University of Minnesota Law School
Scholarship Repository

Minnesota Journal of International Law

1998

The U.S. Encryption Export Policy: Taking the Byte out of the Debate

Mai-Tram B. Dinh

Follow this and additional works at: https://scholarship.law.umn.edu/mjil

 Part of the Law Commons

Recommended Citation

Dinh, Mai-Tram B., "The U.S. Encryption Export Policy: Taking the Byte out of the Debate" (1998). *Minnesota Journal of International Law*. 37.
https://scholarship.law.umn.edu/mjil/37

This Article is brought to you for free and open access by the University of Minnesota Law School. It has been accepted for inclusion in Minnesota Journal of International Law collection by an authorized administrator of the Scholarship Repository. For more information, please contact lenzx009@umn.edu.

Notes

The U.S. Encryption Export Policy: Taking the Byte Out of the Debate

Mai-Trâm B. Dinh

Today, the Internet is one of the fastest-growing vehicles for commerce. With billions of dollars at stake, it is not surprising that any controversy concerning Internet commerce will elicit heated debate from interested parties. The U.S. encryption export policy has been no exception. The government has imposed restrictions on the export of encryption software, with the goal of safeguarding national security. The Clinton administration has instituted the policy over the objection of encryption software developers, who argue that its restraints will hamper their ability to compete in the international market.

This Note argues that while the U.S. encryption export policy may not be ideal, no alternative achieves a better balance of interests in privacy, economic growth, and national security. Section I explains the background of the Internet as a vehicle for electronic commerce (e-commerce) and outlines the U.S. policy statement concerning e-commerce. Section II describes the U.S. encryption export policy. Section III sets forth the effects of encryption technology on e-commerce and analyzes the export policy in the context of the United States' stated goals. Finally, Section IV explains why criticism of the current policy is unwarranted.

I. ENCRYPTION REGULATION ON THE INFORMATION SUPERHIGHWAY

Before discussing the details of the U.S. encryption export policy, it is essential to understand the advent of the "information superhighway" and the Internet's role in commerce. It is also important to explain encryption technology and the history of its regulation.

A. THE "INFORMATION SUPERHIGHWAY"

The Internet consists of a world-wide network of computers.[1] In 1969, the U.S. government established the first computer network, ARPANET, as a Department of Defense initiative to link important research and command sites.[2] The Internet, which evolved out of ARPANET, is a collection of more than 10,000 independent computer networks spanning more than fifty countries.[3] The Internet has no central control because it was designed to maintain a means of communication between incompatible computer systems in the event of a catastrophic attack.[4] Although it has since outgrown its military roots, this decentralized structure is still a key feature of the Internet.

President Clinton has hailed the Internet as an innovation that "has done more to shape and create the world our children will inherit than virtually any invention since the printing press."[5] He has predicted that within a generation, entire collections of books, symphonies, movies, and art will be within every child's reach on home or school computer screens, thereby revolutionizing education.[6]

The Internet is already changing the way American companies do business. Trade on the Internet is doubling or tripling every year, and projections only a few years into the future suggest that it will generate hundreds of billions of dollars of trade in goods and services[7] and help "fuel economic growth well into the 21st century."[8] One analyst predicts that financial transac-

---

1. *See generally, e.g.*, ED KROL, THE WHOLE INTERNET USER'S GUIDE AND CATALOG 13-21 (2d ed. 1994); HARLEY HAHN & RICK STOUT, THE INTERNET COMPLETE REFERENCE 1-2 (1994).

2. *See* KROL, *supra* note 1, at 13. The acronym ARPANET stands for the network developed by the Department of Defense's Advanced Research Project Agency. *See* Andrew Grosso, *The National Information Infrastructure*, 41 FED. BAR NEWS & J. 481, 481 (1994). The Defense Advanced Research Project Agency oversaw the administration of the Internet until 1983. *See* Gary Chapman, *Is the Internet a Matter of National Security?*, L.A. TIMES, Sept. 22, 1997, at D6.

3. *See generally* KATIE HAFNER & MATTHEW LYON, WHERE WIZARDS STAY UP LATE (1996).

4. *See* KROL, *supra* note 1, at 13; Chapman, *supra* note 2, at D6.

5. *Remarks Announcing the Electronic Commerce Initiative*, 33 WEEKLY COMP. PRES. DOC. 1003, at 1004 (July 1, 1997).

6. *See id.*

7. *See id.*

8. *Memorandum on Electronic Commerce*, 33 WEEKLY COMP. PRES. DOC. 1006, at 1007 (July 1, 1997).

tions on the Internet could foster the growth of electronic commerce from $3 billion in 1997 to $1 trillion by 2010.[9]

The Internet presents great opportunities to small and large businesses alike. Companies of all sizes find the low operating costs and access to millions of consumers around the world attractive. Entrepreneurs can start businesses more easily and access a worldwide network of potential customers without a large amount of capital.[10] The Internet is expected to revolutionize retailing by allowing consumers to shop from home for a wide variety of products and services, offered by sellers worldwide and around-the-clock[11]— and to change business practices by allowing companies to operate more efficiently both internally and with suppliers and customers.[12] The number of medium-sized and large companies using e-commerce "will grow by more than 50% [in 1998,] to include nearly two-thirds of U.S. companies."[13] Currently, an estimated 35 million consumers and 190,000 businesses are connected to the Internet.[14] Most forecasters predict that by the year 2000, hundreds of millions of people worldwide will use the Internet.[15]

---

9. *See Online Payments Gain Appeal*, INTERNET MAG., Oct. 1997, at 29.

10. *See* THE WHITE HOUSE, A FRAMEWORK FOR GLOBAL ELECTRONIC COMMERCE, at 2 (July 1, 1997). [hereinafter FRAMEWORK]. This document is available in book form and also at <http://www.iitf.nist.gov/eleccomm/ecomm.htm>.

11. *See id.*; *see also* David Baum, *Fast Track to E-Commerce*, ORACLE MAGAZINE, Jan./Feb. 1998, at 46, 48.

12. *See Memorandum on Electronic Commerce*, *supra* note 8, at 1007.

13. Clinton Wilder, *E-Commerce Gains Support as Companies Watch Profits*, INFORMATIONWEEK, Dec. 1, 1997, at 32.

14. *See* Craig W. Harding, *Selected Issues in Electronic Commerce: New Technologies and Legal Paradigms*, *in* DOING BUSINESS ON THE INTERNET 7, 9 (Practising Law Institute ed., 1997).

15. Estimates of the number of future Internet users vary significantly. *See, e.g.*, Kara Swisher, *There's No Place Like a Home Page*, WASH. POST, July 1, 1996, at A1 (52 million); John Zarocostas, *Limitations of Statutes*, J. COMM, May 14, 1997, at 1C (90-120 million); James Champy, et al., *Creating the Electronic Community*, INFORMATIONWEEK, June 10, 1996, at 57, 64 (170 million); Camille DeMarzo, *Year in Review*, COMPUTER RESELLER NEWS, Nov. 18, 1996, at 267, 278 (300 million); *Fraud on the Internet: Statement Before the Permanent Subcomm. on Investigations of the Senate Comm. on Government Affairs*, Feb. 10, 1998, *available in* 1998 WL 51659 (F.D.C.H.) (1998) (statement of Sen. Susan M. Collins) (500 million); Mary Hayes, *Working Online, Or Wasting Time?*, INFORMATIONWEEK, May 1, 1995, at 38, 44 (700 million). The explanation for the disparity in estimates may lie in how "Internet use" is defined: one study measuring "true, actual Internet use, not simply e-mail use or potential Internet access," resulted in an estimate of 25.4 million users by 2000. *Find/SVP Estimates 9.5 Million "True" Internet Users*, NEWSBYTES, June 11, 1996, *available in* LEXIS, News Library, Wires File.

Digitized information on the Internet includes on-line copies of computer programs, information sources, literature, videos, and music.[16] A retail consumer may search the Internet for the information he or she seeks, pay for it using electronic cash,[17] and then download it onto his or her computer. Other businesses which are proliferating on the Internet include those in the fields of information, financial, and technical services; professional consulting; educational ventures; medical diagnostics; and advertising.[18] The types of goods and services that can be bought and sold electronically are essentially unlimited.

As businesses and consumers participate in the electronic marketplace, they are developing new forms of commercial interaction which are modifying traditional business and economic practices.[19] The transfer of digitized information through the Internet raises trade issues that are unique to electronic commerce. Because the Internet is composed of independent computer networks which have no central control,[20] it is difficult to regulate. Additionally, while some Internet transactions are readily compared to non-electronic transactions,[21] the transfer of digitized information has no easily discernible parallel in the non-electronic realm. Thus, regulatory frameworks established for telecommunications, radio, and television may not fit the needs of the Internet or our "new electronic age."[22] As one European commissioner has said, "[i]t is ironic, but the possibilities of the Internet make it impossible to regulate."[23]

---

16. *See* James D. Cigler & Susan E. Stinnett, *Treasury Seeks Cybertax Answers with Electronic Commerce Discussion Paper*, 8 J. INT'L TAX'N 56, 61 (Feb. 1997). *See generally, e.g.*, Visa Shopping Guide (visited Mar. 10, 1998), <http://shopguide.yahoo.com>; Excite Shopping (visited Mar. 10, 1998), <http://www.excite.com/channel/shopping>.

17. Electronic cash (e-cash) is used by on-line banks and consumers as a currency that can be electronically negotiated for goods and services. *See* David Post, *E-Cash: Can't Live With It, Can't Live Without It*, AM. LAW., Mar. 1995, at 116, 116 (describing e-cash as "digital tokens accepted as the equivalent of legal tender"). E-cash is made secure through the use of encryption technology, which can prevent forgery and protect consumer privacy. *See id.*

18. *See Memorandum on Electronic Commerce*, *supra* note 8, at 1007.

19. *See* FRAMEWORK, *supra* note 10, at 2.

20. *See supra* text accompanying note 4.

21. For example, product orders placed on the Internet can be analogized to orders placed by mail or telephone.

22. FRAMEWORK, *supra* note 10, at 5.

23. Matthew Slater, *Europeans Clash with U.S. over Encryption*, TECHWIRE, Oct. 9, 1997, *available in* LEXIS, News Library, Wires File.

B. ENCRYPTION[24]

In order for electronic commerce to develop to its full economic potential, consumers and businesses must be assured that their communications will not be intercepted or modified.[25] Additionally, businesses want to avoid the release of confidential information to their competitors.[26] Encryption technology makes the achievement of these goals possible. Encryption software applies a mathematical function, called an algorithm, to scramble e-mail messages, computer files, telephone conversations, and other data to render them unreadable by unintended recipients such as spies and thieves.[27] Encryption products protect the confidentiality of electronically transmitted or stored data and communications by "converting plain text into cipher text, an unreadable string of numbers and letters."[28] The algorithm which is used to unscramble, or decrypt, the message is called a decryption key.[29]

The strength of an encryption algorithm depends on the length of its key, which is measured in bits, and the complexity of the algorithm.[30] Each bit doubles the number of possible key sequences; thus, as the number of bits increases, the encryption becomes dramatically stronger.[31] For example, a 40-bit key permits more than a trillion possible combinations, while a 56-bit

---

24. This Note offers only a basic discussion of encryption. For more comprehensive background material on the subject, see e.g., Adam C. Bonin, *Protecting Protection: First and Fifth Amendment Challenges to Cryptography Regulation*, 1996 U. CHI. LEGAL F. 495; A. Michael Froomkin, *The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709 (1995); and Thinh Nguyen, Note, *Cryptography, Export Controls, and the First Amendment in* Bernstein v. United States Department of State, 10 HARV. J. LAW & TECH. 667 (1997).

25. *See* Charles R. Merrill, *Proof of WHO, WHAT, and WHEN in Electronic Commerce Under the Digital Signature Guidelines, in* DOING BUSINESS ON THE INTERNET 133, *supra* note 14, at 136.

26. *See* Bradley D. Brown, *Securing Transactions in Network Applications*, ORACLE MAG., Jan./Feb. 1998, at 91, 91.

27. *See* Willie Schatz, *The Government Eyes Encryption*, INFORMATIONWEEK, Sept. 8, 1997, at 60; *see also* Stewart A. Baker, *Decoding the OECD's Guidelines for Cryptography Policy, in* DOING BUSINESS ON THE INTERNET 265, *supra* note 14, at 267.

28. Wendy R. Leibowitz, *Battle over Encryption Export Flares*, NAT'L L.J., Sept. 29, 1997, at A1; *see also* Baker, *supra* note 27, at 267.

29. *See* Baker, *supra* note 27, at 267.

30. *See id.*

31. *See* COMPUTER SCIENCE AND TELECOMMUNICATIONS BOARD, NATIONAL RESEARCH COUNCIL, CRYPTOGRAPHY'S ROLE IN SECURING THE INFORMATION SOCIETY 63 (Kenneth W. Dam & Herbert S. Lin eds., 1996) [hereinafter NRC REPORT].

key permits more than 72 quadrillion possible combinations.[32] Longer keys complicate a brute-force decoding attack, which relies on trial and error.[33] More complex algorithms hamper mathematical attacks and thus require differential cryptanalysis.[34]

Encryption is used for three primary reasons: "to ensure the confidentiality of data, [to] authenticate data, and to ensure its integrity."[35] Encryption ensures the confidentiality of data by preventing computer users other than the proper recipient from decoding the message.[36] It authenticates data by allowing a recipient to confirm that a particular sender transmitted the communication—usually by the use of a digital signature.[37] Authentication can confirm that the message was not a forgery; it can also be used to prevent the sender from later denying that he or she actually sent the message.[38] Encryption ensures data integrity by allowing a recipient to confirm that the message was not altered in transit.[39]

With the "key escrow" system, also known as "key recovery,"[40] independent "trusted" third parties[41] hold encryption key

32. *See* Peter Coffee, *No Crypto Is Too Tough to Crack*, PC WEEK, Sept. 29, 1997, at 16, 16.

33. *See id.*

34. *See id.* "Differential cryptanalysis compares differences between encrypted files against differences between their plain-text files." *Id.*

35. Baker, *supra* note 27, at 267.

36. *See id.*

37. *See id.* at 268. Digital signing is usually accomplished when a signer "encrypts the information with his or her private key, thereby 'signing' the document." *Id.*

38. *See id.*

39. *See id.* This is achieved through the use of hash functions, which reduce the length of the information and thereby produce a condensed "message digest." The sender encrypts and sends both the original message and the message digest. The receiver then applies the same hashing algorithm to the received text to create a second message digest. If the second digest matches the original digest, then the recipient knows that the message was not altered. *See id.*

40. *See* Harding, *supra* note 14, at 14. *See also infra* text accompanying notes 85-92.

41. Examples of trusted third parties—also known as key recovery agents—include private companies, banks, or other commercial or government entities that meet statutory criteria for trustworthiness. *The Impact of Encryption on Public Safety: Statement Before the Subcomm. on Technology, Terrorism, and Government Information of the Senate Comm. on the Judiciary*, 105th Cong. (Sept. 3, 1997) (statement of Louis J. Freeh, Director, Federal Bureau of Investigation) [hereinafter *Impact of Encryption Statement*]. A key recovery agent must certify that individuals who will have access to keys are suitable and trustworthy, as indicated by having no record of criminal convictions or pending criminal charges, never having breached any fiduciary responsibilities,

codes on all encryption software shipped internationally.[42] These outside parties can use the keys to decode messages for law enforcement agencies if the government suspects illegal activities and obtains court approval to execute a wiretap.[43]

C. ENCRYPTION REGULATION IN THE UNITED STATES

Until recently, the Department of State regulated encryption technology as a munition.[44] At the end of 1996, in recognition of its value in legitimate commercial and communications contexts and to simplify and accelerate the licensing procedure, jurisdiction for licensing of encryption exports was transferred to the Department of Commerce.[45] The Department of Commerce, pursuant to the Export Administration Act[46] and the Export Administration Regulations (EAR),[47] now regulates the export of all commercial encryption products.[48]

---

and having a favorable credit record; an active U.S. government security clearance at the Secret level or higher, issued or updated within the last five years, will also suffice. *See* Key Escrow or Key Recovery Agent Criteria, Security Policies, and Key Escrow or Key Recovery Procedures, 15 C.F.R. § 742, Supp. 5 (1997). The key recovery agent itself must submit evidence of its viability and economic security through documents such as a certificate of good standing from the state of incorporation, credit reports, and errors/omissions insurance. *See id.* An agent must also disclose whether any of the following have occurred within the ten years prior to the application: a felony conviction of the business, a material adverse civil fraud judgment or settlement, or a debarment from government contracting. *See id.*

42. *See* Charlotte Dunlap, *Global Web Policy Nets Some Support*, COMPUTER RESELLER NEWS, Sept. 15, 1997, at 34, 34.

43. *See* Geoffrey R. Greiveldinger, *Digital Telephony and Key-Escrow Encryption Initiatives: A Critical Juncture as Law Enforcement Agencies Work to Save Electronic Surveillance*, 41 FED. B. NEWS & J. 505, 508 (Aug. 1994).

44. *See* Exec. Order No. 13,026, 61 Fed. Reg. 58,767 (1996) (Administration of Export Controls on Encryption Products); *see also* United States Munitions List, 22 C.F.R. § 121.1 (1997); 22 U.S.C. § 2778 (1994) (prescribing administration of the United States Munitions List).

45. *See* Exec. Order No. 13,026, *supra* note 44; Encryption Export Policy Presidential Press Release (Nov. 15, 1996), *available at* <http://www.bxa.doc.gov/m961115.htm> [hereinafter Encryption Press Release]; *see also* David Aaron, U.S. Special Envoy for Cryptography, *International Views of Key Recovery*, Comments at RSA Data Security Conference (Jan. 28, 1997), *available at* <http://www.bxa.doc.gov/aaron.htm>.

46. Pub. L. No. 96-72, 93 Stat. 503 (codified as amended in scattered sections of 50 U.S.C. app. §§ 2401-2420 (1994)).

47. 15 C.F.R. §§ 730-74 (1997).

48. *See* Harding, *supra* note 14, at 14; *see also* Encryption Press Release, *supra* note 45; United States Munitions List, 22 C.F.R. § 121.1, Category XIII(b) (1997).

Although Americans can use any encryption system domestically,[49] in 1996 President Clinton announced a qualified ban on the export of strong encryption which prevents law enforcement agencies from accessing plain-text versions of the messages and data sent over the Internet.[50] The government's primary concern is that the use of encryption outside the United States will threaten U.S. foreign policy and national security objectives.[51] The detection and prosecution of criminals such as terrorists and drug traffickers is hindered when they employ data-scrambling technology to mask their activities.[52] From 1995 to 1996, the number of instances in which criminals' use of encryption frustrated the Federal Bureau of Investigation's (FBI) court-authorized electronic surveillance efforts increased more than two-fold.[53] Additionally, recent international terrorism attacks display a "trend toward . . . large-scale incidents designed for maximum destruction, terror, and media impact," thereby placing more Americans at risk, both at home and abroad.[54]

While domestic law enforcement agencies also harbor concerns about the use of encryption to conceal criminal activity, the Clinton administration has drafted the encryption export restrictions primarily with an eye to foreign policy; the restrictions are intended to protect the United States against national security threats.[55] The profound effect of encryption regulation on U.S. international competitiveness, the growth of global electronic commerce, and the privacy of data and communications in

---

49. *See* Aaron, *supra* note 45.

50. Exec. Order No. 13,026, *supra* note 44. "Strong" encryption software refers to programs with key lengths of more than 40 bits. *See* William A. Hodkowski, *The Future of Internet Security: How High Technologies Will Shape the Internet and Affect the Law*, 13 SANTA CLARA COMPUTER & HIGH TECH. L.J. 217, 234 (1997). The Data Encryption Standard (DES), now widely used, utilizes a 56-bit key. *See id.*

51. *See* Encryption Press Release, *supra* note 45.

52. *See* Paula Rooney, *Gore Tells SPA Attendees Not to Expect Change to U.S. Encryption Export Policy*, COMPUTER RETAIL WEEK, Sept. 15, 1997, at 2, 2.

53. *See World Wide Threats to U.S. National Security: Hearing Before the Senate Select Comm. on Intelligence*, 105th Cong. (1998) (statement of Louis J. Freeh, Director, Federal Bureau of Investigation), *available at* 1998 WL 8991513 [hereinafter *World Wide Threats Hearing*]. The number of instances increased from five to twelve. *See id.*

54. *Id.*

55. *See generally* Encryption Press Release, *supra* note 45. The U.S. national security concerns include the protection of U.S. citizens in the United States and abroad, as well as the safety of citizens of other countries. *See id.*

business and personal contexts influenced the narrow tailoring of the encryption restrictions.[56]

D. PRINCIPLES OF THE U.S. FRAMEWORK FOR GLOBAL ELECTRONIC COMMERCE

On July 22, 1994, representatives from the United States and the Russian Federation signed a Memorandum of Understanding on the Global Information Infrastructure (GII) Initiative.[57] One of its goals was the formation of a "mutual exchange and sharing of information on objectives and priorities" for developing information superhighways.[58] The "information superhighway" refers to the concept of merging all sources of information into a single database, retrievable from any computer by users in their homes, offices, or libraries.[59]

After a two-year study on the commercial potential of computer networks,[60] the Clinton Administration developed the Framework for Global Electronic Commerce ("Framework") to discuss the commercial implications of the GII.[61] The Adminis-

---

56. *See generally id. See also infra* text accompanying notes 114-24.

57. *U.S. Signs Understanding with Russia on Global Information Infrastructure*, 11 Int'l Trade Rep. (BNA) No. 32, at 1249 (Aug. 10, 1994). Signing the agreement for the United States were the U.S. Coordinator for Communications and Information Policy, the Chairman of the Federal Communications Commission, and the Assistant Secretary of Commerce for Communications and Information. *See id.* The Russian signatories included the Minister of Post and Telecommunications and the Chairman of the Presidential Committee of the Russian Federation for "Informatization" Policy. *See id.*

58. *Id.*

59. See Al Gore, *Networking the Future: We Need a National "Superhighway" for Computer Information*, WASH. POST, July 15, 1990, at B3. Vice President Gore is credited with coining this phrase in Note, *The Message in the Medium: The First Amendment on the Information Superhighway*, 107 HARV. L. REV. 1062, 1062 n.3 (1994).

60. *See* Mark Rockwell, *Clinton Policy: No Taxes, No Regs on 'Net Commerce,'* COMMUNICATIONSWEEK, July 7, 1997, at 9, 9.

61. *See* FRAMEWORK, *supra* note 10. The interagency group which worked on the Framework on behalf of the Administration consisted of high-level representatives of Cabinet agencies, including the Departments of Treasury, State, Justice, and Commerce; representatives of the Executive Office of the President including the Council of Economic Advisors, the National Economic Council, the National Security Council, the Office of Management and Budget, and the Office of Science and Technology Policy; the Office of the Vice-President; the U.S. Trade Representative; and independent commissions including the Federal Communications Commission and the Federal Trade Commission. *See* Walter A. Effross, *Putting the Cards Before the Purse?: Distinctions, Differences, and Dilemmas in the Regulation of Stored Value Card Systems*, 65 UMKC L. REV. 319, 333 n.43 (1997). Ira Magaziner, senior adviser to the President for policy development, authored the Framework. *See* Dunlap, *supra* note 42, at 34.

tration stated that "no single force embodies our electronic transformation more than the evolving medium known as the Internet."[62] The Framework, released on July 1, 1997,[63] outlines the U.S. plan for using the Internet to facilitate international commerce—a plan which considers policy principles, guidelines for international negotiation, and agency involvement.[64]

In order to fully recognize the Internet's potential for prosperity, the Framework seeks to establish a global free-trade zone for electronic commerce.[65] The United States "encourage[s] all nations to refrain from imposing discriminatory taxes, tariffs, unnecessary regulations, [and] cumbersome bureaucracies on electronic commerce."[66] The Administration has announced its dedication to keeping the Internet market-driven as opposed to government-regulated,[67] clearly stating that regulation of e-commerce will hinder the Internet's development in the global economy.[68] The Framework's ultimate goal is to create "a predictable [and] consistent legal environment . . . [in which electronic] trade and commerce . . . [may] flourish on fair and understandable terms."[69] To provide guidelines for meeting this goal, the Framework articulates five principles.

1. "The private sector should lead."[70]

The Clinton administration recognizes that the private sector has driven the expansion of the Internet and that innovation, expanded services, widespread participation, and greater efficiency result from a market-driven environment.[71] Thus, where government action is necessary, the private sector should participate in the policy making process.[72]

---

62. FRAMEWORK, *supra* note 10, at 1.

63. *See* FRAMEWORK, *supra* note 10.

64. *See generally id.*

65. *Remarks Announcing the Electronic Commerce Initiative*, *supra* note 5, at 1005.

66. *See id.* In his announcement of the electronic commerce initiative on July 1, 1997, President Clinton directed United States Trade Representative Charlene Barshefsky to "work within the . . . World Trade Organization, to turn the Internet into a free-trade zone" by July 1, 1998. *Id.*

67. Dunlap, *supra* note 42, at 34.

68. *See* Rockwell, *supra* note 60, at 9.

69. *Remarks Announcing the Electronic Commerce Initiative*, *supra* note 5, at 1005.

70. FRAMEWORK, *supra* note 10, at 4.

71. *See id.*

72. *See id.*

2. *"Government should avoid undue restrictions on electronic commerce."*[73]

The Clinton Administration recognizes that unnecessary regulation of commercial activities will hinder development of the electronic marketplace and has stated that "government attempts to regulate are likely to be outmoded by the time they are finally enacted, especially to the extent such regulations are technology-specific."[74] In his announcement of the Framework, President Clinton asked Vice President Gore to oversee the country's progress in meeting the initiative, directed all federal department and agency heads to review their policies to ensure they were consistent with the Framework's principles, and instructed the Treasury Secretary to avoid "new discriminatory taxes on electronic commerce."[75]

3. *"Where governmental involvement is needed, its aim should be to support and enforce a predictable, minimalist, consistent, and simple legal environment for commerce."*[76]

In some cases, consumer protection or facilitation of electronic commerce may require government involvement.[77] In those situations, governments should establish a legal environment based on a "decentralized, contractual model of law rather than one based on top-down regulation"[78] to enhance private-sector participation.

4. *"Governments should recognize the unique qualities of the Internet."*[79]

Laws and regulations which may burden electronic commerce should be modified or eradicated.[80] The government should impose only those regulations which achieve widely-accepted goals.[81]

---

73. *Id.*
74. *Id.*
75. *See Remarks Announcing the Electronic Commerce Initiative*, *supra* note 5, at 1005.
76. FRAMEWORK, *supra* note 10, at 5.
77. *See id.*
78. *Id.*
79. *Id.*
80. *See id.*
81. *See id.* For example, President Clinton directed the Commerce Secretary to establish basic consumer and copyright protections for the Internet. *See Remarks Announcing the Electronic Commerce Initiative*, *supra* note 5, at 1005.

5. "Electronic commerce over the Internet should be facilitated on a global basis."[82]

The Framework calls for the application of coherent principles across state and national borders.[83] The goal is a system which will produce consistent results notwithstanding the jurisdiction of the particular buyer or seller.[84]

II. THE U.S. ENCRYPTION EXPORT POLICY

The Commerce Department generally requires that encryption exporters obtain a license for each encryption export; however, the Department may grant a license exception for certain encryption items after the exporting entity passes a one-time review.[85] For example, mass-market software that uses algo-

82. FRAMEWORK, *supra* note 10, at 5.

83. *See id.*

84. *See id.*

85. *See* Harding, *supra* note 14, at 14, citing Stewart A. Baker & Michael Hintze, *United States Policy on Encryption Technology*, 3 COMPUTER & TELECOMS L. REV. 109 (1997). The "export" of encryption source code includes "downloading, or causing the downloading of, such software to locations (including electronic bulletin boards, Internet file transfer protocol, and World Wide Web sites) outside the U.S., or making such software available for transfer outside the United States, over wire, cable, radio, electromagnetic, photooptical, photoelectric or other comparable communications facilities accessible to persons outside the United States . . . unless the person making the software available takes precautions adequate to prevent unauthorized transfer of such code outside the United States." Important EAR Terms and Principles, 15 C.F.R. § 734.2(b)(9) (1997). "License" refers to the Bureau of Export Administration's (BXA) authorization of an export. *See* Export Administration Regulations, Definition of Terms, 15 C.F.R. § 772 (1997). Licenses for encryption items are required for all destinations except Canada. *See* Encryption Items, 15 C.F.R. § 742.15(a) (1997). "License exception" refers to "[a]n authorization described in § 740 of the EAR [allowing one] to export . . . under stated conditions, items subject to the EAR that would otherwise require a license." 15 C.F.R. § 772.

The encryption export regulations might seem to contravene the fundamental objective of the General Agreement on Tariffs and Trade (GATT), which is the "reduction of tariffs and other barriers to trade." General Agreement on Tariffs and Trade, *opened for signature* Oct. 30, 1947, 61 Stat. A-11, T.I.A.S. 1700, 55 U.N.T.S. 188. However, the export policy seems to fall under GATT's security exception, Article XXI. Article XXI relates to fissionable materials or the materials from which they are derived; traffic in arms, ammunition, and implements of war; traffic in goods and materials conducted to supply a military establishment; actions taken in time of war or other international relations emergency; and actions taken by a country pursuant to its obligations under the United Nations Charter "for the maintenance of international peace and security." *Id.*

The President's inherent powers include his "plenary and exclusive power . . . as the sole organ of the federal government in the field of international relations." United States v. Curtiss-Wright Export Corp., 299 U.S. 304, 320

rithms with forty or fewer bits may be exempted, after a one-time review, from the usual licensing procedures which require key-recovery.[86] Additionally, U.S. software manufacturers may also receive a license exception allowing them to export highly secure 56-bit DES[87] or equivalent encryption products for two years without key-recovery.[88] This is known as "License Exception KMI" (Key Management Infrastructure).[89] To qualify for this exception, manufacturers must commit to an acceptable plan to have keys developed and escrowed by the end of 1998.[90] U.S. manufacturers may export encryption software programs of any strength and key length as long as they provide a key to the government.[91] Thus, current policy prohibits U.S. software ven-

(1936). Thus, it is probably within the Administration's discretion to institute the encryption export policy as a measure to protect the nation from terrorists and foreign espionage.

86. *See* 15 C.F.R. § 742.15(a)(1). "Mass market" describes software that is "available to the public . . . at retail selling points . . . [and is] designed for [user] installation . . . without substantial support by the supplier." Guidelines for Submitting a Classification Request for a Mass Market Software Product that Contains Encryption, 15 C.F.R. § 742, supp. 6, at (a)(1)(i)-(ii) (1997). Substantial support means technical support more intensive than telephone help-line services or basic operation training. *See id.* at (a)(1)(ii).

87. The Data Encryption Standard, or DES, a widely-used 56-bit encryption system, was originally developed by IBM. *See* Hodkowski, *supra* note 50, at 227 n.82. In 1977, the U.S. government endorsed it as an official standard, and it has been periodically recertified by the National Institute of Standards and Technology. *See id.*

88. *See* 15 C.F.R. § 742.15(b)(3); *see also* Review Criteria for Exporter Key Escrow of Key Recovery Development Plans, 15 C.F.R. § 742, supp. 7 (1997).

89. *See* Key Management Infrastructure, 15 C.F.R. § 740.8 (1997). *See also generally* Harding, *supra* note 14, at 14; *The Security and Freedom Through Encryption (SAFE) Act: Hearing on H.R. 695 Before the Subcomm. on Telecommunications, Trade, and Consumer Protection of the House Comm. on Commerce*, 105th Cong. 55 (1997) (statement of William A. Reinsch, Undersecretary of Commerce for Export Administration) [hereinafter *Reinsch Hearing*].

90. *See* 15 C.F.R. § 740.8(d)(2)(i); *see also* 15 C.F.R. § 742.15(b)(3)(i); 15 C.F.R. § 742, supp. 7. The BXA conducts a complete case-by-case analysis of the license application, along with any documentation submitted in support of the application, to "determine whether the export . . . is consistent with U.S. national security and foreign policy interests." 15 C.F.R. § 742.15(b). In addition to reviewing the item and its use, the BXA assesses the commitment of the applicant to developing a key management infrastructure. *See* 15 C.F.R. § 742.15(b)(3)(i); 15 C.F.R. § 742, supp. 7. The BXA may consult with other U.S. departments and agencies regarding the license application. *See* 15 C.F.R. § 742.15(b). Each grant of License Exception KMI remains valid for six months. *See* 15 C.F.R. § 740.8(d)(2). An encryption exporter may request renewal of the license exception by sending a letter to the BXA every six months, reporting that it has progressed in meeting the milestones set forth in the exporter's plan to provide key recovery products and services. *See id.*

91. *See* 15 C.F.R. § 740.8(b)(1); 15 C.F.R. § 742.15(b)(2). The BXA would grant this license exemption after a single review of the plan by the Depart-

dors from exporting software with more than forty bits of encryption unless the vendors provide the government with decryption keys or commit to providing such keys within two years.[92]

III. TOWARD A SOLUTION

A. PROTECTION OF DATA WITH ENCRYPTION

Because experts concede that foreign governments and terrorists present a small, but growing, risk to U.S. data network security, a prudent policy should satisfy both the commercial need for data protection and the law enforcement need for access to messages containing information that may assist in preventing or solving crimes. The United States' current policy, which requires key escrow and relaxes the export ban on strong encryption programs, is probably a better solution to the Internet security problem than its opponents would like the public to believe.

Unless data transmitted over the Global Information Infrastructure remains secure from unauthorized access or modification, consumers may not use the Internet for routine commercial transactions.[93] With strong encryption, consumers can protect data such as their credit card numbers and personal information. Additionally, businesses will have the ability to protect trade secrets and other valuable information.[94]

President Clinton has recognized data protection as a prerequisite to realizing the Internet's potential as a vehicle for commerce. He directed "all executive departments and agencies to promote efforts domestically and internationally to make the Internet a secure environment for commerce."[95] His directive

---

ments of Commerce, Justice, and Defense. *See Reinsch Hearing*, *supra* note 89, at 55.

92. *See* Dunlap, *supra* note 42, at 34. Currently, an exception to the general policy allows banks to export secure encryption products without restriction because of the especially pressing need for security in that area and its centrality to the growth of e-commerce. *See* Gary G. Yerkey, *Commerce Plans to Allow Credit Card Firms, Brokerages to Export Encryption Technology*, 15 Int'l Trade Rep. (BNA) No. 7, at 260 (Feb. 18, 1998). A proposed rule change would extend this exemption to a wider range of financial services institutions. *See id.*

93. *See* Merrill, *supra* note 25, at 136. *See also supra* text accompanying notes 25-39.

94. *See* Merrill, *supra* note 25, at 136.

95. *Memorandum on Electronic Commerce*, *supra* note 8, at 1009.

included "guaranteeing confidentiality of electronic information to protect data from unauthorized use."[96]

Nevertheless, strong encryption does have its disadvantages. The encrypted data may be obscured forever if the decryption key is lost accidentally or through the actions of a malicious employee.[97] Such a loss may be significant, depending on the nature and value of the information.[98] For example, if a chemist stores his secret formula for a new and potentially lucrative chemical in encrypted code and then loses the key, he may never recover his ideas or the potential revenue therefrom. Terrorists and other criminals may also use encryption to reduce the ability of law enforcement officials to intercept and read their communications.[99]

B. THE POLICY'S EFFECTIVENESS

The encryption software industry has responded quickly to the key-recovery commitment requirements of the new license applications.[100] During the first eight months the new regulation was in effect, the Bureau of Export Administration (BXA) received over 1,000 license applications for exports valued at over $500 million.[101] As of August 4, 1997, thirty-three companies, including some of the largest software and hardware manufacturers in the United States, had submitted plans which outline how they plan to build key recovery products.[102]

On October 8, 1997, the European Union (EU)—through the European Commission (EC), which regulates trade in the fifteen countries of the EU—announced its refusal to follow the United States in banning certain encryption exports because such a move "could threaten privacy and stifle the growth of electronic commerce and . . . might simply be ineffective."[103] The EC has urged its member governments to take a "hands off" approach to regulating encryption, "warning against putting a technological

96. *Id.*
97. *See* Aaron, *supra* note 45.
98. *See* FRAMEWORK, *supra* note 10, at 20.
99. *Id.*
100. *See generally Reinsch Hearing, supra* note 89.
101. *See id.* at 56.
102. *See Number of License Applications Shows Success of Encryption Policy, Reinsch Says*, 14 Int'l Trade Rep. (BNA) No. 32, at 1363 (Aug. 6, 1997). As of that time, the BXA had approved twenty-nine of the thirty-three plans and had rejected none. *See id.*
103. Edmund L. Andrews, *Europeans Reject U.S. Plan on Electronic Cryptography*, N.Y. TIMES, Oct. 9, 1997, at D4.

straitjacket on a developing market."[104] However, the EC has not balanced these economic interests against national security interests. In contrast, the U.S. approach strikes a compromise which satisfies both by allowing the export of any encryption product as long as it meets the key recovery standards.[105]

Martin Bangemann, the European commissioner responsible for high-technology affairs, stated, "[i]n technological terms it is not possible to prevent criminals from obtaining and using encryption techniques. Therefore, there seems little point in preventing legal users from protecting themselves."[106] Moreover, some assert that criminals who are aware of the potential for decryption will simply avoid using encryption products which permit the government to decode their messages.[107] Yet, criminals today realizing that the government, with authorization, can eavesdrop on phone conversations, still use the telephone.[108]

Additionally, "the U.S. computer industry [currently] has no peer . . . [in the manufacture of] strong encryption technolog[y]."[109] Australia, Israel, Canada, China, and New Zealand boast growing encryption industries.[110] However, these governments generally enforce far more restrictive export controls than the United States.[111] Moreover, none of the countries of the Organisation for Economic Cooperation and Development (OECD) have relinquished sovereign access to encrypted data.[112] Thus, the international encryption market is not as open as many argue.[113]

C. U.S. ECONOMIC COMPETITIVENESS

At an industry conference on the future of information technology, a panel of U.S. experts on privacy and security supported the European line, coming to a consensus that "[t]he

104. *U.S. Will Keep Pushing Net Encryption Plan*, SEATTLE TIMES, Oct. 9, 1997, at D4.

105. *See* 15 C.F.R. § 740.8(b)(1) (1997) (describing how a business may qualify for a license exception).

106. Slater, *supra* note 23.

107. *See Reinsch Hearing*, *supra* note 89, at 55.

108. *See id.*

109. Richard Lardner, *Keys to the Code*, GOV'T EXECUTIVE, July 1997, at 29, 29.

110. *See* Michael Kanellos, *Is Key Recovery the Answer?*, COMPUTER RESELLER NEWS, Feb. 24, 1997, at 57, 57.

111. *See id.*

112. *See id.* at 58.

113. *See id.* at 57.

impasse over the use and control of encryption . . . is eroding the country's competitive edge [and] delaying the onset of electronic commerce."[114] The panelists agreed that the success of e-commerce depends on consumers' confidence in the system and their belief that transactions are safe from meddlers.[115]

Raymond Ozzie, creator of the popular software Lotus Notes, told the Senate Judiciary Committee that "[i]nformation security is critical to the integrity, stability, and health of both corporations and governments."[116] He added that cryptography is the "keystone of secure distributed systems."[117] The Business Software Alliance, an industry group in Washington, contends that the U.S. encryption export policy places American companies at risk of losing sixty billion dollars in the global software market[118] because some international software companies may export software with encryption as strong as 128 bits.[119]

A recent study concluded that thirty-five countries produce encryption products.[120] Of the more than 1,000 encryption products manufactured across the globe, only 435 are not produced in the United States.[121] William A. Reinsch, Undersecretary of Commerce for Export Administration, recently stated that no empirical evidence supported the assertion that American firms are suffering grave losses because other countries do not restrict the export of encryption software.[122] He stated that the Administration did not perceive an economic threat from foreign makers of encryption technology.[123] The contention that the U.S. computer industry has no peer in developing strong encryption technologies[124] bolsters the Administration's position. The mere fact that other countries produce encryption programs of some strength does not prove that they can capably compete with U.S.

---

114. David Braun, *Encryption Stalemate Threatens E-Commerce, National Security*, TECHWIRE, Oct. 9, 1997, *available in* LEXIS, News Library, Wires File. The panel included the following: former Federal Trade Commissioner Christine Varney, former CIA director John Deutsch, constitutional lawyer and free-speech advocate Floyd Abrams, and director of technology of the National Computer Security Association Ira Winkler. *See id.*

115. *See generally* Braun, *supra* note 114.

116. Schatz, *supra* note 27, at 60.

117. *Id.*

118. *See id.*

119. *See* Dunlap, *supra* note 42, at 34.

120. *See* Greg Rattray, *The Emerging Global Information Infrastructure and National Security*, 21 FLETCHER F. WORLD AFF. 81, 88 (1997).

121. *See id.*

122. *See Reinsch Hearing, supra* note 89, at 56.

123. *See id.*

124. *See* Lardner, *supra* note 109, at 29.

manufacturers with respect to the strong technologies addressed in the Administration's regulations.

D. THE KEY ESCROW POLICY

At this time, the National Research Council (NRC) rejects a key management system as untested. Instead, it encourages the U.S. government to invest in advanced counter-encryption technologies.[125] Its concerns include the following:

> [a] lack of operational experience with how a large-scale infrastructure for escrowed encryption would work; [a] lack of demonstrated evidence that escrowed encryption will solve the most serious problems that law enforcement authorities face; [and] the likely harmful impact on the natural market development of applications made possible by new information services and technologies.[126]

Additionally, the NRC expresses apprehension over the uncertainty of market response to the aggressive promotion of escrow procedures.[127]

While the NRC's recommendation may provide an idealistic vision for the future, it does not solve the government's need to protect national interests today. A skilled hacker can break the code for a 40-bit encryption key in about forty seconds.[128] In contrast, in one experiment, a 56-bit key required 120 days to be broken, even with the power of a nationwide group of network computers.[129] Today's fastest computers would require millions of years to descramble even stronger versions of encryption software.[130] While the government works on reducing that time requirement, it must have an effective means of law enforcement.

The potential adverse impact on public safety and national security associated with any "wait and see" approach is too great to justify catering to the narrow interests of computer software companies.[131] Even reducing the decoding time to days or weeks may not be sufficient to prevent the types of crime the

---

125. *See* NRC REPORT, *supra* note 31, at 11-12. The NRC recommends that "[h]igh priority should be given to research, development, and deployment of additional technical capabilities for law enforcement and national security for use in coping with new technological challenges." *Id.* at 12.

126. *Id.*

127. *See id.*

128. *See* Jim Kerstetter, *Crypto Crew, Feds at Odds*, PC WEEK, Jan. 26, 1998, at 35, 35.

129. *See id.*

130. *See* David Stipp, *Techno-Hero or Public Enemy?*, FORTUNE, Nov. 11, 1996, at 173, 176.

131. *See Impact of Encryption Statement, supra* note 41.

export policy targets. Legally authorized wiretaps generally provide crucial information just before a crime is to occur; similarly, a nearly instantaneous ability to decode messages is necessary to prevent crimes on the Internet.[132] Effective law enforcement depends on electronic surveillance and search and seizure.[133] The framers of the Fourth Amendment established a delicate balance between "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures" and the legitimate right and necessity for the police to have access to evidence of illegal acts.[134] Moreover, access to a wide variety of keys through key recovery may help the government develop its decoding capabilities by exposing it to a broad technology base.

By requiring deposit of a decryption key in the escrow program for all encryption software shipped internationally, the government will have better access to the tools it needs to uncover covert operations affecting national security. Some argue that, contrary to popular belief, the risk of concealed criminal activity bears little relation to whether U.S. companies may legally export strong encryption programs.[135] Criminals are, of course, willing to break or circumvent the law to achieve their objectives. For example, foreign criminals may use encryption programs manufactured in foreign countries for which keys have not been deposited. Recent evaluations suggest that the current U.S. export controls reflect an unrealistic view of federal law's ability to constrain actors from obtaining encryption products to conduct strategic information attacks or conceal information about their operations.[136] Over the long term, the U.S. government may not succeed in restricting the use of encryption technology which is freely available in the United States and from foreign companies.[137] However, while the government develops the means to cope with this technological reality, a key-recovery system remains its only currently viable alternative.[138] To allay the burden on U.S. industry, the policy even allows an organization to appoint an internal key recovery agent as long as the or-

132. *See* Greiveldinger, *supra* note 43, at 507.

133. *See Impact of Encryption Statement, supra* note 41.

134. U.S. CONST. amend. IV; *see also Impact of Encryption Statement, supra* note 41.

135. *See, e.g.*, Dan Gillmor, *Decoding Positions on Encryption Policy*, CHICAGO TRIB., Jan. 19, 1998, § 4 (Business & Technology), at 5.

136. *See* Rattray, *supra* note 120, at 89.

137. *See* David Moschella, *Contrarian Thinking on Encryption Controls*, COMPUTERWORLD, Oct. 13, 1997, at 114, 114.

138. *See World Wide Threats Hearing, supra* note 53.

ganization implements safeguards to "ensure the . . . agent's structural independence from the . . . organization [and the availability,] security, and confidentiality [of keys]."[139]

Legislators in France have proposed a law guaranteeing government access to corporate electronic data.[140] In addition to imposing stringent controls on the export of encryption software, France also prohibits the domestic use of cryptography. The proposed legislation would allow the use of encryption products only if the manufacturer deposits a decryption key with a government-approved entity.[141] Those who choose not to surrender their decryption keys would be limited to using weaker encryption software, decodable by law enforcement agencies without keys.[142] Gen. Jean-Louis Desvegnes, chief of France's Central Service for the Security of Information Systems, refers to this policy as the best way "to find a balance between national-security interests, economic interests and the protection of personal privacy."[143]

The U.S. government's access to decryption keys through an escrow program would probably not significantly harm the public's confidence in the security of electronic commerce systems.[144] Generally, businesses themselves voluntarily maintain a key recovery plan; in the absence of a way to decode information, forgotten passwords, misplaced information, and other clerical mishaps could cause significant delays or losses to the business.[145]

The fact that the government proposes an escrow program probably alleviates some consumer concerns about the improper use of keys. Because a third party actually maintains the keys and uses them only at the direction of law enforcement officials, the structure of the escrow policy allows the government and the

---

139. 15 C.F.R § 742, supp. 5(I)(8) (1997).

140. *See* Jennifer L. Schenker, *French Plan for Key Encryption Alarms Corporations and the EU*, WALL ST. J. EUR., Oct. 20, 1997, at 2.

141. *See id.*

142. *See id.*

143. *Id.*

144. However, some European businesses and government officials suspect that the United States could use such a key system to conduct industrial espionage. *See* Kenneth Cukier, *Europe to Resist U.S. Cryptography Policy*, COMMUNICATIONSWEEK INT'L, Sept. 22, 1997, at 1, 1. Additionally, officials at the German Ministry of Economics fear that the U.S. key escrow approach violates the data privacy rules in Germany and the EU. *See id.* The use of an international tribunal, rather than a U.S. court, to approve the use of decryption keys on data involving international parties might alleviate such concerns.

145. *See* Rockwell, *supra* note 60, at 87.

third party to maintain checks on each other to assure that the keys are not employed inappropriately. While those entrusted with the keys may use them improperly, any violation of key-holding obligations constitutes a violation of the EAR, and the government may impose sanctions accordingly.[146]

E. THE POLICY'S FIT WITH THE UNITED STATES' OBJECTIVES

While the U.S. ban seemingly contradicts many of the objectives outlined in the Framework for Global Electronic Commerce, it does so only to the extent necessary to protect the nation's legitimate security interests. The United States encouraged other nations to refrain from imposing unnecessary regulations and undue restrictions on electronic commerce.[147] Some argue that the ban is "unnecessary" and "undue" since there is no empirical evidence that it is achieving its purpose. Others criticize the Administration for implementing the ban amid wide-spread, longstanding opposition from the U.S. computer software industry,[148] despite its statement that private sector participation should be a formal part of the policy-making process.[149] Additionally, the initial ban flatly contravened the President's directive that the Internet should be a "secure environment for commerce . . . guaranteeing confidentiality of electronic information to protect data from unauthorized use."[150] By initially banning the export of strong encryption products altogether, the government curtailed the ability of foreign users to use these programs to protect their transactions. However, a recent executive order relaxed the ban, allowing the export of encryption technology of any strength, as long as a key recovery commitment accompanied its license application.[151] This new policy probably presents the best balance between national se-

146. *See* 15 C.F.R. § 740.8(d)(1)(i)(E) (1997).

147. *See Remarks Announcing the Electronic Commerce Initiative*, *supra* note 5, at 1005.

148. *See, e.g.*, Russ Mitchell, *Is the FBI Reading Your E-mail?*, U.S. NEWS & WORLD REP., Oct. 13, 1997, at 49, 49 (criticism of policy generally); Michelle Quinn, *U.S. Asked to Lift Ban on Encryption*, SAN FRANCISCO CHRON., Jan. 17, 1996, at B2 (objections to policy voiced by executives from companies including Apple Computer, Silicon Graphics, and Sun Microsystems); Hiawatha Bray, *Panel Criticizes U.S. Government's Encryption Stand*, BOSTON GLOBE, May 31, 1996, at 36 (reporting National Research Center's opposition); Rajiv Chandrasekaran, *Freeh Seeks Encryption Decoding Key*, WASH. POST, Sept. 4, 1997, at E1 (citing protests of privacy advocates, Software Publishers Association, and Business Software Alliance).

149. *See* FRAMEWORK, *supra* note 10, at 4.

150. *Memorandum on Electronic Commerce*, *supra* note 8, at 1009.

151. *See* 15 C.F.R. § 740.8; *see also* Exec. Order No. 13,026 *supra* note 44.

curity, privacy, and economic interests in view of where encryption technology stands today and law enforcement's limited ability to cope with the dangers it presents.

F. CONSTITUTIONAL CONSIDERATIONS

In the United States, some have suggested that the notion that transactions can be rendered illegal because authorities cannot readily access them clearly violates several aspects of the Bill of Rights.[152] On August 26, 1997, a federal judge in San Francisco held the current federal rules limiting encryption exports unconstitutional.[153] Daniel Bernstein, a math professor at the University of Illinois, sued the government in 1995, arguing that federal controls on encryption violated his First Amendment rights to free speech.[154] U.S. District Court Judge Marilyn Hall Patel approved an injunction, forbidding the government from prosecuting Bernstein for posting his encryption software on the Internet.[155] The case is currently on appeal.[156]

Judge Patel wrote that "a licensing scheme with a content-neutral purpose must still contain adequate procedural safeguards in order to be constitutional."[157] The government "may not *condition* . . . speech on obtaining a license or permit from a government official in that official's boundless discretion."[158] The court classified computer source code as speech, thus granting encryption software First Amendment protection.[159] The court noted that although the EAR provides that license applications will be resolved or referred to the President within ninety days, there is no time limit on an application that has been referred to the President.[160] Moreover, if the BXA rejects an application, the agency provides an internal appeals process which requires only that it must render a decision "within a reasonable time."[161] Most importantly, there are no standards for decision; the EAR reviews license applications on a "case-by-case basis"

152. *See, e.g.*, Steve Steinke, *The Latest on Crypto Regulation*, NETWORK MAG., Nov. 1997, at 16, 18.
153. *See* Bernstein v. United States Dep't of State, 974 F. Supp. 1288 (N.D. Cal. 1997).
154. *See id.* at 1292.
155. *See id.* at 1310-11.
156. *See* Leibowitz, *supra* note 28, at A1.
157. *Bernstein*, 974 F. Supp. at 1307.
158. *Id.* at 1304 (citing Lakewood v. Plain Dealer Publ'g Co., 486 U.S. 750, 764 (1988)) (emphasis in original).
159. *See id.* at 1303.
160. *See id.* at 1308.
161. *Id.*

and apparently does not curtail agency discretion.[162] As the regulations stand, the court held that they constitute an unconstitutional prior restraint on speech.[163]

The court concluded that the President possesses the authority to maintain the export regulations based on his broad discretion under the International Emergency Economic Powers Act.[164] It directed its objections to the administrative procedures outlined in the regulations, rather than their substantive effect. Therefore, although a federal court held the encryption export regulations unconstitutional, the Administration may easily cure their defects without affecting its underlying policy.

IV. CONCLUSION

The U.S. encryption restrictions do not reach criminals who operate solely in the United States and use encryption technologies to conceal their activities. The limitations apply exclusively to exports, evidencing the government's commitment to acting only to the extent necessary to protect national security interests from foreign-based criminals such as terrorists.

A policy of allowing encryption technology exports when accompanied by key recovery presents the best-balanced position for the government at this time. While the NRC is very ambitious in its recommendation that the government direct its resources to the development of advanced counter-encryption technologies, that stance does not solve the government's need to protect national security interests today. The government must have a means of law enforcement to use while it works on meeting the NRC's goals.

The current U.S. policy, while not ideal, may be the most well-balanced formulation for the present. The policy does not seek to expand the powers of law enforcement or reduce the privacy protection of individuals. Its intent is to maintain, in the face of technological advances, the legal tools which Congress and the Constitution have determined are necessary for safeguarding the nation's security interests.

162. *See id.* (citing 15 C.F.R. § 742.15(b) (1997)).
163. *See id.* at 1307-08.
164. *See id.* at 1298-1303.