print in December 1996, the regulations governing exports of cryptographic products and technology were undergoing substantial revision. On December 13, 1996, the Clinton Administration implemented part of its "key recovery" proposal in the form of an interim final rule issued by the Commerce Department's Bureau of Export Administration. *See* 61 Fed. Reg. 65,462 (1996). In a separate but related development, Commerce Department officials announced their intention to publish a rule by the end of December that would transfer regulatory jurisdiction over commercial encryption exports from the State Department's Office of Defense Trade Controls to the Commerce Department's Bureau of Export Administration. *See id.*

Assuming that such a jurisdictional transfer occurs, commercial encryption exports will be governed by the Commerce Department's Export Administration Regulations rather than by the State Department's International Traffic in Arms Regulations. As a result, the references in the discussion below to the International Traffic in Arms Regulations will become obsolete. Nonetheless, we expect that the Commerce Department will adopt virtually all of the rules and interpretations discussed below. In other words, although the governing regulations and agencies will change, the basic export licensing requirements and policies are expected to remain essentially the same.

That being said, there will be a few significant differences under the new regulatory regime. First, the new regulations will allow encryption products that meet "key recovery" criteria (as determined by the Commerce Department) to be exported without an export license, regardless of algorithm or key length. Second, companies that persuade the Commerce Department that they are moving toward the development of such "key recovery" products will be eligible—at least temporarily—for liberal export licensing treatment with respect to other encryption products with a key length of up to 56-bits. Third, although the NSA will continue to play a major role in shaping encryption export policy, the Justice Department and the Federal Bureau of Investigation will, for the first time, participate in export licensing decisions.

- An individual license is required for every export.

To dispel these misconceptions, the following discussion explains how U.S. export controls actually work, both in terms of what types of products are controlled and of the nature of the export licensing process.

A. *Scope of Export Controls*

U.S. controls on exports of "information security" are exceedingly broad. The term "information security" is defined to include any technique that leaves data or text in a form that is not readable.[9] Controls apply to exports of hardware, software, and related technology.[10] Although the controls do not apply to general scientific or engineering principles commonly taught in schools or to information in the public domain,[11] they do apply to virtually all information and products that are treated as proprietary.[12]

The controls apply to all "exports" from the United States to any foreign country.[13] This includes the situation in which an engineer instinctively stashes some floppy disks in his or her coat pocket and departs the United States without realizing he or she has just exported the software, in possible violation of U.S. law.[14] The term "export" also includes transfers of technology to any "foreign national" in the United States.[15] The term "foreign national" includes any person who is neither a citizen nor a permanent resident alien (i.e., green card holder) of the United States, even if the person holds an H-1 visa or the equivalent. In addition, the controls apply

[9] *See* Export Administration Regulations ("EAR"), 61 Fed. Reg. 12,714, 12,930 (1996) (to be codified at 15 C.F.R. pt. 772) (defining "information security" as "[a]ll the means and functions ensuring the accessibility, confidentiality or integrity of information or communications").

[10] *See generally* International Traffic in Arms Regulations ("ITAR"), 22 C.F.R. pts. 120-130 (1996) (regulating export and import of certain defense-related articles and services). For an outline of U.S. rules that govern the exportation of cryptographic products, see SCHNEIER, *supra* note 3, at 610-17.

[11] *See* 22 C.F.R. § 120.10(a)(5).

[12] *See* EAR, 61 Fed. Reg. at 12,747 (to be codified at 15 C.F.R. § 734.3(b)(3)(i)) (exempting from EAR control "publicly available" technology and software that are published or will be published); *id.* at 12,749 (to be codified at 15 C.F.R. § 734.7(b)) ("Software and information is published when it is available for general distribution either for free or at a price that does not exceed the cost of reproduction and distribution.").

[13] *See* 22 C.F.R. § 120.17(a) (defining "export" as "sending or taking a defense article out of the United States in any manner"); 15 C.F.R. pt. 772 (defining "export" as "an actual shipment or transmission of items out of the United States").

[14] *See* SCHNEIER, *supra* note 3, at 610 (warning of grave consequences of exporting protected information without proper license). *But see* 22 C.F.R. § 123.27 (permitting temporary export of cryptographic hardware and software by U.S. citizen without export license).

[15] *See* 22 C.F.R. § 120.17(a)(4).

to re-exports of U.S.-origin products and technology from one foreign country to another.[16]

B. Agency Jurisdiction

The State Department's International Traffic in Arms Regulations ("ITAR")[17] regulate the export of defense articles, technology, and services under the statutory authority of the Arms Export Control Act.[18] Items are controlled by the ITAR if they are described in the U.S. Munitions List, which is contained in the ITAR.[19] These regulations, which are administered and enforced by the State Department's Office of Defense Trade Controls,[20] impose an export licensing requirement for the export of every item that is listed on the Munitions List.[21]

Separately, the Commerce Department's Bureau of Export Administration regulates the export of so-called "dual-use" commodities and technical data through a complex set of rules set forth in the Export Administration Regulations ("EAR").[22] The term "dual-use" refers to items that have both a civilian and a military application.[23] In general terms, the export control jurisdiction of the EAR extends to all products that are not designated on the Munitions List and that therefore are not subject to ITAR control.[24]

Until recently, products with cryptographic features or capabilities have been subject to the exclusive export control jurisdiction of the ITAR. Today, most types of encryption software, technical data, and hardware still are controlled by the ITAR under Category XIII of the Munitions List.[25] Through the implementation of regulatory exceptions, however, the State Department has waived its jurisdiction over certain categories of those items and now permits the Commerce Department to regulate those excepted products.[26]

[16] *See id.* § 120.16.

[17] *Id.* pts. 120-130.

[18] 22 U.S.C. § 2778(a)(1) (1994).

[19] *See* 22 C.F.R. pt. 121.

[20] *See id.* § 120.1(a).

[21] *See id.* § 123.1 (imposing licensing requirement for export of defense articles).

[22] 61 Fed. Reg. 12,714-13,041 (to be codified at 15 C.F.R. pts. 730-774).

[23] *See id.* at 12,735 (to be codified at 15 C.F.R. § 730.3); *see also* 15 C.F.R. pt. 774 (providing Commerce Control List ("CCL") of commodities covered by EAR).

[24] *See* 61 Fed. Reg. 12,714, 12,747 (to be codified at 15 C.F.R. § 734.3(b)(1)(i)) (noting that exports included on U.S. Munitions List are not controlled by Bureau of Export Administration); *see also* 22 C.F.R. § 121.1 (listing defense articles, services, and related technical data controlled by ITAR).

[25] 22 C.F.R. § 121.1 cat. XIII(b).

[26] *See id.* § 121.1 cat. XIII(b)(1)(i)-(ix) (excepting enumerated "cryptographic equipment and software" from ITAR).

The National Security Agency ("NSA") historically has played the lead role in shaping encryption export control policy. Charged with deciphering and monitoring international communications, the NSA has the largest stake and the greatest technical expertise of any U.S. government office in the area of cryptography.[27] Accordingly, the State Department relies almost entirely on the NSA to determine what products are subject to a licensing requirement and the licensing policy for such items.[28] To fulfill its mission, of course, the NSA needs to be able to decrypt or "crack" encoded messages. Because there are no restrictions on the sale and use of encryption domestically, controls on exports represent the only effective way for the NSA to limit the level of encryption technology that is deployed overseas. The inherent limitation of this approach is that it does not reach encryption products and technology that are developed overseas and therefore not subject to U.S. export controls.

C. ITAR Controls on Cryptographic Products

As noted above, exports of products with the capacity to encrypt or decrypt information generally are governed by the ITAR.[29] Specifically, Category XIII of the U.S. Munitions List, set forth in Part 121 of these regulations, covers "Information Security Systems and equipment, cryptographic devices, software, and components specifically designed or modified therefor, including: (1) Cryptographic . . . software with the capability of maintaining secrecy or confidentiality of information or information systems."[30] If a particular product falls within this description, it is—subject to the exceptions discussed below—deemed a "defense article" and therefore falls within the ITAR export licensing regime.[31] In that event, the product will require prior export approval from the State Department's Office of Defense Trade Controls.[32]

[27] Although the NSA's primary interest is in its ability to monitor global communications, especially those of foreign militaries and potential terrorists, it also recognizes the United States' interest in preserving the global activities and leadership of its companies and financial institutions.

[28] In some cases, the State Department will override an NSA recommendation for licensing approval, particularly if it has foreign policy concerns about the country of destination or problems with the end-user of the proposed export. These issues often arise in the context of proposed exports to China.

[29] *See supra* note 24 and accompanying text.

[30] 22 C.F.R. § 121.1 cat. XIII(b)(1).

[31] *See id.* § 120.1(a) (stating that purpose of ITAR is "to control the export and import of defense articles and defense services"); *see also id.* § 120.6 (defining "defense article" for purposes of ITAR).

[32] *See id.* § 123.1(a).

The general rule of State Department jurisdiction, however, is subject to certain exceptions. Of the total of nine exceptions currently set forth in the ITAR,[33] five are used most commonly. First, the *Banking or Money Transactions Exception* applies to products that are

> [s]pecifically designed, developed or modified for use in machines for banking or money transactions, and restricted to use only in such transactions. Machines for banking or money transactions include automatic teller machines, self-service statement printers, point of sale terminals or equipment for the encryption of interbanking transactions.[34]

Second, the *Access Control Exception* encompasses products with information security

> [l]imited to access control, such as automatic teller machines, self-service statement printers or point of sale terminals, which protects password or personal identification numbers (PIN) or similar data to prevent unauthorized access to facilities but does not allow encryption of files or text, except as directly related to the password of [sic] PIN protection.[35]

Third, the *Data Authentication Exception* covers encryption products that are

> [l]imited to data authentication which calculates a Message Authentication Code (MAC) or similar result to ensure no alteration of text has taken place, or to authenticate users, but does not allow for encryption of data, text or other media other than that needed for the authentication.[36]

Fourth, the *Data Compression Exception* applies to information security products that are "[r]estricted to fixed data compression or coding techniques."[37] Fifth, the *Restricted Broadcast Exception* covers products "[l]imited to receiving for radio broadcast, pay television or similar restricted audience television of the consumer type, without digital encryption and where digital decryption is limited to the video, audio or management functions."[38] Any product that falls within one or more of these exceptions is subject to the export control jurisdiction of the Commerce Department rather than of the State Department.[39]

[33] *See id.* § 121.1 cat. XIII(b)(1)(i)-(ix).

[34] *Id.* § 121.1 cat. XIII(b)(1)(ii).

[35] *Id.* § 121.1 cat. XIII(b)(1)(v).

[36] *Id.* § 121.1 cat. XIII(b)(1)(vi).

[37] *Id.* § 121.1 cat. XIII(b)(1).

[38] *Id.*

[39] *See* 61 Fed. Reg. 12,714, 13,004 (1996) (to be codified at 15 C.F.R. pt. 774, cat. 5(II)) (listing information security equipment and software controlled by EAR).

The regulatory exceptions to Category XIII make no reference to the relative sophistication or complexity of the encryption routine. Because they are "algorithm-neutral," the availability of the exceptions hinges on the purpose and function of the encryption rather than on the specific algorithm being used. Nevertheless, the NSA and the Department of Commerce typically will inquire about the level of encryption used in a particular product; incorporating an unusually high level of encryption for a relatively simple function could suggest that the encryption in fact is intended for other, unauthorized uses beyond the scope of the exceptions.

In addition, the regulatory exceptions do not apply a "foreign availability" test. That is, the regulations provide no exception for cryptographic software readily available overseas or on the Internet. Thus, if a cryptographic product fails to satisfy one of the exceptions, the export licensing requirement applies regardless of whether the product is widely and easily available outside the United States.

D. *EAR Controls*

Under the EAR, most types of software with a cryptographic function that are exempt from ITAR control fall under Export Control Classification Number ("ECCN") 5D002(c) of the Commerce Control List ("CCL").[40] In the case of software controlled under ECCN 5D002(c), an individual export license is not required if the software qualifies under the relevant Advisory Notes.[41]

III. PROPOSED CHANGES TO ENCRYPTION EXPORT CONTROLS

U.S. controls on encryption exports have been under increasing attack in recent years. U.S. exporters—from software developers to financial institutions to computer and telecommunications companies—routinely criticize encryption export controls for being too restrictive and cumbersome, as well as for being ineffective given the growing availability of competing products overseas.[42] Principally in response to this groundswell of industry opposition, Congress and—to a far lesser degree—the Clinton Administration have proposed a number of reforms to the export control framework.

[40] *See id.* at 13,005 (to be codified at 15 C.F.R. pt. 774, supp. 1) (listing information security software as item on Commerce Control List ("CCL")).

[41] *See id.* (excepting from EAR export licensing requirement cryptographic software needed for use of certain equipment, such as automated teller machines, data authentication devices, and machines used for banking or money transactions).

[42] *See* Stephan Barlas, *Key Decisions Likely on Encryption Exports*, IEEE SOFTWARE, Nov. 1996, at 102; *New Administration Encryption Paper Sparks Industry Criticism*, INSIDE U.S. TRADE, May 24, 1996, at 1, 26-27 [hereinafter *Encryption Paper*].

A. *Key Management Proposals*

The Clinton Administration's key management initiatives have evolved considerably since the "clipper chip" was proposed in April 1993.[43] The history and details of these proposals are chronicled in the various Internet cites of organizations that have been following this issue.[44]

In early October 1996, the Administration announced a new "key management" or "key recovery" initiative.[45] As currently proposed, this initiative will provide favorable export licensing treatment to companies that submit plans to develop key recovery products within a two-year period beginning on January 1, 1997.[46] During that two-year period, companies that obtain "general license" approvals from the Commerce Department will be authorized to export non-key recovery products with up to 56-bit key lengths.[47] Although the government has not yet issued criteria for key recovery products, their critical features will allow a government agency, in appropriate circumstances, to obtain the key to a particular identified communication.[48]

In addition, the Administration has announced that it will shift export licensing jurisdiction for encryption products from the State Department to the Commerce Department.[49] This shift in licensing jurisdiction will require both agencies to amend their regulations, but—standing alone—it will not result in major changes in licensing

[43] *See* SCHNEIER, *supra* note 3, at 591 ("The Clipper Chip . . . is an NSA-designed, tamper-resistant . . . chip designed for encrypting voice conversations; it is one of the two chips that implements the U.S. government's Escrowed Encryption Standard (EES). . . . The chip implements . . . an NSA-designed classified secret-key encryption algorithm.").

[44] *See, e.g.*, Center for Democracy and Technology (last modified Jan. 29, 1997) <http://www.cdt.org> (on file with *The American University Law Review*); Electronic Frontier Foundation, *EFFweb* (visited Jan. 29, 1997) <http://www.eff.org> (on file with *The American University Law Review*); Electronic Privacy Information Center Homepage (last modified Jan. 25, 1997) <http://www.epic.org> (on file with *The American University Law Review*).

[45] *See* Exec. Order No. 13,026, 61 Fed. Reg. 58,767 (1996); Statement of the Vice President on Encryption (Oct. 1, 1996) (on file with *The American University Law Review*); *Administration Offers New Plan to Ease Encryption Export Controls*, INSIDE U.S. TRADE, Oct. 4, 1996, at 8 [hereinafter *New Plan*].

[46] *See New Plan*, *supra* note 45, at 8; Statement of the Vice President on Encryption, *supra* note 45.

[47] *Id.*

[48] The Clinton Administration is seeking to convince foreign governments to adopt a key management approach on a multilateral basis. Thus far, efforts to develop multilateral rules for controlling encryption are under consideration within the "Group of Seven" industrialized countries and the Organization for Economic Cooperation and Development. *See* BIAC/ICC Joint Discussion Paper on International Cryptography Guidelines (Apr. 25, 1996) (on file with *The American University Law Review*); *G-7, In Its Effort to Contain Terrorism, Appears Ready to Regulate Encryption*, 13 Int'l Trade Rep. (BNA) No. 32, at 1268, 1269 (Aug. 7, 1996).

[49] *See supra* note 8.

policies. The NSA will continue to play a major role in shaping encryption export licensing policy. Moreover, for the first time, the Justice Department and the FBI in particular will participate in individual export licensing decisions in response to requests received by the Commerce Department. Reflecting the increasing concerns of the domestic law enforcement community regarding encryption, this use of export controls to serve a domestic law enforcement interest is a new and controversial development.

The key management concept has generated strong opposition from the exporting community.[50] On one level, industry is concerned that customers—particularly foreign customers—will reject any product that offers U.S. government access, regardless of Fourth Amendment or other protections. Would a French company accept a software product that could give a U.S. entity access to its keys? Would a U.S. company accept such a product if French companies, the French government, or both potentially could access its keys?

On another level, there is a growing consensus that the proposed 56-bit key length would not allow a sufficient level of security in today's marketplace. A panel of distinguished cryptographers and computer scientists recently concluded that 56-bit keys are increasingly inadequate and recommended a minimum key-length of 90-bits for non-public key systems and a key-length of ten or more times that for public key systems.[51]

The Administration's proposal nonetheless may hold some promise for certain companies and industry sectors. IBM, Apple, Digital Equipment, Hewlett-Packard, Sun, and others have formed a coalition to develop a key recovery system that will meet the Administration's criteria.[52] The potential appeal of key recovery is based on the premise that a company or a financial institution that develops and controls its own software might even prefer to have a key recovery ability in its software. That capability would allow it to trace improper activity if necessary.

Other companies and industry sectors, however, do not benefit from the Administration's proposal and are "extremely unhappy" with

[50] *See Encryption Paper*, *supra* note 42, at 30; *Key Senators Attack New Administration Encryption Policy*, INSIDE U.S. TRADE, Oct. 18, 1996, at 9.

[51] *See* Matt Blaze et al., *Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security: A Report by an Ad Hoc Group of Cryptographers and Computer Scientists* (last modifiedJan. 1996) <http://www.bsa.org/policy/encryption/cryptographers.html> (on file with *The American University Law Review*).

[52] *See New Plan*, *supra* note 45, at 1; Michael Moeller, *IBM Boosts Encryption Initiative*, P.C. WEEK, Sept. 16, 1996, *available in* 1996 WL 12549915.

it.[53] Moreover, it is not at all clear how key management could be applied to uses such as the Internet. Would Microsoft, Netscape, and every other Internet provider wishing to provide a decent level of security be required to track keys for every Internet message? Likewise, companies producing voice communication products have indicated that they have no interest in attempting to develop key recovery products.[54]

B. *Foreign Availability and Commerce Department/NSA Study*

Even if the Clinton Administration's key management proposal were otherwise satisfactory, it soon may be too little and too late. The realities of the international marketplace quickly are catching up with the government's ability to control cryptographic technology. Foreign software manufacturers increasingly are developing and offering reliable, high-level cryptographic products.

In January 1996, the Commerce Department and the NSA released a joint study on the international market for encryption software.[55] Although the report found that the U.S. industry still dominates the world market for software encryption products, it noted that competing foreign products do exist and that controls on U.S. exports can have a negative effect on U.S. competitiveness.[56]

Critics of the study charge that it significantly understates the adverse competitive effects of the controls. In particular, these critics assert that the study does not adequately address the "first-mover" effect.[57]

[53] *See New Plan*, *supra* note 45, at 1.

[54] *See id.* at 22-23.

[55] DEPARTMENT OF COMMERCE & NATIONAL SECURITY AGENCY, A STUDY OF THE INTERNATIONAL MARKET FOR COMPUTER SOFTWARE WITH ENCRYPTION [hereinafter *Commerce/NSA Study*] (on file with *The American University Law Review*); *see also* Neal Weinberg, *Industry Groups Seek to Secure "Cyberproperty"*, COMPUTER WORLD, Jan. 22, 1996, at 12 (noting that Clinton Administration has proposed that government would retain spare set of "code-breaking keys" in exchange for permitting further use of cryptographic software); Dinah Zeiger, *Brown to Urge Easing Export Controls on Encryption Software*, DENV. POST, Jan. 13, 1996, at E1 (reporting that Commerce Department's position on cryptography indicates that Clinton Administration intends to loosen controls on cryptographic software).

[56] *See Commerce/NSA Study*, *supra* note 55, at III-7, 8; *see also* Zeiger, *supra* note 55, at E1 (noting that past controls have stifled market for encryption software).

[57] The "first-mover" effect, sometimes referred to as a "headstart" or "pioneer" effect, describes the advantage that can be obtained by a company that is the first to the market with a new or better product. *See generally* RALPH E. BIGGADIKE, CORPORATE DIVERSIFICATION: ENTRY, STRATEGY, AND PERFORMANCE (1979); William T. Robinson et al., *First-Mover Advantages from Pioneering New Markets: A Survey of Empirical Evidence*, 9 REV. INDUS. ORG. 1, 15 (1994); F. M. Scherer, *First-Mover Advantages from Pioneering New Markets: Comment*, 9 REV. INDUS. ORG. 173 (1994); Richard Schmalensee, *Product Differentiation: Advantages in Pioneering Brands*, 72 AM. ECON. REV. 349 (1982).

As relevant here, the first-mover effect suggests that so long as U.S. software companies are considered to be reliable sources of sufficiently strong cryptographic software, it will be hard for foreign companies to break into the market for such software. Who wants to buy software of

U.S. industry has seized and expanded on the concerns expressed in the Commerce Department/NSA study. In a separate report,[58] also issued in January 1996, a number of CEOs of technology companies[59] concluded that current U.S. export controls threaten to harm significantly the U.S. computer industry as well as the banking, telecommunications, pharmaceutical, and other sectors.[60] The CEOs highlighted the growing demand for global security solutions that they claim "sharply" contrast with current U.S. policies restricting the availability of U.S. solutions in international markets.[61] They argued that the Internet (the "Global Information Infrastructure") offers unprecedented business and individual opportunities, but that it will need security features.[62] "[W]ith or without U.S. government intervention," they asserted, the need for encryption "will inevitably be met by better cryptographic products."[63]

Recent articles in the trade press confirm this trend. For example, RSA Data Security, Inc., the dominant U.S. supplier of encryption software, has announced that it will begin producing full-strength encryption software in China, which currently has no export controls.[64] The Apache Group, based in the United Kingdom, advertises that U.S. companies cannot match the 128-bit encryption capability in its Unix Internet Server software.[65] Similarly, Nippon Telephone and Telegraph has indicated that it will be exporting triple-DES chips.[66]

uncertain strength if a known, adequate product already is available? In fact, the first-mover effect can be even stronger if the software product becomes a de facto standard. If Microsoft and Netscape were to agree on a cryptographic standard for the Internet, their standard would become virtually impossible to compete against. However, if U.S. export controls prevent U.S. companies from maintaining their first-mover advantage, foreign companies will be able to compete, or even to seize the first-mover advantage for themselves. At that point, U.S. companies will be placed at a severe competitive disadvantage or may find themselves locked out completely.

[58] Computer Systems Policy Project, *Perspective on Society in the Information Age* (visited Nov. 13, 1996) <http://www.cspp.org/reports/reportl-96.html> (on file with *The American University Law Review*).

[59] *See* Computer Systems Policy Project, *Computer Systems Policy Project Home Page* (visited Nov. 13, 1996) <http://www.cspp.org/index.html> (on file with *The American University Law Review*) (stating that Computer Systems Policy Project is organization made up of CEOs of Apple, Compaq, Data General, Digital Equipment, Hewlett-Packard, IBM, NCR, Silicon Graphics, Stratus Computer, Sun Microsystems, Tandem, and Unisys). The goal of the organization is to "develop and advocate public policy positions on current trade and technology issues." *Id.*

[60] *See Computer Systems Policy Project Report*, *supra* note 58.

[61] *See id.*

[62] *See id.*

[63] *See id.*

[64] *See* Don Clark, *China, U.S. Firm Challenge U.S. on Encryption-Software Exports*, WALL ST. J., Feb. 8, 1996, at A10.

[65] *See* Barlas, *supra* note 42, at 102-03.

[66] *See id.*

C. *National Research Council Report*

On May 30, 1996, the National Research Council released a report that has further fueled the push for export liberalization. The congressionally-mandated report, entitled "Cryptography's Role in Securing the Information Society,"[67] challenged the aggressiveness of the government's push for key escrow and underscored the need for strong encryption to ensure confidentiality, provide reliable user authentication, and detect unauthorized tampering with electronic data.[68] The report recommended the ready exportation of products with up to 56-bit key lengths and called for streamlining export licensing requirements.[69]

D. *Proposed Legislation*

Exporters' calls for easing encryption export controls have found a voice in Congress. During the 104th Congress, three bills relating to encryption were considered, each bill having some measure of bipartisan support.[70] All three bills would have eased export controls on encryption software and hardware.

The Encryption Communications Privacy Act of 1996 ("ECPA") bill would have liberalized export controls[71] on the theory that stringent limits on exports of encryption technology effectively cap the level of technology marketed in the United States[72] and thus restrict Americans' access to the best technology possible. The companion bill to the ECPA, the Security and Freedom Through Encryption Act

[67] NATIONAL RESEARCH COUNCIL, CRYPTOGRAPHY'S ROLE IN SECURING THE INFORMATION SOCIETY (Kenneth Dam & Herbert Lin eds., 1996). *See generally* Elizabeth Corcoran, *Easing of Encryption Technology Curbs Backed; Panel Says Restrictions on Exports of Computer Programs Are Hurting American Citizens*, WASH. POST, May 31, 1996, at B3.

[68] *See* NATIONAL RESEARCH COUNCIL, *supra* note 67, at 8-26.

[69] *See id.* at 8-16 to 8-17.

[70] Two of these bills, the Encryption Communications Privacy Act of 1996 ("ECPA"), S. 1587, 104th Cong. (1996), and the Security and Freedom Through Encryption Act ("SAFE"), H.R. 3011, 104th Cong. (1996), were companion bills that were introduced in the Senate and the House, respectively, in March 1996. The third and most recent bill, the Promotion of Commerce On-Line in the Digital Era Act ("Pro-CODE"), S. 1726, 104th Cong. (1996), was introduced in the Senate in early May 1996.

[71] *See* S. 1726 (proposed for codification at 18 U.S.C. § 2805(b)) (delineating controls for export of information security hardware, software, and technology).

[72] Because it can be difficult for companies to produce two separate lines of products for domestic and foreign use, companies often make products using the lowest common denominator of technology that can be sold in both markets. According to many high technology companies, this prevents Americans from having access to the highest possible standard of technology.

("SAFE"), was introduced in the House on March 5, 1996,[73] the same day that its counterpart was introduced in the Senate.[74]

In early May, the Senate introduced the Promotion of Commerce On-Line in the Digital Era Act ("Pro-CODE"),[75] a second version of the ECPA bill mentioned above.[76] Pro-CODE was narrower in scope than the original ECPA bill, and its sponsors viewed it as a "streamlined" measure designed to move through committee more quickly.[77]

Although the structure and the scope of the ECPA, SAFE, and Pro-CODE bills differed, the substantive portions addressing encryption export controls were similar. All three bills would have shifted exclusive authority over commercial encryption exports from the State Department to the Commerce Department. All three proposed the "generally available" standard to determine whether a license is required for export. Finally, all three called for the "financial institutions" standard, although they differed as to whether they would apply this standard to software, hardware, or both.

Senator Burns (R.-Mont.), a chief sponsor of the ECPA bill and the Pro-CODE bill, has indicated that he will re-introduce similar legislation in the 105th Congress. Representative Goodlatte (R.-Va.), a primary sponsor of the House counterpart, has indicated that he is not satisfied with the Administration's proposal, and both he and Senator Burns are likely to push for oversight hearings in 1997.[78]

IV. RECENT LEGAL CHALLENGES TO U.S. ENCRYPTION EXPORT CONTROLS

Litigation has brought encryption export controls out of the closet and into the courtroom. In one recent case, a U.S. engineer named Philip Karn sought permission from the State Department to export, in floppy disk form, the text of a book on encryption that provided the program language for a version of cryptographic software.[79] The State Department's Office of Defense Trade Controls determined that

[73] *See* 142 CONG. REC. H1715 (daily ed. Mar. 5, 1996).

[74] *See id.* at S1516.

[75] *See id.* at S4624 (daily ed. May 2, 1996).

[76] *See supra* notes 71-72 and accompanying text (outlining provisions of ECPA).

[77] *See* 142 CONG. REC. at S4625 (statement of Sen. Leahy).

[78] *See New Plan, supra* note 45, at 1, 23.

[79] *See* Karn v. Department of State, 925 F. Supp. 1, 3-4 (D.D.C. 1996). For additional information on *Karn*, see Phil Karn, *The Applied Cryptography Case* (last modified Dec. 12, 1996) <http://www.qualcomm.com/people/pkarn/export> (on file with *The American University Law Review*) and Electronic Frontier Foundation, *Karn Archive* (last modified Sept. 25, 1996) <http://www.eff.org/pub/Privacy/ITAR_export/Karn_Schneier_export_case> (on file with *The American University Law Review*).

the diskette was subject to ITAR control, and Karn appealed.[80] After the denial of his appeal, Karn filed a lawsuit in the U.S. District Court for the District of Columbia.[81] Judge Charles R. Richey issued summary judgment for the government, holding that the State Department's export licensing process is not subject to judicial review.[82] The court also held that regulation of encryption software does not constitute restraint of free speech.[83]

In another recent case,[84] the Electronic Frontier Foundation filed suit in the U.S. District Court for the Northern District of California on behalf of Daniel Bernstein, a graduate student at the University of California at Berkeley.[85] The issue presented in that case concerned Bernstein's right to publish a new encryption algorithm electronically.[86] In a ruling denying the government's motion to dismiss, the court held that software, including encryption software, is speech entitled to certain First Amendment protection.[87]

Not all speech, however, is protected in an export control context. Courts consistently have upheld national security-based restrictions on exports of information.[88] Thus, in encryption export control cases,

[80] *See Karn*, 925 F. Supp. at 4.

[81] *See id.*

[82] *See id.* at 8 (dismissing Karn's Administrative Procedures Act challenge of State Department's jurisdiction determination because Arms Export Control Act, 22 U.S.C. § 2778(a)(1), pursuant to which ITAR was promulgated, precludes judicial review).

[83] *See id.* at 12 (granting summary judgment to government on Karn's First Amendment claim that regulation of encryption software constitutes restraint on free speech).

[84] *See id.* at 14 (granting summary judgment to government on Karn's Fifth Amendment claim that government regulation of diskette containing encryption program violated his right to substantive due process).

[85] *See* Bernstein v. Department of State, 922 F. Supp. 1426, 1428 (N.D. Cal. 1996). For more information on *Bernstein*, see Electronic Frontier Foundation, *Bernstein Archive* (last modified Dec. 30, 1996) <http://www.eff.org/pub/Privacy/ITAR_export/Bernstein_case> (on file with *The American University Law Review*). Bernstein requested a commodity jurisdiction determination from the State Department to ascertain whether encryption software he developed as a Ph.D. candidate was controlled by ITAR. *See Bernstein*, 922 F. Supp. at 1430. The Office of Defense Trade Controls concluded that the software was indeed a defense article under Category XIII(b)(1) of the U.S. Munitions List. *See id.* at 1429-30 (citing 22 C.F.R. § 121.1 cat. XIII(b)(1)).

[86] *See Bernstein*, 922 F. Supp. at 1430. Bernstein challenged ITAR's prohibition against teaching his algorithm or publishing it in a journal or on-line without a license. *See id.* at 1430-31.

[87] *See id.* at 1436 ("For the purposes of First Amendment analysis, . . . source code is speech."). In *Karn*, however, Judge Richey declined to rule on whether the program language (or "source code") of encryption software fell within the gamut of First Amendment protection as speech. *See Karn*, 925 F. Supp. at 9 n.19.

[88] *See, e.g.*, United States v. Posey, 864 F.2d 1487, 1496 (9th Cir. 1989) (finding that First Amendment does not bar government restrictions on export of information included in U.S. Munitions List, even when information at issue already is available publicly); United States v. Edler Indus., Inc., 579 F.2d 516, 521 (9th Cir. 1978) (holding that statute and accompanying regulations controlling export of technical data related to items in U.S. Munitions List were not overbroad and therefore did not interfere with constitutionally protected speech); Trane Co. v. Baldridge, 552 F. Supp. 1378, 1388 (W.D. Wisc. 1983) (concluding that provision of Export

courts must balance First Amendment protections with the government's regulation of export privileges.[89] That is, in determining the constitutionality of encryption export controls, courts must ascertain whether there is a sufficiently compelling governmental interest in regulating encryption exports and whether the regulation is narrowly tailored to further that interest.[90]

Finally, in a third case, a Case Western Reserve University law professor filed suit in the U.S. District Court for the Northern District of Ohio challenging the State Department's controls on exports of cryptographic computer software.[91] He alleged that the controls violate the First Amendment by limiting his ability to teach foreign students and to discuss cryptographic material with foreign colleagues.

CONCLUSIONS AND RECOMMENDATIONS

As noted above, there is a growing commercial imperative for strong information security.[92] For financial institutions that must protect transmissions, the authentication and data integrity exceptions[93] no longer are sufficient, and the banking exception is too narrow and ill-defined.[94] Similarly, telecommunications companies—including pay-television, cable, cellular and digital telephone services—need to offer effective security to their customers. Users of

Administration Act and accompanying regulations, prohibiting certain communications by U.S. persons with boycotted countries or with blacklisted firms or persons, did not violate First Amendment), *aff'd*, 728 F.2d 915 (7th Cir. 1984); *cf.* Konigsberg v. State Bar, 366 U.S. 36, 50-51 (1961) ("[G]eneral regulatory statutes, not intended to control the content of speech but incidentally limiting its unfettered exercise, have not been regarded as the type of law the First . . . Amendment forbade Congress . . . to pass, when they have been found justified by subordinating valid governmental interests . . . ."); United States v. Brumage, 377 F. Supp. 144, 150 (E.D.N.Y. 1974) ("[A] federal statute regulating foreign commerce closely related to foreign affairs and national security . . . is entitled to the highest presumption of validity.").

[89] *See Bernstein*, 922 F. Supp. at 1433-38 (analyzing whether subjecting encryption software to licensing requirement raises colorable First Amendment claim).

[90] *See Karn*, 925 F. Supp. at 9-13. In assessing the constitutionality of the ITAR, the court in *Karn* applied the criteria set forth in *United States v. O'Brien*, 391 U.S. 367 (1968), a case in which the Supreme Court upheld the government's prohibition against burning draft cards. *See id.* at 386. Under the *O'Brien* analysis, a regulation that is content-neutral such as ITAR (that is, the intent of ITAR is not to control the content of speech or expressive conduct, but rather to thwart the encryption efforts of foreign intelligence sources) may be justified so long as the regulation "'furthers an important or substantial governmental interest,' and 'the incidental restriction on alleged First Amendment freedoms is no greater than is essential to the furtherance of that interest.'" *Karn*, 925 F. Supp. at 11 (quoting *O'Brien*, 391 U.S. at 377).

[91] For information on *Junger*, see Electronic Frontier Foundation, *Junger Archive* (last modified Oct. 2, 1996) <http://www.eff.org/pub/Privacy/ITAR_export/Junger_v_DoS> (on file with *The American University Law Review*).

[92] *See supra* Part I (discussing information security needs in today's global economy).

[93] *See supra* text accompanying notes 35-36 (describing Access Control and Data Authentication Exceptions to ITAR).

[94] *See supra* text accompanying note 34 (presenting Banking or Money Transactions Exception to ITAR).

communications software are demanding greater information security as well. Companies with sites around the world must be able to transmit customer information, design information, and financial information with absolute confidence. Encryption export controls should not be so strict as to prevent U.S. software developers and U.S. hardware manufacturers from offering security products to compete for such customers.

From the commercial perspective, U.S. companies increasingly rely on international sales to remain viable. Indeed, the market for information security is international. If U.S. businesses cannot meet those demands, domestic companies almost certainly will forfeit their competitive edge in encryption technology. Meanwhile, strong cryptographic products often are readily available overseas. For instance, at least one company has announced a partnership with the Chinese Government and the Academy of Sciences to implement the RSA algorithm.[95] Against this backdrop, one significant gap in current encryption export policy is the absence of a "foreign availability" standard, which would relax U.S. controls on products that already are available overseas.

At a more fundamental level, the availability of cryptographic software outside the United States underscores the futility of overly restrictive unilateral export controls. In today's global marketplace, geographic boundaries present fewer and fewer barriers to trade. Thus, now that the business world is linked electronically, U.S. restrictions arguably will drive the restricted activities outside the United States without limiting the development or dissemination of the "controlled" technology.

Although the debate regarding the pace and direction of export liberalization will continue, there is no doubt that controls will be relaxed in the days ahead. The commercial and technical strains on the existing control framework simply are too great, and they are growing almost daily. Efforts to liberalize controls will seek to balance commercial and individual privacy against law enforcement needs and national security concerns. That balancing act suggests that some form of export restrictions will survive the debate and that future advances in information technology could lead to even further efforts by the government to control it.

[95] *See* Don Clark, *China, US Firm Challenge US on Encryption-Software Exports*, WALL ST. J., Feb. 8, 1996, at A10.