ENCRYPTION'S IMPORTANCE TO ECONOMIC AND INFRASTRUCTURE SECURITY

F. LYNN MCNULTY*

I. INTRODUCTION

The national and societal view of the role of encryption will be one of the defining issues for our culture in the twenty-first century. Encryption is cited by Michael Baum, chairman of the Information Security Committee of the American Bar Association, as "an enabling technology that provides companies, their business partners, customers and end users with the ability to get the information and service they need much faster and more securely."[1] Ubiquitous digital communications will result in either a secure environment to conduct personal affairs and electronic commerce or a Kafkaesque world laid bare by digital fingerprints indicating our every transaction and thoughts. The information age has brought to light many important issues: protection of privacy, infrastructure protection, law enforcement, national security, and economic competitiveness. In a democracy, it is important to have a public debate on these issues and to ensure that our laws adequately address the issue of cryptography to carry us forward into the twenty-first century.

II. EQUITIES AND ENCRYPTION GROWTH

The heart of the matter, which is how the nation will protect its information systems, has been obscured by concerns of equity regarding the interests of all involved parties, including business, privacy advocates, national security agencies, and law enforcement.

[*] F. Lynn McNulty is the Director of Government Affairs for RSA Data Security, the country's leading provider of commercial cryptography technology. Prior to joining RSA Data Security, Mr. McNulty was the Associate Director for Computer Security at the National Institute of Standards and Technology. During his thirty-year federal government career, he held increasing computer security responsibilities at the Central Intelligence Agency, Federal Aviation Administration, and Department of State. He is also a retired Army Reserve Intelligence Officer. Mr. McNulty has a B.A. in International Relations from the University of California, Berkeley, a M.A. in International Relations from San Jose State University, and a M.S. in Administration from the George Washington University.

[1] Laura DiDio, *Internet Boosts Cryptography*, COMPUTERWORLD, Mar. 16, 1998, at 32.

Senator Sam Nunn has spoken about the need for breaking the deadlock on encryption, which he says is "absolutely essential for infrastructure protection as well as for any kind of commercial activities which are beginning to emerge in the world of the Internet."[2] Nunn added, "I do not think that we can limit the power of encryption successfully over the long term. That's like trying to limit technology. I do not think it can be done."[3]

On 6 April 1998, International Business Machines (IBM) Chairman and Chief Executive Officer, Lou Gerstner, echoed Nunn's comments on the importance of unrestricted use of encryption for legitimate purposes.[4] Gerstner advocated unrestricted levels of encryption technology within the United States to secure corporate networks from hackers and other unauthorized users.[5] Gerstner also urged the Clinton administration "to work closely with other nations on a global encryption policy" compatible with domestic U.S. requirements.[6]

In general, interest in encryption is at an all-time high and demand for it in the commercial marketplace is soaring. As of April 1998, there were over 300 million copies of RSA[7] products in the commercial marketplace.[8] Although most encryption users are law-abiding, a few are not. More importantly, a number of companies in twenty-nine other countries produce 656 encryption products that are

[2] *US Counterterrorism Policy: Hearing Before the Senate Judiciary Committee*, FEDERAL NEWS SERVICE, Sept. 3, 1998 (statement of Senator Leahy quoting Senator Nunn), *available in* LEXIS, News Library, Fednew File. *See generally Testimony March 17, 1998 James S. Gorelick & Sam Nunn Co-Chairs Advisory Committee to the President's Commission Senate Judiciary Technology, Terrorism and Government Information Preventing Terrorism*, FEDERAL NEWS SERVICE, Mar. 17, 1998, *available in* LEXIS, News Library, Fednew File.

[3] *US Counterterrorism Policy: Hearing Before the Senate Judiciary Committee*, *supra* note 2.

[4] *See* Nancy Weil, *Gerstner Calls for Unrestricted Encryption*, INFOWORLD DAILY NEWS, Apr. 6, 1998 *available in* LEXIS, News Library, Infwld File.

[5] *See id.*

[6] *See id.*

[7] Rivest-Shamir-Adleman (RSA) are the developers of the first commercialized public key cryptographic product. "RSA technologies are part of existing and proposed standards for the Internet and World Wide Web . . . and business, financial, and electronic commerce networks around the globe." *Security Dynamics Appoints Art Coviello President and Jim Bidzos Vice Chairman; Signals Further Integration of Security Dynamics and RSA Business Units*, PR NEWSWIRE, Mar. 8, 1999, *available in* LEXIS, News Library, Prnews File.

[8] *See* RSA Data Security, Inc., *RSA '99: Overview* (last modified Nov. 10, 1998) <http://www.rsa.com/conf99/home.html>.

as strong as or stronger than encryption products that U.S. companies sell on the world market.[9]

In the early 1990s, RSA hosted its first cryptography conference with approximately sixty people in attendance.[10] Beginning in 1996, the commercial interest in cryptography increased significantly. By January 1998, the RSA conference filled the Masonic auditorium on Nob Hill in San Francisco, with at least 3,000 people in attendance.[11] The conference grew to 5,000 people in 1999.[12] The majority of attendees are no longer cryptographers, mathematicians, and other members of academia, but rather are persons from the business and computer-user communities.[13]

With respect to electronic payments, secure electronic mail, and network encryption, numerous standards are developing outside the public policy debates concerning encryption.[14] New developments include cryptographic applications programming interfaces (CAPIs) that are bundled with various commercial shrink-wrapped software products designed to operate with IBM/IBM-compatible and Apple computers.[15] Due in part to large profit realization on the sale of security products and systems, significant consolidations in the security product industry are occurring. For example, in 1996, Security Dy-

[9] *See* Network Associates Products, *Total Network Security: Cryptographic Products* (visited Feb. 22, 1999) <http://www.nai.com/products/security/tis_research/crypto/crypt_surv.asp>.

[10] *See* Jeffrey Kutler, *At RSA Confab: An Endless Loop of Intrigue; Conspiracy Theories, Martin Luther King Jr. Tribute, and Encryption News*, AM. BANKER, Jan. 29, 1999, at 12.

[11] *See RSA Conference Ends with Push to Educate Business, Consumers and Policy Makers About Need for Data Security*, PR NEWSWIRE, Jan. 20, 1998, *available in* LEXIS, News Library, Prnews File.

[12] *See* Kutler, *supra* note 10.

[13] *See* RSA Data Security, Inc., *RSA '99, Frequently Asked Questions* (last modified Nov. 10, 1998) <http://www.rsa.com/conf99/faq.html>.

[14] *See* RSA Data Security, Inc., *Frequently Asked Questions About Today's Cryptography; Question 1.5, What are Cryptography Standards?* (last modified Jan. 26, 1999) <http://www.rsa.com/rsalabs/faq/html/1-5.html>. "Cryptography standards are needed to create interoperability in the information security world. Essentially they are conditions and protocols set forth to allow uniformity within communication, transactions, and virtually all computer activity." *Id.* These standards are developed not only by the government, but by private industry and other organizations. *See id.*

[15] *See* RSA Data Security, Inc., *Frequently Asked Questions About Today's Cryptography; Question 5.2.1, What are CAPIs?* (last modified Jan. 26, 1999) <http://www.rsa.com/rsalabs/faq/html/5-2-1.html>. "A CAPI, or cryptographic application programming interface, is an interface to a library of functions software developers can call upon for security and cryptography services. The goal of a CAPI is to make it easy for developers to integrate cryptography into applications." *Id.*

namics Technologies, Inc. acquired RSA for over $200 million.[16] Trusted Information Systems, a company with a patent on key recovery systems, was acquired for $300 million by Network Associates, the same company that previously acquired Pretty Good Privacy (PGP), the vendor of the popular electronic mail encryption program.[17] We should anticipate more such mergers and acquisitions as the industry continues this exponential pattern of growth.

The public's interest in encryption revolves primarily around Internet applications. For example, people want to protect their credit card information when engaged in Internet commerce.[18] Due to this public demand, new Internet applications that use encryption as their basis permit such transactions to occur in a secure manner.[19] Cryptography is also used in on-line state lottery systems,[20] software driven slot machines,[21] and electronic money applications such as electronic purse smart cards.[22]

III. U.S. CRYPTOGRAPHY POLICY DEVELOPMENT

Cryptography provides confidentiality as well as three other basic functions: authentication, integrity, and non-repudiation.[23] Although cryptography can furnish numerous benefits, many of these

[16] *See* Karen Rodriguez, *One-Stop Shop Planned-Security Dynamics Acquires RSA for Improved Security*, INTERNETWEEK, Apr. 22, 1996, *available in* LEXIS, News Library, Intwk File.

[17] *See* Jerry Knight, *In the Winner's Circle: Technology and Takeovers*, WASH. POST, Apr. 6, 1998, at F07.

[18] *See* RSA Data Security, Inc., *Frequently Asked Questions About Today's Cryptography; Question 1.7, Why is Cryptography Important?* (last modified Jan. 26, 1999) <http://www.rsa.com/rsalabs/faq/html/1-7.html>.

[19] *See id.*

[20] *See* Robert Gillette, *Computer Experts Grapple with Vulnerable Systems*, L.A. TIMES, Nov. 25, 1988, at 1.

[21] *See Silicon Gambling, Inc. Receives Nevada Gaming Commission Approval for Sale of Slot Machines in Nevada; SGI's Odyssey, Employing RSA Technology, Brings Next-Generation Technology to Casino Gaming*, BUSINESS WIRE, Apr. 2, 1997, *available in* LEXIS, News Library, Bwire File.

[22] *See* Jeffrey Kutler, *Smart Cards: Even Abundant Security Features Don't Spur Smart Card Buy-in*, AM. BANKER, Nov. 18, 1998, at 1; *see also* Gillette, *supra* note 20.

[23] Task Force on Electronic Commerce, *Security/Cryptography, Part I: Cryptography and its Applications* (last modified Mar. 14, 1999) <http://e-com.ic.gc.ca/english/crypto/631d13.htm>. "Confidentiality: keeping information protected from unauthorized disclosure or viewing by mathematically scrambling the original text." *Id.* "Authentication: proof that users are who they claim to be or that resources (e.g., computer device, software or data) are what they purport to be." *Id.* "Non-repudiation: proof that a transaction occurred, or that a message was sent or received, thus one of the parties to the exchange cannot deny that the exchange occurred." *Id.* "Integrity—so that data cannot be modified without detection." *Id.*

benefits have not been fully utilized in either the private or public sectors. For example, the controversy arising from the Social Security Administration's attempt to provide personal earnings and benefits statements on-line[24] would not have failed if the government agency had taken advantage of Web browser-embedded cryptography and digital signatures. Instead, the agency was forced to rescind its announcement that it was going to make the statements available to citizens, and the net result was public embarrassment, wasted time, and a loss of public confidence.[25] However, cryptography is only one integral component of a secure information system. As Professor Dorothy Denning of Georgetown University notes, information system security depends on many other factors: "access controls, authentication, auditing, configuration management, vulnerability testing and repair, intrusion and misuse detection, malicious code detection, and security training and awareness."[26]

The recent public debate on cryptography policy has its primary roots in the Clinton administration's key escrow-based Clipper chip proposal of 1993.[27] The handling of that proposal effectively poisoned the well in terms of any kind of constructive debate on encryption use. General distrust of the Clipper chip arose because the cryptographic algorithm on which the chip was based (the Skipjack algorithm) was developed in secret by the National Security Agency (NSA).[28] The designation of two federal agencies as key escrow re-

[24] *See* Frank Tiboni, *SSA Again Tests PEBES for Web Accessibility; Social Security Administration's Personal Earnings and Benefit Earnings Statements; Government Activity*, GOV'T COMPUTER NEWS, July 27, 1998, at 3.

[25] *See id*.

[26] *Prepared Statement of Dorothy E. Denning, Georgetown University, Computer Science Department Before the House Committee on the Judiciary Subcommittee on Courts and Intellectual Property*, FEDERAL NEWS SERVICE, Mar. 4, 1999, *available in* LEXIS, News Library, Fednew File.

[27] *See* Rutrell Yasin, *Senators Pledge to Push Encryption Reform*, INTERNETWEEK, June 22, 1998, *available in* LEXIS, News File, Intwk File. The Clipper chip proposal would have required every computer to contain an encryption key allowing the government to unlock any encrypted data. *See* Reinhardt Krause, *The Encryption Export Debate*, INV.'S BUS. DAILY, May 21, 1998, at A1, *available in* LEXIS, News Library, Invdly File.

[28] *See* RSA Data Security, Inc., *Frequently Asked Questions About Today's Cryptography; Question 3.6.7, What are Some Other Block Ciphers?* (last modified Jan. 26, 1999) <http://www.rsa.com/rsalabs/faq/html/3-6-7.html>. "Skipjack is the encryption algorithm contained in the Clipper chip, designed by the NSA . . . . Initially the details of Skipjack were classified and the decision not to make the details of the algorithm publicly available was widely criticized . . . . Aware of such criticism, the government invited a small group of independent cryptographers to examine the Skipjack algorithm. They issued a report which stated that although their study was too limited to reach a definitive conclusion, they nevertheless believed Skipjack was secure. In June of 1998 Skipjack was declassified by the NSA." *Id.*

positories engendered further public distrust.[29] Federal agency involvement in this manner represented a huge departure from past practice in the development of federal technical standards. Standards development historically had been carried out in public by the National Institute of Standards and Technology (NIST) and its predecessor, the National Bureau of Standards.[30]

In the following years, the Clinton administration slowly moved toward a more reasonable policy by emphasizing the private sector's dependence on cryptography and identifying where business and government interests coincide.[31] But, as Secretary of Commerce William Daley recognized in April 1998, the administration still had not crafted an acceptable encryption policy.[32] This continued failure is largely the result of the government's relatively unsuccessful attempts to influence the commercial marketplace through the promulgation of standards, leveraging government procurements, and export controls. With respect to encryption products available in countries outside the U.S., Daley noted that "most of these producers do not need an export license if they want to ship encryption software, a tremendous market advantage."[33] According to Daley, this advantage would result in foreign domination of the market meaning "a loss of jobs here and products that do not meet either our law enforcement of national security needs."[34] More recently however, the administration's rhetoric has shifted to the advocacy of a more balanced approach on encryption use. For example, the government has run various key recovery[35] demonstration projects, thirteen of which

[29] *See* Ellen Messmer, *U.S. Government Sets New Course on Security*, NETWORK WORLD, Feb. 28, 1994, at 6. In February 1994, the Clinton administration announced that the Department of Treasury and the NIST were to be key escrow repositories for the Clipper chip split keys. *See id.* "Key escrow is a security technique that places a cryptographic key into the hands of a trusted third party." *See* Mary Mosquera, *Federal Encryption Plan Estimated at $7B*, TECHWEB NEWS, June 10, 1998, *available in* LEXIS, News Library, Techwb File.

[30] *See* RSA Data Security, Inc., *Frequently Asked Questions About Today's Cryptography; Question 6.2.1, What is NIST?* (last modified Jan. 26, 1999) <http://www.rsa.com/rsalabs/faq/html/6-2-1.html>.

[31] *See* William H. Daley, Remarks by U.S. Secretary of Commerce William M. Daley—"The Emerging Digital Economy", (Apr. 15, 1998) (transcript available in LEXIS, News Library, Feddoc File) [hereinafter Daley Speech].

[32] *See* Bill Pietrucha, *Sen. Burns Renews Push To Loosen Encryption Regs*, NEWSBYTES, Apr. 20, 1998, *available in* LEXIS, News Library, Nwsbyt File.

[33] *Id.*

[34] *Id.*

[35] "Key recovery is a general term encompassing the numerous ways of permitting 'emergency access' to encrypted data." RSA Data Security, Inc., *Frequently Asked Question*

were briefed to the public in November 1997.[36] Eleven of the thirteen projects were for the key recovery of stored data.[37]

Many computer vendors question the feasibility of these key recovery schemes. In June 1998, several chief executive officers of the leading American computer firms issued a report in which they concluded that government plans to institute a federal key recovery/escrow infrastructure, designed to give law enforcement and intelligence agencies access to encrypted materials, would cost as much as $7.7 billion a year.[38] The report, entitled "The Cost of Government-Driven Key Escrow Encryption" and issued by the Business Software Alliance, was endorsed by Microsoft, Novell, Adobe, Bentley Systems, FileMaker, Lotus Development, Sybase, and Symantec.[39] Novell's CEO, Eric Schmitt, said, "'Encryption policy must be guided by the digital Hippocratic Oath—first, do no harm.' . . . The high cost of the key-escrow system does not pass this test."[40]

In September 1998, Vice President Al Gore announced a slight alteration in U.S. export policy.[41] The United States eased licensing requirements on exporting products with varying strengths (including those products above 56-bits) to foreign subsidiaries of U.S. corporations[42] and strategic foreign partners of U.S. companies.[43] The government also eased exports to foreign insurance companies in forty-five countries as well as to foreign health and medical organizations.[44] Unfortunately, pharmaceutical firms were not included in this category;[45] a possible indication that the administration's intelligence-gathering priorities are directed against that particular industry. License exceptions were authorized for the export of client-server applications and applications designed for on-line transactions.[46] But for general exports, the Clinton administration only eased burden-

About Today's Cryptography; Question 7.12, What is Key Recovery? (last modified Jan. 26, 1999) <http://www. rsa.com/rsalabs/faq/html/7-12.html>.

[36] *See Questions Trail Federal Key Recovery Pilot Projects' Progression*, HIGH PERFORMANCE COMPUTING, Nov. 17, 1997, *available in* LEXIS, News Library, Curnws File.

[37] *See id.*

[38] *See* Mosquera, *supra* note 29.

[39] *See id.*

[40] *Id.*

[41] *See* Joel Brinkley, *U.S. Eases Encryption Software Export Bans*, N.Y. TIMES, Sept. 17, 1998, at C7.

[42] *See id.*

[43] *See id.*

[44] *See id.*

[45] *See id.*

[46] *See id.*

some licensing and reporting requirements on products operating at 56-bits and under.[47] Exports of strong encryption products for use by the large population of individual users are still subject to arcane export controls. The new regulations also favor key recovery products and other "plain text access" features over those lacking such features.[48]

The administration's selection of forty-five countries to receive special attention appears arbitrary because restrictive export controls on encryption were maintained on certain countries placed in a special category known as "Tier 3."[49] This category is one step above the category including terrorist countries, such as Cuba and North Korea, against which the United States applies comprehensive economic sanctions.[50] Tier 3 includes Andorra, a significant financial center located between France and Spain; Bahrain, a significant financial services center in the Persian Gulf; Estonia, Latvia, Lithuania, and Romania, all NATO applicants; Kuwait, Oman, Qatar, Saudi Arabia, and the United Arab Emirates, U.S. allies hosting significant U.S. petroleum interests; Vanuatu, an important South Pacific financial services center; and Israel, another significant U.S. strategic Middle East partner.[51]

[47] *See* Statement by the Press Secretary: Administration Updates Encryption Policy, 34 WEEKLY COMP. PRES. DOC. 1832 (Sept. 16, 1998).

[48] *See id.* A key recovery product is either "a) [a] stored data product containing a recovery feature that, when activated, allows recovery of the plaintext of encrypted data without the assistance of the end user; or b) [a] product or system designed such that [a] network administrator or other authorized persons can provide law enforcement access . . . without the knowledge . . . of the end user." Bureau of Export Administration, *Definitions; Related to the Administrations's Encryption Policy Guidance Announced September 16, 1998* (last modified Feb. 23, 1999) <http://207.96.11.93/Encryption/ Definitions.html>. "Plaintext" refers to the data initially presented before the encryption takes place. *See id.*

[49] *See* Bureau of Export Administration, *Export Administration Regulations, Commerce Control List Overview and the Country Chart* (visited Mar. 16, 1999) <http://frwebgate.access. gpo.gov/cgibin/getdoc.cgi?dbname=bxa&docid=f:738spir. pdf>.

[50] *See id*.

[51] *See* Nancy Weil & Torsten Busse, *Thirteen Companies Support Encryption Alternative*, INFOWORLD DAILY NEWS, July 14, 1998, *available in* LEXIS, News Library, InfoWorld Daily File. The other Tier 3 countries are Afghanistan, Albania, Algeria, Angola, Armenia, Azerbaijan, Belarus, Bosnia & Herzegovina, Bulgaria, Cambodia, China (People's Republic of), Comoros, Croatia, Djibouti, Egypt, Georgia, India, Jordan, Kazakhstan, Kyrgyzstan, Laos, Lebanon, Macedonia (The Former Yugoslav Republic of), Mauritania, Moldova, Mongolia, Morocco, Pakistan, Russia, Serbia & Montenegro, Tajikistan, Tunisia, Turkmenistan, Ukraine, Uzbekistan, Vietnam, and Yemen. *See id.*

IV. THE WASSENAAR ARRANGEMENT CHANGES

In December 1998, a major change took place in the Wassenaar Arrangement, a group of thirty-three industrialized countries that banded together after the Cold War to restrict exports of military and military-civilian "dual use" technology to certain renegade and pariah countries such as Iran and Libya.[52] The Wassenaar countries extended the group's Dual-Use Control List to encryption hardware and software cryptography products above 56-bits, which include web browsers, e-mail applications, electronic commerce servers, and telephone scrambling devices.[53] The Wassenaar members also reimposed controls on other mass-market products with strengths over 64-bits, such as personal computer operating systems, word processing, and data base programs.[54]

The revised Wassenaar controls, with their restrictions on the free trade of cryptographic products, directly challenge the international protections against arbitrary interference with individual privacy and free expression of ideas. The issuance of the new controls took place within a week of the celebration of the Fiftieth Anniversary of the Universal Declaration of Human Rights (UDHR).[55] The timing of these events is ironic because Article 12 of UDHR states, "No one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence . . . ."[56] If cryptography is viewed as a form of language, restrictions on its use could be construed as representing a restriction on free correspondence. Similarly, privacy advocates around the world recognize cryptography as a "privacy-enhancing technology."[57] Therefore, under Article 12 of the UDHR, restricting its free use can be viewed as an arbitrary interference with one's privacy. Furthermore, on 18 September 1998, Human Rights Watch spoke out against Wassenaar's planned new restrictions on

[52] *See* Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, *Welcome to the Wassenaar Arrangement* (last modified Feb. 24, 1999) <http://www.wassenaar.org/docs/index1.html>.

[53] *See* Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, *Dual-Use List-Category 5-Part 2-"Information Security"* (last modified Dec. 16, 1998) <http://www.wassenaar.org/list/cat5p2.pdf>.

[54] *See id.*

[55] *See* Universal Declaration of Human Rights, G.A. Res. 217A (III), U.N. Doc. A/810 (1948), art. 12.

[56] *Id.* art. 12.

[57] Suzanne Andrew, *Executive Summary Report, Symposium on Privacy-Enhancing Technologies* (last modified June 15, 1998) <http://strategis.ic.gc.ca/ SSG/pv01167e.html>.

cryptography[58] by warning that communications in coded languages are protected as a right of free expression under Article 19 of the International Covenant on Civil and Political Rights,[59] an agreement to which most members of the Wassenaar Arrangement are parties.[60]

Notwithstanding these concerns, Clinton administration officials cited the new Wassenaar controls as a victory in their effort to extend U.S. levels of export controls on cryptography to the rest of the world. John P. Barker, Deputy Assistant Secretary of State for Export Controls, cited the U.S. government's "success in achieving consensus on new multilateral export controls on encryption products and software" through the Wassenaar Arrangement.[61] He said that this success was a result of the "Attorney General and the Deputy Secretary of Defense [writing] letters to their foreign counterparts, and NSA [working] closely with similar agencies in other countries."[62] Barker also said that "[t]he Deputy Secretary of State and senior National Security Council officials also made personal contacts in support of the U.S. approach, and our embassies in Wassenaar capitals conducted a series of demarches."[63]

The American Electronics Association (AEA), an industry group representing more than 3,000 U.S.-based technology companies, supports the Clinton administration's decision to align U.S. export regulations with the new Wassenaar requirements and to de-

[58] *See* Human Rights Watch, *Crypto Controls Threaten Human Rights; Vienna Conference Warned Against Restricting Free Expression* (last modified Mar. 10, 1999) <http://www. hrw.org/hrw/ press98/sept/crypto.htm>.

[59] *See id.*

> Everyone shall have the right to hold opinions without interference. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary: (a) For respect of the rights or reputations of others; (b) For the protection of national security or of public order (ordre public), or of public health or morals.

International Covenant on Civil and Political Rights, Dec. 19, 1966, art. 19, 999 U.N.T.S. 171, 176 (entered into force Mar. 23, 1976).

[60] *See* Human Rights Watch, *supra* note 58.

[61] *Prepared Statement of John P. Barker, Deputy Assistant Secretary of State for Export Controls Before the Senate Banking, Housing and Urban Affairs Committee, Subcommittee on International Trade and Finance*, FEDERAL NEWS SERVICE, Mar. 16, 1999, *available in* LEXIS, News Library, Fednew File.

[62] *Id.*

[63] *Id.*

regulate products up to 56-bits, but feels the response is inadequate.[64] The group characterized the Wassenaar decision to reimpose controls on mass market software with key lengths exceeding 64-bits as a "rollback" because previously there were no limits on key lengths for mass market software.[65] The AEA correctly pointed out that it "defies simple logic to suggest that mass market software products with 65 bit keys is now susceptible to control, but mass market software with 64 bit keys are not."[66] Law enforcement and intelligence agencies find it no less difficult to break 64-bits than 65-bits. The difference is virtually meaningless for purposes of cryptanalysis and accordingly the separation is purely arbitrary. In addition, the AEA concluded that the Wassenaar agreement to control a common list of products does not mean that members will adhere to a level playing field, because Wassenaar members have the discretion either to require or not require export licenses for certain encrypted mass market products.[67]

A. Export of Weapons and Wassenaar

Wassenaar's attempt to control the export of weapons to countries at war demonstrates the difficulty in enforcing export regimes. For example, Russia, a Wassenaar member, has violated the Arrangement by delivering $150 million worth of combat aircraft, helicopters, and other military equipment to Ethiopia.[68] While Wassenaar does not control the export of small arms, like rifles, it does seek to deter the export of large armaments to warring or "pariah" states. Pyotr Litavrin, the Head of Division for the Russian Department for Security and Disarmament Affairs, criticizes Wassenaar for failing to halt Russian arms exports to Iran.[69] Litravin maintains that many disagreements between the United States and Russia prevent Wassenaar from becoming "a comprehensive and efficient arms export control regime."[70] In October 1998, Pier Benedetto Francese, Italy's Representative to the United Nations, told the General As-

[64] *See Administration Encryption Efforts with Wassenaar Arrangement Come up Short*, PR NEWSWIRE, Dec. 9, 1998, *available in* LEXIS, News Library, Prnews File.

[65] *See id.*

[66] *Id.*

[67] *See id.*

[68] *See Concern For Weapons Sales to African Nations*, AFRICA NEWS, Dec. 11, 1998, *available in* LEXIS, News Group File, Afrnws File; *see also* Raymond Bonner, *New Weapons Sales to Africa Trouble Arms-Control Experts*, N.Y. TIMES, Dec. 6, 1998, sec. 1, at 14.

[69] *See* Walter C. Uhler, *Russia in the World Arms Trade*, 266 THE NATION 63 n.4 (1998).

[70] *Id.*

sembly that in 1999, the Wassenaar Arrangement would be revised to close loopholes and include the establishment of an international agenda on small arms and light weapons.[71] Bulgaria, another Wassenaar signatory, has also violated the weapons restrictions by selling tanks to Ethiopia and Uganda[72] and smaller weapons to rebel movements in Sri Lanka, Congo, and Rwanda.[73] In addition, at least two other Wassenaar participants, Slovakia,[74] and Ukraine,[75] routinely violate Wassenaar arms export restrictions.

Many arms control specialists believe that Wassenaar has not been effective at limiting the proliferation of conventional weapons. Lora Lumpe, an arms trade specialist with the Federation of American Scientists, has said that the value of the Wassenaar Arrangement is difficult to see.[76] There is no reason to believe that certain countries will comply with Wassenaar's cryptography export controls. Moreover, the United States selectively enforces Wassenaar in pursuit of its own clandestine interests around the world. For example, the Clinton administration has turned a blind eye to Bulgarian arms shipments to Africa.[77] In addition, the United States has reportedly violated Wassenaar prohibitions against sensitive technology transfers to China, prompting both a Justice Department probe and a congressional inquiry.[78] The allegedly illegal technology transfer included cryptographic printed circuit boards that permit ground control operators to send secure commands to orbiting telecommunications satellites.[79] In a written assessment, the NSA stated, "If the

[71] *See Response to Crises, Peacekeeping Among Subjects Addressed as General Assembly Concludes Discussion*, M2 PRESSWIRE, Oct. 7, 1998, *available in* LEXIS, News Library, M2pw File.

[72] *See* Bonner, *supra* note 68.

[73] *See* Raymond Bonner, *Bulgaria Becomes a Weapons Bazaar*, N.Y. TIMES, Aug. 3, 1998, at A3.

[74] *See* Nicholas Watt & Richard Norton-Taylor, *Blair Challenged on Arms Supplies for African Rebels*, THE GUARDIAN (LONDON), Feb. 11, 1999, at 8, *available in* LEXIS, News Library, Guardn File.

[75] *See* Taras Kuzio, *Ukraine's Arms Sales Continue To Expand*, 9 JANE'S INTELLIGENCE REV. 108 n.3 (1998); *Museveni Probes Tank Purchase*, AFRICA NEWS, Jan. 2, 1999, *available in* LEXIS, News Library, Afrnws File; *Export Official Denies Arms Supplied to Taleban*, UNIAN (Kiev, Ukraine), Aug. 11, 1998, *available in* LEXIS, News Library, Curnws File.

[76] *See* Bonner, *supra* note 68.

[77] *See id*.

[78] *See* Simon Beckin, *The Furor Over Collaboration With China Is Shaping Up To Be The Single Biggest Threat To The Democrats In This Congressional Election Year*, S. CHINA MORNING POST, May 24, 1998, at 11, *available in* LEXIS, News Library, Schina File.

[79] Michael Kelly, *A Chance to Jolt China With Straight Talk*, 30 NATIONAL J. 1488 n.26 (1998).

encryption board was reverse-engineered, the knowledge gained could be used to strengthen adversaries' knowledge of the systems the United States uses to safeguard its satellite communications system."[80]

In addition to arms control specialists, many other vendors and industry associations around the world decried the Wassenaar controls, arguing against cryptography controls in much the same fashion that U.S. companies voiced their opposition to the Clipper chip some five years earlier. For example, Electronic Frontiers Australia spokesperson Greg Taylor declared,

> Cryptography controls have been universally condemned by privacy advocates, industry groups, and professional bodies for many years. At a time when there was an expectation that common sense might finally prevail, the world's cold warriors have met in closed session in Vienna to rebuff their many critics and to extend existing controls to commonly available commercial products.[81]

Wassenaar has had at least one important consequence: the debate on cryptography policy has became an international one.

B. Burgeoning International Debate

In an interview with the Finnish national newspaper *Helsingin Sanomat*, Finnish Prime Minister Paavo Lipponen alluded that it was the very powerful position of the United States that forced through the changes to Wassenaar.[82] He added that "the Wassenaar negotiations are highly secret."[83] The Prime Minister, noting that the controls could hurt Finnish industry, stated that "Finland still aims for openness and free markets also in this area."[84] Lipponen had to consider the position of Nokia, a Finnish firm with a large market share of the international cellular telephone market. Nokia's trade policy director told *Helsingin Sanomat* that his firm believed, along with other industry sectors, that strong encryption should be permitted and its export should not be restricted.[85] The Nokia executive said that applying for export restrictions creates additional work and costs and the process is a "difficult thing."[86] Finland had previously an-

[80] *Id.* at 1488.

[81] Electronic Frontiers Australia Inc. Media Release, *New Encryption Controls Condemned* (last modified Dec. 13, 1998) <http://www.efa.org.au/Publish/ PR981214.html>.

[82] *See Finnish Prime Minister On Wassenaar*, HELSINGIN SANOMAT, Dec. 15, 1998, at B7.

[83] *Id.*

[84] *Id.*

[85] *See id.*

[86] *Id.*

nounced a policy that ensured the freedom to use cryptography products and a liberalized approach to the trade of products using cryptography.[87]

Like Finland, Denmark has decided not to overly restrict cryptography use. Announcement of its signature to the Wassenaar Arrangement caused a political backlash, with some Parliament members complaining that the Danish government had violated its earlier commitment not to restrict the technology.[88] Kim Behnke, the parliamentary leader of the pro-free trade Progress Party[89] demanded an explanation from the Danish Science Minister as to why Denmark acceded to the new Wassenaar controls.[90]

In Germany, Bundnis 90/Die Grünen (the Green Party), a key player in the governing coalition, also criticized the German government for caving in to U.S. pressure for stronger controls on cryptography above 64-bits.[91] In early 1998, the parliamentary faction of the Green Party specifically asked the German government if it was aware that agencies such as the NSA were "watering down" encryption standards and systems.[92] The government's response was surprisingly candid: the restrictive U.S. export policies on encryption were well known and the German cryptographic agency, the Bundesamt fur Sicherheit in der Informationstechnik (Federal German Information Security Agency) (BSI), was generally hesitant to recommend U.S. encryption products for use by German government agencies and corporations.[93] BSI's reluctance may be explained by the fear that exported U.S. cryptographic products have been weakened or contain some type of back door access mechanism. Such concerns adversely affect foreign customer confidence in the security afforded by such products.

[87] *See* Government of Finland, *National Cryptography Policy* (last modified Jan. 28, 1998) <http://www.vn.fi/lm/telecom/cryptography/guidelines.htm>.

[88] *See* Bo Elkjaer, *Wassenaar Explosion in Denmark* (last modified Dec. 16, 1998) <http://jya.com/wass-dk.htm>.

[89] The Progress Party is opposed to trade sanctions and other impediments. Its platform states that the best way to promote human rights in all countries and combat totalitarian regimes is through free trade and the exchange of information. *See The Progress Party (Fremskridtspartiet, Fp)* (visited Mar. 29, 1999) <http://www.frp.dk/foreign/engelsk.htm>.

[90] *See* Elkjaer, *supra* note 88.

[91] *See* Bert-Jaap Koops Homepage-Crypto Law Survey, *Overview Per Country, Version 14.3, February 1999, Germany* (last modified Feb. 1, 1999) <http://cwis.kub.nl/~frw/people/koops/ cls2.htm#ge>.

[92] *See* Gleiss Lutz Hootz Hirsch, *Federal Government Remarks Concerning Encryption*, MONDAQ BUSINESS BRIEFING, Apr. 17, 1998, *available in* LEXIS, News Library, Mondaq File.

[93] *See id*.

Some U.S. political leaders have also criticized the amended Wassenaar regulations. One such leader is Republican Senator Conrad Burns, chairman of the Senate Commerce Communications Subcommittee and a champion of Senate Bill 377 (Promotion of Commerce On-Line in the Digital Era [Pro-CODE]), a bill that would loosen export controls on encryption and prohibit the federal government from restricting the domestic use of cryptography.[94] Burns criticized the Wassenaar restrictions by saying, "It is still baffling to people like me who view the Internet as an information revolution that should be allowed to grow and flourish that the Clinton-Gore Administration would work consistently to thwart the security backbone of electronic commerce and computer privacy."[95] Burns also declared that the administration "continues to live in this mythical world in which turning back the tide on technology and privacy is the policy tool of choice. If they think that getting a few countries to agree to their restrictions is going to get the job done in the Digital Age, they're farther down the primrose path than I thought."[96] Burns alleged further that the Clinton administration treats any law-abiding citizen who wants to participate in Internet activities as an "enemy of the state."[97]

The Clinton administration's impetus to control encryption around the world received a severe blow in January 1999 when France, a country having even stronger cryptographic controls than the United States (it restricted the domestic use of encryption), announced it was dropping all controls on cryptography up to 128-bits in strength.[98] On 19 January 1999 Prime Minister Lionel Jospin issued the following announcement:

> To change the orientation of our legislation, the government has adopted the following orientations, which I discussed with the President of the Republic:
>
> - to offer total freedom in the use of cryptography;

[94] *See* Robert MacMillan, *Burns, McCain To Tackle Encryption, Telecom*, NEWSBYTES, Dec. 11, 1998, *available in* LEXIS, News Library, Nwsbyt File.

[95] *International Export Group Wants New Encryption Ban,* COMM DAILY, Dec. 4, 1998, *available in* LEXIS, News Library, Comdly.

[96] *Id.*

[97] MacMillan, *supra* note 94.

[98] *See Conférence de presse de Monsieur Lionel JOSPIN, Premier ministre, à l'issue du Comité interministériel pour la société de l'information Hôtel de Matignon* [*Press Conference of Mr. Lionel Jospin, Prime Minister, on the issue of the Interministerial Committee on the Information Society, Hotel Matignon*], Jan. 19, 1999 (visited Feb. 22, 1999) <http://www. premierministre.gouv.fr/ PM/D190199.HTM>.

> - to remove the obligatory character of requiring the deposit of encryption keys with third parties;
>
> - to supplement the current legal authority with the introduction of obligations, together with penal sanctions, concerning the handing-over to judicial authorities, when required, of plain text transcriptions of encrypted documents. Additionally, the technical capacities of the public authorities will significantly be reinforced . . . .
>
> Changing the law will take several months. The government wanted the principal obstacles that deter citizens from protecting the confidentiality of their communications and stymie development of the electronic commerce mitigated. While waiting for the announced legislative modifications, the government has decided to raise the threshold of unrestricted cryptography from 40-bits to 128-bits . . . .[99]

France's new policy abolished its complex licensing scheme for cryptographic imports and domestic use, mandatory key registration requirements for the domestic use of encryption, and a system of government-approved trusted third parties.[100]

Prime Minister Jospin likened France's draconian encryption policies to the Second World War's Maginot Line, a military barricade along the French border with Germany that later proved completely ineffective. Criticizing the 1996 French law on cryptography, Jospin said that "[it] is no longer viable. It strongly holds back the usage of cryptography in France, and does not have any impact on allowing the authorities to effectively fight the criminal use of encryption."[101] Rather than impose key registration or escrow regulations, the government said it would sponsor legislation for criminal sanctions against suspects who refuse to decrypt data pursuant to a lawful court order.[102]

V. THE CANADIAN APPROACH

It is worthwhile to contrast the American approach on encryption to that of Canada. Early in 1998, the Canadians put forward a draft cryptography policy as part of its Electronic Commerce Strategy.[103] The document spelled out the government's approach to cryp-

[99] *Id.*

[100] *See id.*

[101] Kenneth Neil Cukier, *France Heralds Fall of its Crypto 'Maginot Line'*, COMM. WK. INT'L, Feb. 1, 1999, *available in* LEXIS, News Library, Curnws File.

[102] *See id.*

[103] *See* Government of Canada, *Minister Manley Outlines Canadian Cryptography Policy* (visited Mar. 29, 1999) <http://info.ic.gc.ca/cmb/welcomeic.nsf/261ce500dfcd72598525648200 68dc6d/85256613004a2e1785256690004c70fb?OpenDocument>.

tography use and invited the public to offer their own thoughts and proposals.[104] The Canadians framed their discussion around whether key recovery for stored data should be market driven, revolve around minimum government standards, or be subject to mandatory standards.[105] The other major component, real time communications (i.e., active, live communications), was also discussed.[106] The debate centered around whether the status quo should be maintained (i.e., no key recovery), statutory requirements on telecommunications providers should be implemented, or a public key infrastructure, in which key recovery would be an integral part of the national infrastructure of Canada, should be adopted.[107] Finally, the report asked for public comment on export controls. Three options were suggested: relaxation, status quo maintenance, or extension.[108] The Canadian approach represents a novel and refreshing method for starting a public dialogue on cryptography and one that should have been tried in the United States. The U.S. government missed an important opportunity to have a realistic public discussion on cryptography after the National Research Council released its 1996 report on cryptography policy, Cryptography's Role in Securing the Information Society (CRISIS Report).[109] At that time, the CRISIS Report accurately reflected the state of United States policy.

VI. THE LOSS OF MARKET SHARE

Commerce Secretary Daley's April 1998 speech highlighted the disagreements within the Clinton administration over strategy and tactics having to do with export controls on cryptographic products.[110] Daley's speech came at a time when the Economic Strategies Insti-

[104] *See* Industry Canada, Strategis, *Cryptography Policy Discussion Paper: Analysis of Submissions, Introduction* (last modified Sept. 28, 1998) <http:// strategis.ic.gc.ca/SSG/ cy01157e.html>.

[105] *See* Industry Canada, Strategis, *Cryptography Policy Discussion Paper: Analysis of Submissions, Analysis of Responses Part 2: Review of Narrative Responses* (last modified Sept. 28, 1998) <http://strategis.ic.gc.ca/SSG/cy01160e. html>.

[106] *See id.*

[107] *See id.*

[108] *See* Industry Canada, Strategis, *Cryptography Policy Discussion Paper: Analysis of Submissions, Analysis of Responses Part 1: Summary of Quantitative Results, Overall Position Towards Controls on Cryptography* (last modified Sept. 28, 1998) <http://strategis.ic.gc.ca/ SSG/cy01159e. html>.

[109] *See* COMPUTER SCIENCE AND TELECOMMUNICATIONS BOARD, NATIONAL RESEARCH COUNCIL, CRYPTOGRAPHY'S ROLE IN SECURING THE INFORMATION SOCIETY (Kenneth W. Dam & Herbert S. Lin eds., 1996).

[110] *See* Daley Speech, *supra* note 31.

tute (ESI) issued a report that, for the first time, came to grips with the economic loss suffered as a result of export controls.[111] The report stated that the U.S. economy could lose $97 billion over the next five years as a result of continued export controls on cryptographic products.[112] Furthermore, the ESI report also estimated "that American companies could lose an additional $140 billion in overseas sales, because foreign buyers will fear that their e-mails and phone calls could be compromised by U.S. intelligence services."[113]

This security fear has already manifested itself in India, for example. In January 1999, the Indian Defense Research and Development Organization (DRDO) issued a "red alert" letter to concerned parties in India expressing its concern about U.S. encryption software products that can be "broken" by the NSA.[114] The DRDO pointed out that "no encryption software products can be exported from the U.S. if they are too strong to be broken by the NSA."[115] The DRDO letter concluded by stating that the quality of such American software exported to India is questionable from a security point of view: "[t]o put it bluntly, only insecure software can be exported. When various multinational companies go around peddling 'secure communication software' products to gullible Indian customers, they conveniently neglect to mention this aspect of the U.S. export law."[116] In 1998, India announced the development of a sophisticated encryption program called Trinetra (ThirdEye), advertised as being as strong as the technology used by U.S. and NATO military forces.[117] If India offers this system, or a scaled-down version of it, to the international commercial marketplace, U.S. business will suffer even further.

To prevent adverse consequences to U.S. businesses, it is essential to begin a dialogue and study the adverse impact of U.S. export controls on cryptography. One German manufacturer of cryptographic products, Brokat Infosystems of Stuttgart, is ecstatic about

[111] *See* Erik R. Olbeter, *Encryption and Security*, J. OF COM., Aug. 6, 1998, at 7A.

[112] *See id.*

[113] *Id.*

[114] Mayur Shetty, *Red Alert Issued Against U.S. Network Software*, ECONOMIC TIMES (India), Jan. 12, 1999 (visited Mar. 10, 1999) <http://www.economictimes.com/120199/lead2.htm>.

[115] *Id.*

[116] *Id.*

[117] *See* Rahul Bedi, *India Develops Latest Secure Data System*, JANE'S DEF. WKLY. (Oct. 28, 1998), *available in* LEXIS, News Library, Jandef File.

current U.S. export controls.[118] The company is setting up virtual shopping malls all over Europe that use the 128-bits encryption currently restricted by U.S. export controls. It claims to have an encryption product market share of forty percent in Europe and ten to fifteen percent worldwide.[119] In addition, Brokat has plans to establish subsidiaries in Belgium and Singapore and is aggressively moving into the U.S. domestic market.[120]

Other countries are benefiting from the Clinton administration's insistence on strong cryptographic export controls. For example, from January to October 1999, the Irish Department of Trade reported that the government granted ninety-nine export licenses to Irish companies to export cryptographic products.[121] Recipients included China, Israel, Saudi Arabia, Taiwan, Qatar, and South Korea.[122]

In addition, Ireland has nurtured an off-shore cryptographic industry that is blossoming due to the continuation of U.S. export controls.[123] On 24 June 1998, the Irish government weighed in with a new cryptographic policy aimed at supporting domestic cryptographic vendors like Baltimore Technologies and its competitors, such as Systemics Ltd. of Dublin.[124] The Irish government cryptography policy rejects key escrow and recovery regimes in favor of court-ordered and warrant-based access to the plain text of encrypted data. Ireland's policy on the use of encryption technologies recognizes that an effective policy should achieve a balance between the rights of the individual in regard to privacy, the need to provide for security and integrity of communications, support for the cryptography industry in Ireland, and the requirements for lawful national security and law enforcement access to data.[125]

[118] *See BROKAT Enters the American Market*, ELECTRONIC COM. BRIEFING, Nov. 1, 1998, *available in* LEXIS, News Library, Curnws File.

[119] *See id.*

[120] *See id.*

[121] *See* Irish Department of Enterprise, Trade, and Employment, *Export Licensing* (last modified Mar. 10, 1999) <www.irlgov.ie/entemp/export>.

[122] *See id.*

[123] *See id.*

[124] *See* Department of Public Enterprise, *Framework for Ireland's Policy on Cryptography and Electronic Signatures* (last modified Mar. 29, 1999*)* <http://www.irlgov.ie/tec/communications/signat. htm>.

[125] *See id.* The policy comprises the following basic principles:

- Users shall have the right to access strong and secure encryption to ensure the confidentiality, security and reliability of stored data and electronic communications.
- Users shall have the right to choose any cryptographic method.

U.S. export controls directly led to the creation of communications security industries in both Finland and Estonia. Finland's Datafellows, a world-class cryptographic services company, was started in 1988; since that time it has doubled its net revenue.[126] Datafellows has strategic partnerships with Finland's Nokia; Sonera, the former Finnish Telecom; and Siemens-Nixdorf, the German information technology giant.[127] It is doubtful that Datafellows would have achieved such success without the imposition of export controls on American firms.

In 1993, Estonia's Forex bank launched an on-line banking service and was the first bank in Eastern Europe to offer home banking.[128] Soon, its major competitor, Hansabank, offered a similar service.[129] But Hansabank had one problem: U.S. export laws limited the encryption used by the banks to 40-bits, a situation they found totally unacceptable.[130] Both Forexbank and Hansabank began with external and foreign security consultants but quickly developed core skills, including in-house security.[131] The decision to cultivate an in-house technical base has paid off well. Now, Forexbank is considering spinning off its technology department to market its skills to rival banks in Estonia and neighboring countries.[132]

As with the two major Estonian banks, Latvian bank Trasta Komercbanka decided not to wait for amendments to U.S. export control laws before it could obtain strong encryption for its on-line

- The production, import and use of encryption technologies in Ireland shall not be subject to any regulatory controls other than obligations relating to lawful access.
- The export of cryptographic products is to continue to be regulated in accordance with the relevant EU Regulations and Decisions and Irish national legislation which reflect the Wassenaar Arrangement on Export Controls for Dual-Use Goods and Technologies and Conventional Arms.
- In order to enable lawful access to encrypted data, legislation will be enacted to oblige users of encryption products to release, in response to a lawful authorization, either plain text which verifiably relates to the encrypted data in question or the keys or algorithms necessary to retrieve the plain text. Appropriate sanctions will be put in place in respect of failure to comply.

[126] *See* Datafellows, *Integrated Solutions For Enterprise Security* (last modified Mar. 9, 1999) <http://www.datafellows.fi/df-info>.

[127] *See id*.

[128] *See Starting From Scratch*, DIRECT DELIVERY INT'L, Sept. 1997, *available in* LEXIS, News Library, Curnws File.

[129] *See id*.

[130] *See id*.

[131] *See id*.

[132] *See id*.

banking.[133] The Latvian bank obtained its encryption authentication cards from Lintel Security SA of Belgium, which uses DES-based AuthentiCards that are calculator-like devices used to secure customer-bank communications. AuthentiCards generate passwords, authentication codes and electronic signatures.[134]

In light of these developments, American businesses have established Americans for Computer Privacy (ACP), which has as its objective the Congressional passage of the Security and Freedom Through Encryption Act (SAFE).[135] The Act will loosen current export controls as well as forestall any attempt to impose domestic controls on encryption.[136] SAFE has significant private sector backing from groups as diverse as the National Association of Manufacturers, the U.S. Chamber of Commerce, and the Association of Floral Telegraph Delivery.[137] For the first time in American history, cryptography is becoming a full-blown political issue. During 1998, the ACP even took out political campaign-style television advertisements in major media markets to decry administration efforts to curb encryption.[138]

Some American firms are not waiting for congressional action to provide relief from export restrictions. Two recent public announcements from RSA and Network Associates represent the beginning of a trend by American companies to form foreign relationships that will allow them to compete better in the global encryption marketplace. In January 1999, RSA announced the establishment of its first overseas development center, RSA Data Security Australia Pty. Ltd., in Brisbane.[139] Network Associates, the American vendor for the PGP encryption program, has set up an international operations headquarters in the Netherlands and has made an arrangement with CNLabs of Switzerland to license PGP to foreign users.[140]

[133] *See* Trasta Komercbanka, *Internet Banking* (visited Mar. 10, 1999) <http://www.tkb.lv>.

[134] *See id.*

[135] Security and Freedom Through Encryption (SAFE) Act of 1997, H.R. 695, 105th Cong. (1997).

[136] *See id.*

[137] *See* Erik Espe, *Tech Firms Join Forces to Fight Encryption Ban*, 16 BUS. J. 1, 14 (1998).

[138] *See id.*

[139] *See* Amy Rogers, *RSA Australia Looks to Secure Sales*, COMP. RESELLER NEWS, Feb. 1, 1999, at 67.

[140] *Encryption Exporters Win One, Lose One; Commerce Department Loosens Some Regs, Court Upholds Others*, ELEC. COM. NEWS, July 20, 1998, *available in* LEXIS, News Library, Curnws File.

In addition, two international groups with responsibility for technical management and standards development for the Internet, the Internet Architecture Board (IAB), and the Internet Engineering Steering Group (IESG), have warned that the Internet will be "weak and vulnerable because of the restrictions recently implemented by the U.S. government on the export of encryption software."[141] The IAB and IESG stated that restrictions on encryption threaten both privacy and protection from criminal assaults on electronic commerce.[142] The groups, supported by the Internet Society,[143] also said that encryption controls will have a "negative impact" on developing countries because "many countries are new to the network and may lack the financial and technical strengths to develop their own cryptographic capabilities."[144]

The announcement of the revised Wassenaar regulations, coupled with the September 1998 Clinton administration decision to relax cryptography controls to certain sectors in forty-five countries and the December 1998 revision of Bureau of Export Administration controls, indicate one important development in the U.S. plan: to restrict the use of cryptography.[145] Rather than relying on technical solutions such as key escrow and key recovery schemes, the administration and its international allies fell back on traditional methods of control: export controls, limitations on key lengths, government licensing, and mutual legal assistance treaties.[146] This choice represented a major change, albeit regressive, in the administration's thinking.

VII. CONCLUSION

The arguments of those who support the freedom to engage in secure communications and data processing are well-founded. Consequently, it is time to have a serious discussion on public policy to-

[141] *Encryption Restrictions Make Internet Weak, Says IAB/IESG Joint Statement*, TELECOMWORLDWIRE, Dec. 25, 1998, *available in* LEXIS, News Library, M2tww File.

[142] *See id.*

[143] The Internet Society is a non-governmental international organization that promotes the global development of the Internet. *See* Internet Society, *All About the Internet Society* (last modified Jan. 19, 1999) <http://www.isoc.org/isoc/mission>.

[144] *Encryption Exporters Win One, Lose One; Commerce Department Loosens Some Regs, Court Upholds Others, supra* note 141.

[145] U.S. Dep't Com., Bureau of Export Administration, *Commerce Updates Export Controls on Encryption Products* (last modified Feb. 25, 1999) <http://www.bxa.doc.gov/press/98/1230encryption. html>.

[146] *See id.*

ward encryption and the inherent balance issues that arise with such a discussion. Cryptography is necessary to protect both our critical infrastructures and our national economic well-being.

With the advent of the computer revolution and recent innovations in the science of encryption, a new market for cryptographic products has developed. The United States should nurture rather than impede this market as secure electronic communications networks have become an integral component of the global economy. Because computers store and exchange an ever-increasing amount of corporate-sensitive and highly personal information, including medical and financial data, it is necessary to secure such information from unauthorized eavesdropping and malicious alteration. Communications applications, such as electronic mail, electronic fund transfers, and on-line purchasing, require secure means of encryption and authentication. Such features can only be provided if cryptographic know-how is widely available and unencumbered by government regulation and outdated export controls.