# Decrypting the Politics: Why the Clinton Administration's National Cryptography Policy Will Continue to be Dictated by National Economic Interest

Christian R. White

## INTRODUCTION

The debate concerning a national cryptography policy and its effect on international economic competition is raging throughout different sectors of the country, including the halls of Congress, the computer industry, the judiciary, organs of the government dealing with security issues and individual households. Why is this subject receiving so much attention? Living in the information age, many of our most personal thoughts and most valuable secrets are transferred from one person or business to another via the Internet. Because businesses and individuals are communicating on-line, they demand assurance that unauthorized individuals cannot gain access to highly sensitive information, be it personal e-mail or a corporate secret. Many businesses and individuals are therefore resorting to encryption technology to preserve the integrity and confidentiality of information.

For businesses which conduct international transactions, reliable and advanced security technology is necessary to prevent competitors from intercepting confidential information. Due to Executive Order 13,026,[1] which imposes export restrictions on advanced forms of encryption technology, the business community has expressed concern that transactions and information sent via the Internet lack the security needed. The use of encryption technology achieves that goal by providing the desired security. The United States computer software industry is worried that billions of dollars will be forfeited to foreign competitors if they are not allowed to export comparable strength encryption products. Loosening export regulations permits the software industry to successfully compete in this market.

This Comment suggests that the original encryption policy initiated by President Clinton's Executive Order will be drastically altered in order to meet the needs of the business community and the computer software industry, while still enhancing national security. Part I discusses the origin and evolution of cryptography. Part II explains how various government entities have regulated encryption software. Part III provides law enforcement's reasoning as to why a relaxation of regulations should not take place. Part IV focuses on how the Clinton Administration has already made concessions to the software industry by loosening the regulations. Lastly, Part V examines why the government's policy will continue to deregulate the export of encryption technology to foreign nations.

## I. CRYPTOGRAPHY: WHAT IT IS, HOW IT WORKS AND WHY IT HAS BECOME SO IMPORTANT

Encryption is one component of the art and science of cryptography.[2] Cryptography is a method of hiding and storing information by using a code

[1] Exec. Order No. 13,026, 61 Fed. Reg. 58,767 (1996) (explaining that President Clinton declared that new provisions will be implemented with respect to the export of encryption technology).

[2] J. Terrence Stender, *Too Many Secrets: Challenges to the Control of the Strong Crypto and the National Security Perspective,* 30 CASE W. RES. J. INT'L. L. 287, 293 (1998). For a more detailed discussion on the technicalities of encryption, *see generally* WHITFIELD DIFFIE AND SUSAN LANDAU, PRIVACY ON LINE (1998); A. Michael Froomkin, *The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution,* 143 U. PA. L. REV. 709 (1995).

or cipher.[3] The process of encryption involves transforming an original text to an unintelligible form, unreadable by anyone except the intended recipient.[4] Information which has not yet been encrypted is referred to as plaintext.[5] Once encrypted, the text is known as ciphertext.[6] Simply, encryption is the process of securing communications and decryption is the way in which ciphertext becomes legible to the intended recipient.[7]

In order for a message to be encrypted, a mathematical function called an algorithm must be applied to the intended text.[8] Basically, an algorithm is a "set of rules or series of mathematical steps"[9] used in the encrypting and decrypting process; it will scramble the text until the recipient applies the corresponding key to unscramble the message.[10] The algorithm is not what allows the text to become secure; rather, security occurs when the user of encryption technology selects an individual key.[11] Similar to a traditional lock box and key, a cryptographic algorithm implements a key to encrypt and decrypt a message.[12] Once the sender encrypts the message and sends it, the recipient must use the same algorithm to decrypt the message.[13]

The length of the key and the complexity of the algorithm determines the strength of the encryption algorithm.[14] The key is measured in bits,[15] and for every bit the number of possible key sequences is doubled, resulting in dramatically stronger encryption as the number of bits increases.[16] For example, over one trillion potential combinations exist for a 40-bit key and more than seventy-two quadrillion potential combinations exist for a 56-bit key.[17] Today, the most advanced forms of encryption software have a key length of 1,052-bits.[18]

As technology advances and the need for security persists, businesses utilize encryption software products as a primary form of security for three main purposes: (1) confidentiality; (2) authentication; and (3) integrity.[19] Confidentiality allows communications between individuals to become

[3] *See* Stender, *supra* note 2, at 293. Cryptography dates back 3,000 years to the Egyptians. *See id.* It was used mainly for keeping military information secret. *See id.* Messages were encrypted in the American Revolution, Civil War, World War I and II. *See id.* Since World War II, the use of encryption has become much more sophisticated due to the advancement in computer technology. *See id. See generally* SAUL K. PADOVER AND JAMES WESTFALL THOMPSON, SECRET DIPLOMACY: ESPIONAGE AND CRYPTOGRAPHY 1500-1815 (1963) (providing a more detailed explanation of both the history and technicalities of cryptography).

[4] FEDERAL BUREAU OF INVESTIGATION, ENCRYPTION: IMPACT ON LAW ENFORCEMENT at 2 (1998) [hereinafter *FBI Report*] (explaining the FBI position on encryption policy and commenting on proposed legislation dealing with encryption in the United States Congress).

[5] *See id.*

[6] *See* Stender, *supra* note 2, at 294 (defining various encryption terms).

[7] *See* FBI Report, *supra* note 4, at 2.

[8] *See* Stewart A. Baker, *Government Regulation of Encryption Technology: Frequently Asked Questions,* Sept. 1996, at 287, 290 (explaining how the process of encrypting and decrypting a message works).

[9] *See* Stender, *supra* note 2, at 294; *see also High Tech Dictionary* (visited Oct. 18, 1998) <phtml?lookup=863>. Algorithm is defined as a "set of instructions for solving a problem. Named after Al-Khawarizmi, an Iranian mathematician," it is commonly used in computer programming to refer to instructions given to the computer. *See id.*

[10] *See* Stender, *supra* note 2, at 295.

[11] *See* Baker, *supra* note 8, at 290. The algorithm may either be a "secret key" or "public key" algorithm. *See id.* A secret key is used for both the encryption and decryption process. *See id.* The secret key is not very difficult to use and provides reliable security, but the sender and receiver must agree on the key before the message is sent. *See id.* A secret key cannot be used to send an encrypted message to a stranger. *See id.* The advantage to using a public key is that a message can be easily sent to or from a complete stranger. *See id.*

[12] *See* FBI Report, *supra* note 4, at 2.

[13] *See* Baker, *supra* note 8, at 290.

[14] *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) [hereinafter NRC Report]; *See also* Ma-Tram B. Dinh, *The U.S. Encryption Export Policy: Taking the Byte Out of the Debate,* 7 Minn. J. Global Trade 375, 379-80 (1998) [hereinafter Dihn] (describing the processes and purposes of encryption).

[15] *See High Tech Dictionary* (visited Oct. 18,1998) <http://www.current.net/resources/dictionary/definition.phtml?lookup=790> (explaining that a bit is an abbreviation for the term binary digit, which is the smallest unit of information a computer can store); *see also* NRC Report, *supra* note 14, at 354 (defining binary digit as "one of two symbols (0 and 1) that are commonly used to represent numerical entries in the binary number system").

[16] *See* NRC Report, *supra* note 14, at 1. The report studies the effect of encryption policy on the computer software industry, national security and individual privacy. *See id.* It concludes that "U.S. policy should be changed to promote and encourage the widespread use of cryptography. . . ." *See id.*

[17] *See* Dinh, *supra* note 14, at 379-80 (explaining statistical information about the lengths of algorithms).

[18] Anthony Aarons, *Tales from the Encrypt,* Cal. Law., Apr. 1997, at 21.

[19] *See* Baker, *supra* note 8, at 290; *see also* Dinh, *supra* note 14, at 379. It is estimated that by the year 2000, hundreds of millions of people will be using the Internet and many of these people will be conducting business transactions over on the Internet. *See* Baker, *supra* note 8, at 290. If companies are

and remain private.[20] Preserving confidential communications is vital to securing business plans, intellectual property, and other private communications.[21] Authentication ensures that a particular message was sent by the stated sender.[22] By authenticating a message, the probability of forgery and repudiation is significantly diminished.[23] Certifying the integrity of a message confirms that a message has not been altered in any way during transit.[24]

## II PRESIDENT CLINTON'S EXECUTIVE ORDER AND ITS EFFECTS ON ENCRYPTION POLICY

On November 15, 1996, President Clinton, by authority derived from the International Emergency Economic Powers Act[25] and the Export Administration Act,[26] issued Executive Order 13,026,[27] entitled "Administration of Export Controls on Encryption Products." This particular Order focuses on the export of encryption technology.[28] The Administration's policy originally deemed the export of data scrambling technology to be a serious threat to national security and foreign policy.[29] The Order authorizes the Secretary of Commerce to issue licenses to manufacturers of encryption technology on a case-by-case basis.[30] In addition, the Order promotes the use of a key recovery management infrastructure — a longstanding cornerstone of the government's policy.[31]

### A. Key Escrow Systems

The Clinton Administration proposed a key recovery or key escrow system[32] as a way to balance the "needs for information security against the needs of law enforcement and to a lesser extent national security."[33] Key escrow encryption systems provide encryption key codes to a trusted third party that stores the keys for the users of such technology.[34] These codes allow the holder of the keys to decrypt any encrypted message.[35] Under this law, encryption key codes on all encryption software shipped internationally would

to operate more efficiently and provide customers with the option to purchase products via the Internet, the buyer and seller must be assured that each and every transaction is secure. *See* Dinh *supra* note 14 at 379.

[20] *Cf. id.* (explaining that many individuals conducting business and communications over the Internet do not want others to be privy to such information).

[21] *See id.* at 290 (claiming that providing confidentiality is essential to commercial success).

[22] *See* Baker, *supra* note 8 at 290 (stating that if a message is authenticated, then the sender cannot deny that he sent the message).

[23] *See id.*

[24] *See id.* Testing the integrity of a message sent via the Internet is comparable to checking whether or not an envelope has been opened during its delivery. *Id.*

[25] 50 U.S.C. ' 1702 (a)(1)(B) (1996). The International Emergency Economic Powers Act extends power to the President to "investigate, regulate, direct and compel, nullify, void, prevent or prohibit any . . . importation or exportation of, or dealing in, or exercising any right, power, or privilege with respect to, or transactions involving, any property in which any foreign country or a national thereof has any interest." *Id.*

[26] Export Administration Act of 1979, Pub. L. No. 96-72, 93 Stat. 503 (codified as amended in 50 U.S.C. app. §' 2401-20 (1994)). The act is based on legislation passed in 1949 that had the primary purpose of blocking exports that may have benefited the former Soviet Union and the expansion of communism. *Id.* The Export Administration Act ("EAA") was rewritten in 1979 and provided the President with the authority to impose export controls in order to achieve foreign policy goals. *Id.* Congress once again rewrote the EEA in 1996, placing new emphasis on "controlling the export of sensitive items . . . ." *Id.* The law reflects a shift from fighting communism to post Cold-War matters such as non-proliferation of weapons of mass destruction and counter terrorism objectives. *Id.*

[27] *See* Exec. Order No. 13,026, *supra* note 1, at 58,767.

[28] *See* Memorandum on Encryption Export Policy, Nov. 15, 1996, at 2397 (concluding that the use of encryption technology can jeopardize the safety of U.S. citizens).

[29] *See* Exec. Order No. 13,026, *supra* note 1, at 58,767 (explaining that the Secretary may look at foreign availability of comparable encryption products to determine whether a license should be issued).

[30] *See id.*

[31] *See id. See also* Baker, *supra* note 8, at 292 (explaining that the government promotes escrow encryption because it is easier for the government to gain access to decryption keys once authorized by a court order); *see also* The Risks of Key Recovery, Key Escrow, Trusted Third Party and Encryption 4 (visited Nov. 2, 1998) <http://www.cdt.org/crypto/risks98/> [hereinafter The Risks of Key Recovery] (explaining that key escrow systems contain a mechanism for obtaining access to the plaintext of an encrypted file).

[32] *See generally* Dinh, *supra* note 14, at 380

[33] *See* NRC Report, *supra* note 14, at 167.

[34] *See* Stender, *supra* note 3, at 298. A trusted third party may be a bank, private company, or other entity that meets certain statutory standards. *Id.* These standards require that the trusted third party not have a criminal history or pending criminal charges, must not have ever breached any fiduciary duty owed to another, and must not have a poor credit history. *See also* Dinh, *supra* note 14, at 380 n.41; 15 C.F.R. § 742 Supp. 5 (1997) (giving the exact statutory requirements); The Risks of Key Recovery, *supra* note 31, at 10 (critiquing the trusted third party policy).

[35] *See* NRC Report, *supra* note 14, at 167-68.

be provided to the trusted third parties.[36] These third parties could release the codes to predetermined authorized parties[37] or to law enforcement officials who have obtained a valid court order.[38]

## B. Transition from the Munitions List to the Commerce Control List

In the past, the Department of State ("DoS") regulated encryption exports[39] under the authority of the Arms Export Control Act[40] and International Traffic in Arms Regulations ("ITAR").[41] Encryption software was specifically placed on the United States Munitions List ("USML") due to the nature of the product.[42] Commercial products using encryption technology were placed on the USML because such items were considered to be used primarily for military purposes.[43] Other items on the USML include bombs,[44] grenades,[45] torpedoes,[46] ballistic missiles,[47] warships,[48] tanks,[49] military aircraft,[50] and rockets.[51] The USML did not differentiate technically between encryption software used solely for military purposes and dual-use encryption software used for business and personal security purposes.[52] Executive Order 13,026 transferred jurisdiction over dual-use[53] encryption software from the DoS to both the Commerce Department[54] and the Department of State's, Office of Defense Trade Control The DoS, however, still regulates encryption software designed primarily for military application.[55]

The Bureau of Export Administration ("BXA"), a division of the Department of Commerce,[56] now regulates dual-use encryption software and places such software on the Commerce Control List.[57] The BXA "administers and enforces laws and regulations that govern exports of dual-use commodities, technology and software from the United States and its territories and reexports of such items from third countries."[58] The BXA is also the agency responsible for the administration of President Clinton's encryption policy.[59]

The Commerce Control List ("CCL") specifies all "the commodities, software and technical data that are subject to export control."[60] The CCL is

[36] *See* Dinh, *supra* note 14, at 380-81 (describing the characteristics of the trusted third party).

[37] *See* Stender, *supra* note 3, at 298.

[38] *See* Dinh, *supra* note 14, at 381 (explaining the requirements needed to recover a key).

[39] *See* 22 C.F.R. § 120.1 (1997).

[40] 22 U.S.C. § 2778 (1994).

[41] *See* 22 C.F.R pts. 120-30 (1997).

[42] *See* 22 C.F.R. § 121.1 (1997). The United States Munitions List is part of the secondary regulations of the International Traffic in Arms Regulations that define which defense articles and services are subject to licensing. *Id.* The USML was established by Section 38 of Arms Export Control Act to advance "world peace and the security and foreign policy of the United States." 22 U.S.C. § 2778(a)(1) (1994). The USML definition of encryption is "(s)peech scramblers, cryptographic devices (encoding and decoding), and specifically designed components thereof, ancillary equipment, and especially devised protective apparatuses for such devices, components and equipment." 22 C.F.R. § 121.01 (1970).

[43] *See* Baker, *supra* note 8, at 293. Cryptographic technology and components thereof are used to keep information secret. *See id.* Government regulations considered this technology a threat to national security. *See id.* Because of such rationale, the government put all forms of encryption technology on the USML, even if it was being used for legitimate business purposes. *See id*; *see also* Encryption Items Transferred From the U.S. Munitions List to the Commerce Control List, 61 Fed. Reg. 68,572 (1996) [hereinafter Encryption Items Transferred] (discussing the rationale for the shift in oversight authority).

[44] *See* 22 C.F.R. § 121.1 Category IV(a) (1997).

[45] *See id.*

[46] *See id.*

[47] *See id.* § 121.1 Category IV(b).

[48] *See id.* § 121.1 Category VI(a).

[49] *See id.* § 121.1 Category VII(b).

[50] *See id.* § 121.1 Category VIII(a).

[51] *See id.* § 121.1 Category IV(a).

[52] *See* W. Clark McFadden II & David Bentley, *Evolution of Encryption Controls: Can They Respond to Current Trends?*, 1997, at 489; 495 PLI Patents, Copyright and Traditional Course Series (explaining that any substantive change in the way encryption technology is categorized is handled by the DoC through the application of the EAR).

[53] *See* Jeffery H. Matsuura & George B. Delta, *Export Controls on the Internet*, 10 No.3 J. Proprietary Rts. 2, 3 (1998) (defining dual-use technologies as those which serve both military and non-military purposes).

[54] *See* Encryption Items Transferred, *supra* note 43, 61 Fed. Reg. at 68,572.

[55] *See* 22 C.F.R. § 120.3 to .4 (1997) (stating that criteria used to determine whether or not encryption technology is used for primarily military application includes the intent of the design, the sponsor of the originating research and development, the configuration or use of military specifications, nomenclature (military or civilian), and application).

[56] *See* Encryption Items Transferred, *supra* note 43, 61 Fed. Reg. at 68,572-87.

[57] *See* 15 C.F.R. § 774, Supp. 1 (1997); *see also* NRC Report, *supra* note 14, at 118-19 (describing the major differences between the USML and the CCL).

[58] *See* Bureau of Export Administration, 1997 Annual Report I-1 (1998).

[59] *See id.*

[60] Charles L. Evans, *U.S. Export Control of Encryption Software: Efforts to Protect National Security Threaten the U.S. Software Industry's Ability to Compete in Foreign Markets*, 19 N.C. J. Int'l & Comm. Reg. 469, 475 (citing John F. McKenzie, Implementation of the Core List of Export Controls: Computer and Software Controls, 5 Software L.J. 1, 3 (1992)).

divided into ten general categories and numerous sub-categories.[61] As of March 1998, the Commerce Control List included over 200 sub-categories of controlled goods and approximately 100,000 specific goods.[62]

### C. The Meaning of President Clinton's Executive Order as Implemented Through the BXA

The President's Executive Order set out the policy towards the exportation of encryption software through a rule which "require[d] a BXA license for the export of dual-use encryption software, hardware and technology to all destinations except Canada."[63] The licensing policy was divided into four distinct groups.[64] The first group dealt with the distribution of mass-market[65] encryption software.[66] In order to obtain a license, the BXA must have conducted a one-time review of the software.[67] Only 40-bit encryption software was eligible for such a license after a seven day review under this policy.[68]

The second group represented the exportation requirements of key escrow or key recovery software and commodities.[69] Similar to the first group, this software was subject to a one-time review by the BXA in order to receive its license.[70] The key escrow software "will receive favorable consideration provided that, prior to the export or reexport, a key recovery agent satisfactory to BXA has been identified . . . and security policies for safeguarding the key(s)[71] or other material/ information required to decrypt cipher text . . . are maintained after export or reexport as required by the EAR."[72] If the software received a favorable recommendation, then manufacturers of encryption software were not limited to any particular key length,[73] and they would have been permitted to export their products to nearly all destinations[74] throughout the world.[75]

The third licensing method concerned non-recovery encryption items with up to a 56-bit key length.[76] Manufacturers could have exported non-recovery encryption software not exceeding a 56-bit key length in exchange for a "good faith effort by the producer to promote key recovery products and infrastructure."[77] In addition, exporters must have submitted an acceptable time frame and business plan to the BXA for review.[78] The exporter had a two-year transition period to "develop, produce, and/or market encryption items and services with recoverable features."[79] The permit needed to be renewed every six months;[80] the renewal process was dependent on how well the applicant adhered to the time frame

[61] *See* 15 C.F.R. § 738.2 (1997) (dividing the ten general categories: nuclear materials, materials, materials processing, electronics, computers, telecommunications and information security, lasers and sensors, navigation and avionics, marine, and propulsion systems).

[62] *See* Matsuura and Delta, *supra* note 53, at 3.

[63] *Encryption Products Transferred to the Commerce Control List* (visited Sept. 13, 1998) <http://www.ffhsj.com/firmpage/cmemos/0096941.htm>.

[64] *See* Encryption Items Transferred, 61 Fed. Reg. at 68,573; *see generally* NRC Report, *supra* note 14, at 113-165 (detailing the history and effectiveness of export controls on cryptography).

[65] Guidelines for Submitting a Classification Request for a Mass Market Software Product that Contains Encryption, 15 C.F.R. pt. 742, Supp.6 (a)(1)(i)(ii)(iii) (1997) (defining mass market as software which is available to the public through retailers in over-the-counter or similar transactions, designed for user installation without substantial supplier support and includes encryption for the purpose of "data confidentiality").

[66] *See* Encryption Items Transferred, 61 Fed. Reg. at 68,573.

[67] *See id.* (explaining the procedure one must follow in order to receive a license to export encryption software from the government).

[68] *See id.* at 68,574; *see also* Center for Democracy and Technology (visited Nov. 19, 1998) <http:www.cdt.org/crypto/> (explaining that 40-bit and even 56-bit encryption technology will not provide adequate security because researchers have cracked 56-bit codes in 56 hours with a machine that only cost $250,000).

[69] *See id. See also* The Risks of Key Recovery, *supra* note 31 (analyzing the fundamental properties of key escrow and the technical risks, costs, and implications of using such a system).

[70] *See* Encryption Items Transferred, 61 Fed. Reg. at 68,574.

[71] *See* Baker, *supra* note 8; Stender, *supra* note 9-10; High Tech Dictionary, *supra* note 9.

[72] *See* Encryption Items Transferred, 61 Fed. Reg. at 68,574.

[73] *See id.*

[74] *See id.* (prohibiting exports to Cuba, Iran, Iraq, Libya, North Korea, Syria, and Sudan under the International Traffic in Arms Regulations, because they are suspected of supporting terrorist activities).

[75] *See id.*

[76] *See id.*

[77] *See id.*

[78] *See* Encryption Items Transferred, 61 Fed. Reg. at 68,574 (explaining that the business and marketing plan must detail the exact steps to be taken to implement a key recovery system by the designated time).

[79] *See id.*

[80] *See id.* (stating that the license exception is not automatically renewed).

of the detailed plan submitted by the company.[81]

The fourth method handled other encryption issues.[82] The policy in effect prior to the issuance of this rule remains the regulatory scheme for all other encryption products.[83] Exporters may apply for a license through the BXA, but each application will be reviewed on a case-by-case basis.[84]

## III. LAW ENFORCEMENT'S DESIRE FOR STRONG REGULATION OF ENCRYPTION EXPORTS

Pressure by the government to regulate the export of encryption flows from two main sources:[85] (1) law enforcement organizations concerned with gathering evidence of criminal activity, such as the Federal Bureau of Investigation ("FBI") or the police;[86] and (2) interests, concerned with gathering intelligence information concerning national security, such as the National Security Agency ("NSA").[87] Although law enforcement organizations understand the importance and necessity of the worldwide exportation of advanced encryption technology, a fear remains that if certain controls are not placed on such technology, then law enforcement's ability to capture criminals and terrorists or thwart their plans will greatly diminish.[88] The need to protect the United States' national security and foreign policy interests are indeed legitimate; therefore, a compromise between the government and the computer industry needs to be negotiated.[89] A question arises as to what extent the government should accommodate law enforcement organization's wants.[90]

The NSA is strongly opposed to any relaxation of export controls on encryption software because such encryption technology may facilitate terrorists' efforts in conducting targeted attacks against U.S. interests.[91] The Aldrich Ames case[92] and Ramzi Yousef case[93] are often cited as examples of criminals who have used encryption technology as a means to avoid revealing their criminal activity.[94]

The FBI firmly believes that criminals will increasingly use encryption technology as a tool in perpetrating their crimes.[95] Therefore, in order to fulfill its "responsibility for protecting public safety and national security,"[96] the FBI argues for key recovery technology that allows "immediate access to the plaintext of encrypted criminal-related data"[97] provided they have obtained a lawful court order.[98]

The FBI is not only interested in obtaining the keys to encryption codes to monitor international criminal activity, but it also wants to monitor domestic criminal activity.[99] Presently, domestic use of the strongest encryption technology is permitted without any key recovery system in place.[100] The FBI is pressuring the Clinton Administration to mandate such systems for both domestic and

[81] *See id.*

[82] *See id.* The fourth licensing arrangement is concerned with the distribution and warehousing of such technology. *See id.* Any other changes in policy will be made on a case-by-case basis. *See id.*

[83] *See id.*

[84] *See* Encryption Items Transferred, 61 Fed. Reg. at 68,575.

[85] *See* Baker, *supra* note 8, at 301.

[86] *See id.*

[87] *See id.*

[88] *See* FBI report, *supra* note 4, at 1.

[89] *See* NRC report, *supra* note 14, at 6 (explaining that encryption is not an industry or law enforcement crisis; rather, it is a policy crisis which must be solved).

[90] *See id.* at 4 (concluding that the current policy dealing with encryption is not satisfactory; therefore, a compromise must be reached between the software industry and law enforcement).

[91] *See* Evans, *supra* note 60, at 485.

[92] *See* FBI Report, *supra* note 4, at 5 (referring to Aldrich Ames, a spy for the former Soviet Union, who encrypted the computer files delivered to them).

[93] *See id* at 6 (referring to Ramzi Yousef, mastermind of the World Trade Center bombing, who encrypted his computer files outlining the details of a plan to destroy U.S. commercial airliners).

[94] *See id* at 5.

[95] *See id.* (explaining that in a 1993 survey conducted as part of a National Institute of Justice Report, 28.4% of state and local law enforcement agencies responding encountered encryption technology being used as a way to conceal criminal activity, and an additional 23.9% anticipated such countermeasures being used).

[96] *See id.* at 7.

[97] *See id.*

[98] *See id.* at 5 (explaining that lawfully intercepted communications will be useless in solving and thwarting crimes if the information is not immediately accessible).

[99] Congressional Research Service, No. 96039: Encryption Technology (updated Sept. 1998) [hereinafter CRS Report]. *See also*, FBI Report, *supra* note 4, at 5. The FBI would like to control domestic use of cryptography because it believes that such technology will be used to conceal domestic criminal activities like illegal drug trafficking, child pornography, and domestic terrorism. *See id.*

[100] *See* CRS Report, *supra* note 99 (explaining that no domestic regulation now exists, though FBI Director Louise Freeh has testified that some domestic use restrictions should be implemented.)

international users of encryption software.[101]

The FBI asserts four main reasons for its policy.[102] First, the key to the encryption algorithm will remain in the hands of the FBI or a trusted third party,[103] thereby providing users with the knowledge that their communications will not be subject to unauthorized disclosure to law enforcement officials or illegal "hacker-type"[104] attack.[105] Second, a specific legal process must be followed to seize the encrypted information.[106] Third, a lawful investigation could be conducted without the knowledge of the suspects.[107] Fourth, law enforcement officials at the state, local and federal levels have the technical ability to immediately decrypt electronically encrypted information.[108] The FBI asserts that such a policy is the appropriate balance between the public safety needs of the country and the needs of the software industry.[109]

## IV. THE CLINTON ADMINISTRATION'S GRADUAL CONCESSION TO AND IMPLEMENTATION OF THE COMPUTER SOFTWARE INDUSTRY'S PREFERRED ENCRYPTION POLICY

### A. The Clinton Administration's Policy

In its inception, the Clinton Administration's policy towards encryption was largely shaped by law enforcement organizations and agencies responsible for national security.[110] Though the Administration does not support domestic controls on the use of encryption technology, it did attempt to steer policy towards the use of key recovery systems by "using the indirect route of export controls to influence what types of encryption products are available."[111]

In April 1994, the first initiative, known as the "Clipper Chip" policy,[112] encouraged the software industry to voluntarily use key recovery systems and governmental key recovery agents.[113] The industry strongly objected, primarily based on the fact that the government would hold the keys.[114] The Clinton Administration eventually abandoned this policy and agreed to discuss other options with industry leaders.[115]

In July 1994, the second Administration policy encouraged the industry to develop key recovery systems voluntarily; this policy created the "trusted third party" concept, thereby removing the keys from government entities.[116] The software industry continued to object to a key-recovery system as well as the export controls, because the government did not relax the controls to their satisfaction.[117]

After the two unsuccessful attempts at reaching a compromise, Vice President Gore released a statement on May 20, 1996, detailing the particular changes to encryption policy under consideration by the Administration.[118] These changes include: the replacement of the term "key escrow" with the term "key recovery."[119] The concept of a "trusted third party" was also expanded to allow

[101] *See* FBI Report, *supra* note 4, at 7 (claiming that implementing these systems is the best way for law enforcement to protect the public safety.)

[102] *See id.*

[103] *See* Baker, *supra* note 8, at 292 (defining what the requirements are to be a trusted third party).

[104] *See* United States v. Riggs, 739 F. Supp. 414, 423 (N.D. Ill. 1990) (stating that the term "hacker" is defined as an individual involved with the unauthorized access of computer systems by various means).

[105] *See* FBI Report, *supra* note 4, at 7

[106] *See id.* (explaining that a request for encrypted information would be subject to public scrutiny and accountability thereby assuring that no abuse of power occurs).

[107] *See id.* (explaining that the confidentiality of an investigation would not be compromised).

[108] *See id.*

[109] *See id. See also* NRC Report, *supra* note 14, at 81 (explaining that law enforcement's ability to obtain information is a key element in both prosecutions and investigations).

[110] *See* CRS Report, *supra* note 99.

[111] *See id.*

[112] *See id.* The government policy would require placing a special semi-conductor device, the "Clipper chip," into all government computers. *See also* Evans, *supra* note 60, at 483-84. The signals from these devices are encrypted as they are sent to the receiver which must also be equipped with the device. *See id.* The encryption algorithm has 80-bit strength. *See id.* During the manufacturing process, each chip is divided into two parts and distributed to two government agencies, which law enforcement officials may obtain after being issued the proper order. *See id.*

[113] *See* CRS Report, *supra* note 99.

[114] *See id.* (explaining that many consumers would not purchase encryption software if they knew the United States government had access to the decryption keys).

[115] *See id. See also* A History of Clinton Administration Encryption Policy Initiatives (visited Nov. 19, 1998) <http://www.cdt.org/crypto/admin/initiatives.html> (analyzing and critiquing the President's "Clipper Chip" policy); *see also* NRC Report, *supra* note 14, at 171 (describing the key technical attributes of the "Clipper Chip" initiative).

[116] *See* CRS Report, *supra* note 99 (stating that some detractors of the program referred to it as "Clipper II").

[117] *See id.*

[118] *See id.*

[119] *See id.* (explaining that the term "key escrow" was identified with government control of the keys whereas "key

an organization or the company itself to hold the key or rather "self escrow."[120] These proposed changes were eventually implemented through President Clinton's November 15, 1996, Executive Order.[121]

Additional evidence of a change in the Clinton Administration's policy surfaced during March and April 1998. Vice President Gore wrote a letter to Senator Tom Daschle expressing the Administration's desire to enter into a good-faith dialogue with the computer industry in order to find a balanced approach to encryption policy without forcing a legislative solution.[122] In the letter, the Vice President also hinted that the possibility of relaxing the export controls existed.[123] In April 1998, the Secretary of Commerce[124] and the Undersecretary of Commerce[125] made public statements foreshadowing a change in the existing policy.

### B. Major Changes Since 1996

On May 8, 1997, one of the first changes in policy by the Administration was directed toward banks and other financial institutions.[126] Banks that conduct international transactions are now allowed to use the most powerful encryption technology available without a key recovery system in place.[127] The Clinton Administration reasoned that such institutions are "subject to explicit legal requirements and have shown a consistent ability to provide appropriate access to transaction information in response to an authorized enforcement request . . . ."[128] In July 1998, this policy was extended to include securities firms.[129] These financial institutions are allowed to use advanced encryption technology in the forty-five countries which have acceptable money-laundering laws according to U.S. standards.[130]

One of the most dramatic policy changes occurred on September 16, 1998.[131] Vice President Gore announced that the licensing requirements implemented only two years ago by the BXA had been totally restructured.[132] In a significant policy shift, the government, after a one-time initial review, now allows the mass marketing of 56-bit encryption technology, as opposed to only 40-bit.[133] Surprisingly, the Administration also elimi-

recovery" would be identified as a way to recover lost, stolen, or corrupted keys).

[120] *See id. See also* The Risks of Key Recovery, *supra* note 31 (claiming that "self-escrow" systems, where companies hold the keys, must "provide sufficient insulation between the recovery agents and the key owners to avoid revealing when decryption information has been released").

[121] *See* Exec. Order No. 13,026, *supra* note 1, at 58,767.

[122] *See* CRS Report, *supra* note 99 (describing Vice President Gore's letter to Senator Daschle). See also Jeri Clausing, *Gore Letter Seems to Soften Stance on Encryption*, N.Y. TIMES, Mar. 5, 1998, at D4.

[123] *See* CRS Report, *supra* note 99.

[124] *See* Jeri Clausing, *Commerce Secretary Seeks Compromise on Encryption*, N.Y. TIMES, Apr. 16, 1998, at D5 (summarizing Secretary Daley's comments which claimed that the Administration's policy towards encryption was a failure.)

[125] *See* CRS Report, *supra* note 99 (summarizing Undersecretary Reinsch's comments that the government was developing a plan in conjunction with industry leaders and that legislation was not needed to resolve differences). Such a position was a change from 1997, when he announced a detailed outline of proposed legislation under consideration by the Administration. *See id.*

[126] U.S. Eases Export Ban on Encrypted Financial Software Programs, 16 No. 11 Banking Pol'y Report 9 (1997).

[127] *See id.*

[128] *See id.*

[129] *See* Mark Hendrickson, *Industry Wins Hard-Fought Battle on Encryption*, Sec. Indus. News, July 13, 1998, at 7; *see also* Maria V. Georgianis, *Commerce Dept Eases Export Rules on Banks' Encryption Pdts*, Dow Jones News Serv., July 7, 1998, at 16:48:00. Securities firms were involved in negotiations with the Department of Commerce when the export policy changed for banks and other institutions. *See id.* At the time, securities firms were not considered financial institutions under the Commerce Department's definition. *See id.* The FBI was originally against allowing securities firms an exemption for fear of setting too broad a precedent. *See id.* After further negotiations, it was decided that securities firms should be exempt. *Id.*

[130] *See* Hendrickson, *supra* note 126, at 7; *see also* Countries Eligible to Receive General Purpose Encryption Commodities and Software Under License Exception, 63 Fed. Reg. 50156 (announcing that Anguilla, Antigua, Argentina, Aruba, Australia, Austria, Bahamas, Barbados, Belgium, Brazil, Canada, Croatia, Denmark, Dominica, Ecuador, Finland, France, Germany, Greece, Hong Kong, Hungary, Iceland, Ireland, Italy, Japan, Kenya, Luxembourg, Monaco, Netherlands, New Zealand, Norway, Poland, Portugal, St. Kitts & Nevis, St. Vincent/Grenadines, Seychelles, Singapore, Spain, Sweden, Switzerland, Trinidad & Tobago, Turkey, Uruguay and the United Kingdom are the countries eligible to receive the encryption software).

[131] *See* John Simmons & David Bank, *Restrictions Are Relaxed on Encryption Exports*, WALL ST. J., Sept. 17, 1998, at A3; *see also* Elizabeth Corcoran, *U.S. to Relax Encryption Limits*, WASH. POST, September 17, 1998, at C4.

[132] *See* Press Briefing by the Vice-President, Deputy Chief of Staff John Podesta, Principal Associate Deputy Attorney General Robert Litt, Assistant Director of the FBI Carolyn Morris, Under Secretary of Commerce William Reinsch, Deputy Secretary of Defense John Hamre, and Deputy National Security Advisor Jim Steinberg at 2 [hereinafter Press Briefing] (announcing the specific change in policy during a question and answer period with the press).

[133] *See id. But see supra* Part II.C. (discussing previous export licensing requirements). The Center for Democracy

nated the requirement that companies create and implement a key recovery system.[134] For those companies that do choose to export key recovery technology, it is no longer necessary to report information to a key recovery agent.[135]

The new policy allows other sectors to use any bit and any length encryption technology in their routine business operations worldwide.[136] These sectors include insurance companies,[137] health and medical organizations,[138] subsidiaries of U.S. firms[139] and on-line merchants.[140] When compared to the regulations implemented only two years ago, it becomes obvious that the computer software industry has wielded its power and convinced government officials that such a dramatic change in policy was necessary. This shift by the Administration demonstrates a willingness to restructure policy in a manner that favors the security needs of the business community.

## V. WHY THE CLINTON ADMINISTRATION POLICY WILL CONTINUE TO CHANGE

### A. Loss of Competitive Edge

In 1996, the pre-packaged software industry was estimated to be worth $109.3 billion and is expected to double to $221.9 billion by the year 2002.[141] The United States traditionally dominates this market, but as the software industry continues to become ever more international, the United States must fight to keep its competitive edge.[142] Analysts argue that the American encryption export policies place companies at risk of losing $60 billion in the global software market[143] because international software companies have the opportunity to export much stronger encryption technology than U.S. companies.[144] Many foreign countries do not have regulations as strict as the United States; therefore, they are able to exploit this weakness and increase their share of the market.[145] Whereas U.S. companies, until just recently, only freely exported encryption software up to 40-bit strength,[146] many foreign countries could freely export up to 128-bit strength software.[147] As a result, American policy actually benefits foreign competitors to the detriment of U.S. software manufacturers.[148]

and Technology claims that 56-bit technology is still not adequate to protect one's security. Center for Democracy and Technology, *New Administration Controls Leave Individual Privacy Concerns Unanswered*, Sept. 16, 1998 (citing a group of California researchers who broke a 56-bit length encryption program in only 56 hours).

[134] *See* Press Briefing, *supra* note 132, at 6. *See also supra* Part II.C. (Describing the previous administrative guidelines).

[135] *See* Press Briefing, *supra* note 132, at 6.

[136] *See id.*

[137] *See* Fact Sheet: Administration Updates Encryption Policy, Sept. 16, 1998 [hereinafter Fact Sheet] (stating that insurance companies will be treated like banks and financial institutions allowing them to export to the same approved countries).

[138] *See* Fact Sheet, *supra* note 137, at 1 (explaining that civilian government health agencies are to be included, but biochemical/pharmaceutical manufacturers are not included in the definition).

[139] *See* Statement by the Press Secretary: Administration Updates Encryption Policy, Sept. 16, 1998 (stating that companies headquartered in the United States can now use advanced encryption technology to communicate with foreign subsidiaries, except those located in the seven restricted terrorist countries).

[140] *See* Fact Sheet, *supra* note 137, at 1 (stating that online merchants for client server applications may use the advance encryption technology to aid in securing electronic transactions between the consumers and merchants).

[141] *See* Organization for Economic Cooperation & Development, Measuring Electronic Commerce: International Trade in Software 222 (1998) [hereinafter OECD Report].

[142] *See id.*

[143] *See* Dinh, *supra* note 14, at 391. Foreign software companies are able to export encryption as strong as 128-bits without restriction. *See id.* An estimated 35 million customers and 190,000 businesses are connected to the Internet. *See id.* If businesses cannot assure its customers that their transactions are secure, then the consumer will go to a business that can provide that protection, i.e. a foreign company. *See id.*; *see also* Americans for Computer Privacy ("ACP") [hereinafter ACP] (visited Oct. 30, 1998) http://www.computerprivacy.org/choice.cgi (explaining that U.S. export restrictions could prevent 200,000 high-skill, high-wage jobs from being created).

[144] *See* Dinh, *supra* note 14, at 391.

[145] *See* ACP, *supra* note 143; *see also* Evans, *supra* note 60, at 481-82. Russia's constitution forbids any restrictions on the use of cryptography. *Id.* at 482. Also, in European countries such as Germany, France and Switzerland, the export of encryption technology is "fairly routine." *Id.*

[146] *See* Aarons, *supra* note 18, at 21.

[147] *See* Dinh, *supra* note 14, at 391.

[148] *See* Edmund L. Andrews, *U.S. Restrictions on Exports Aid German Software Maker*, N.Y. TIMES, Apr. 7, 1997, at D1. (reporting that Brokart Informationssysteme G.m.b.H., a German software company, has created a very profitable business selling strong encryption software to companies like America Online, Netscape Communications, Microsoft and others because the United States government does not allow American companies to export powerful data scrambling technology). The President's Export Council Subcommittee on Encryption ("PECSENC") reported that in the past four

## B. Easy to Avoid Regulations

Numerous U.S. international companies, discouraged by government regulations, are attempting to skirt U.S. encryption policy by forming foreign ventures.[149] Such ventures will allow them to develop, manufacture and export powerful data scrambling technology without regard to the U.S. export policy.[150] Network Associates Inc., a data-security software retailer based in Santa Clara, California, for example, is conducting business through a Dutch subsidiary in order to sell their data security software.[151] As a result of this outsourcing, it is estimated that the United States could forfeit 200,000 jobs to foreign competition by year 2000.[152]

Encryption technology is also widely distributed through illegal means. A personal use exemption exists that allows U.S. citizens and permanent residents to travel abroad with encryption hardware and software.[153] Although guidelines are in place for travel with such equipment, no definitive means exist to determine if a product is illegally exported or not, thereby enabling the illicit transportation of the software.[154] This is also easily accomplished by sending the software to foreign countries via a modem.[155] For the government to assert that regulating the export of encryption technology will prevent foreign nations or individuals from acquiring these products is clearly unrealistic.

## C. The Market Will Sort It Out

The Clinton Administration stated that the best way to allow Internet commerce to expand is by allowing the private sector to determine how it will operate.[156] The President directed "all executive departments and agencies to promote efforts domestically and internationally to make the Internet a secure environment for commerce."[157] Experts agree with the specific application of this policy towards the encryption debate.[158] A panel set up by President Clinton to study encryption policy explained that "reliance on users choices and market forces is generally the most rapid and effective way to promote the widespread utilization of any new and useful technology."[159] These experts concluded that mass use of encryption technology is in our national interest; therefore, encryption policy should align itself with market forces.[160]

The government must meet the responsibility of enhancing public safety and national security, but the requirements it imposes should not be so burdensome as to hinder the development of products that incorporate encryption technology.[161] The market will determine if a demand exists for technologies like escrow encryption systems.[162] As businesses have already shown, they generally maintain a voluntary key recovery plan in the case of a forgotten password, misplaced information or other possible mistakes.[163]

years, Brokart has grown to over 250 employees and has offices in numerous countries including the United States. *President's Export Council Subcommittee on Encryption Findings*, Sept. 18, 1998 [hereinafter PECSENC Findings]. Encryption is only 10 % of Brokart's revenue. *See id.* The company expanded by offering support for other forms of electronic commerce, thereby acquiring a larger share of the electronic software market. *See id.* The report also claims that Brokart's success foreshadows "a weakening of the U.S. position as a leader in electronic commerce generally." *See id.*

[149] *See* Dan Goodwin, True Tales from the Encrypt, LEGAL TIMES, Apr. 21, 1997, at 2; *see also* PECSENC Findings, *supra* note 148, at 2. Many computer software manufactures are combining foreign encryption technology with U.S. commercial applications. *See id.* The result is that U.S. companies have encouraged the advancement of encryption development outside the United States. *See id.* In fact, German, Swiss, Canadian, Russian, and Israeli manufactures of encryption software have all "benefit[t]ed from this unintended consequence of U.S. encryption policy." *See id.*

[150] *See* Goodwin, *supra,* note 149, at 2.

[151] *See Network Associates Skirts Encryption-Export Rules,* ASIAN WALL ST. J., Mar. 23, 1998, at A18.

[152] *See* Mike Tonsing, *Deciphering the Encryption Debate*, 45 Fed. Law. 20 (May 1998) (citing information released by the Americans for Computer Privacy).

[153] *See* Baker, *supra* note 8, at 300.

[154] *See* Evans, *supra* note 60, at 490.

[155] *See id.*

[156] *See* Rajiv Chandrasekaran, *Don't Regulate or Tax Internet, Urges Presidential Report,* THE COMMERCIAL APPEAL (Memphis), June 30, 1997, at A1.

[157] Memorandum on Electronic Commerce, 33 WEEKLY COMP. PRES. DOC. 1006, at 1009 (1997).

[158] *Cf.* NRC Report, *supra* note 14, at 7 (explaining that the committee was compromised of individuals with an extensive background in government service, computer technology, cryptography, communications, law enforcement, intelligence, civil liberties, national security, diplomacy and international trade).

[159] *Id* at 7.

[160] *See id.* (stating that cryptography now has more important non-governmental interests and is disconnected with market reality and the needs of the private sector).

[161] *See* OECD Report, *supra* note 141, at 222.

[162] *Cf.* NRC Report, *supra* note 14, at 7 (explaining that customers will consider the costs and benefits of a key escrow system and then make a determination if it fits their needs).

[163] *See* Dinh, *supra* note 14, at 394.

## D. Deregulation Aids Law Enforcement

Law enforcement agencies claim that the increased use of encryption technology will hinder effective policing and protection of the public.[164] This allegation, though correct, must not be the sole reason for strict regulation of encryption software.[165] Encryption will aid law enforcement in its efforts to prevent crime.[166] Cryptography protects a company's trade secrets, which in turn diminishes the likelihood that a competitor will commit economic espionage, which will then aid law enforcement.[167] Also, encryption technology can secure "nationally critical information systems and networks against unauthorized penetration," thereby helping to protect national security.[168]

The export of encryption technology will also aid law enforcement in a broader sense.[169] Because domestic companies supply most of the encryption to foreign nations, the United States is able to keep abreast of how commercial encryption technology is developing.[170] Monitoring commercial development is an easier task when U.S. companies are the primary suppliers of cryptographic software as opposed to foreign suppliers.[171] Also, if U.S. companies abroad are not allowed the same strength of encryption software available to their domestic counterparts, these companies will be forced to buy from foreign vendors, who may be persuaded by their government to sell weak or faulty encryption software to those U.S. companies.[172] If these foreign vendors were to obtain a substantial market share, then the security of U.S. companies would be greatly compromised.[173]

## E. Helping Law Enforcement Cope with Encryption

Changing technologies forced law enforcement organizations and intelligence organs of the government to modify their policies throughout the years; encryption will be no different.[174] One solution to help law enforcement cope with the widespread use of encryption technology is to legislate strict penalties for persons who use encryption for illegitimate or illegal purposes.[175] Obviously, the advantage to such a proposal is that the legislation focuses on individuals using encryption unlawfully rather than individuals using it for legitimate purposes.[176]

Investment in research and development regarding rapid technological change is another creative and productive way to assist law enforcement.[177] Creating a technical center to assist law enforcement agencies without the expertise and resources to battle technological crime is another example of how police may pursue the criminal without punishing the innocent.[178] Inevitably,

[164] *See* FBI Report, *supra* note 4, at 2.

[165] *Cf.* NRC Report, *supra* note 14, at 9.

[166] *See id.* at 37(explaining that encryption provides law-abiding businesses with a way to help prevent crimes from occurring); *see also* Kenneth Flamm, *Deciphering the Cryptography Debate*, POLICY BRIEF NO. 21, July 1997, at 4 (stating that law enforcement recognizes that encryption technology helps prevent electronic crimes, but they still argue for strong controls).

[167] *See* NRC Report, *supra* note 14, at 8; *see also* Thinh Nguyen, *Cryptography, Export Controls, and the First Amendment in Berstein v. United States*, 10 HARV. J.L. & TECH. 667, 670 (stating that U.S. corporations lose more economic and industrial information by illegal interceptions of business secrets than any other way).

[168] *See* NRC Report, *supra* note 14, at 3.

[169] *See id.*

[170] *See id.* at 8; *see also* Flamm, *supra* note 166, at 4 (arguing that if American encryption technology dominates the market than American technologists will be able to better assist law enforcement because they will be more familiar with the domestic products as opposed to unfamiliar and poorly understood foreign encryption software).

[171] *See* NRC Report, *supra* note 3, at 156 (claiming that monitoring the development of commercial encryption software aids traditional national security interest); *see also* Flamm, *supra* 166, at 4 (stating that the economic success of the U.S. software industry is a critical and integral part of effective national security policy).

[172] *See* NRC Report, *supra* note 14, at 156; *see also* Flamm, *supra* note 166, at 4 (claiming that strong encryption advances national security interest whether the codes are breakable or not, because the political adversaries of the U.S. will most likely not have the ability to penetrate and acquire vital national security information).

[173] *See* NRC Report, *supra* note 14, at 156.

[174] *See id.* at 10 (explaining that law enforcement and national security authorities have adapted quite well to changing technological environments).

[175] *See id.* at 12.

[176] *See id.*; *see also* Flamm, *supra* note 166, at 4. Other problems exist besides random individuals using encryption for illegal purposes. *Id.* For example, there is a fear that members of the law enforcement community will be tempted to abuse their power with respect to the access of decrypted information. *Id.* Therefore, "clear guidelines and strict accountability" must be implemented to assure that such abuse does not occur. *Id.*

[177] *See* NRC Report, *supra* note 14, at 12.

[178] *See id.* at 12 (explaining that a technical center should be established to aid federal, state, and local officials burdened with the task of solving highly sophisticated technological problems); *see also* FBI Report, *supra* note 3, at 6. The FBI created the Computer Analysis and Response Team

cryptography will play a substantial role in all transactions over the Internet, but it is unlikely to happen in the immediate future.[179] Now is the most opportune time for the U.S. to study the effects of a relaxed regulatory scheme for encryption, enabling the national security authorities sufficient time to cope with a new technical reality.[180]

### F. Mounting Political Pressure

Though the battle to loosen encryption regulations has been fought mainly between the government and the actual software industry, many in the computer industry are now trying to increase public awareness in order to assert political pressure on the Clinton Administration.[181] Americans for Computer Privacy ("ACP"), a group of ninety companies, including Microsoft, Intel and Sun Microsystems, are engaged in a $2 million advertising campaign in an attempt to educate and motivate the public about the national cryptography policy.[182] The computer industry is lobbying to ease export restrictions and is also focusing on the government's refusal to abandon the idea that all encryption keys should be stored, such goals have been partially realized by the latest shift in the Administration's policy.[183] In an effort to bypass the administration, the ACP is hoping that the ad campaign will encourage citizens to contact Congress in order to persuade them to vote in favor of one of the numerous bills[184] dealing with encryption.[185]

In addition to the ad campaign, another computer industry group is offering the Clinton Administration a plan of its own that satisfies the needs of both law enforcement and software companies.[186] The proposed plan allows the technology to encrypt the information being sent and provides for restricted access to the information "at the beginning and end of each transmission."[187] The White House responded to the plan by stating the government and computer industry were headed in a "refreshing new direction."[188] Undoubtedly, this ad campaign and suggested proposal have had an impact on the Administration's position as evidenced in the Vice President's press briefing on September 16, 1998 and will continue to affect encryption policy.

The Clinton Administration is experiencing political pressures from international organizations like the Organization for Economic Cooperation and Development[189] and the European Union (EU).[190] The EU expressed disapproval of the Clinton Administration's desire to implement a key escrow system.[191] In fact, some foreign governments view the U.S. policy as a potential method of committing industrial espionage, though the main EU argument is that it is opposed to "imposing a specific technological ap-

("CART") which is responsible for "providing assistance in law enforcement investigations where computer generated or stored magnetic media has been obtained pursuant to search and seizure." *Id.*

[179] *Cf.* Flamm, *supra* note 166, at 3 (suggesting that encryption is slowly becoming a cheaper and more common practice in the government and the private sector, but has yet to reach the individual user in a significant manner).

[180] *See id.*

[181] John Simons, *Silicon Valley Lobs Populist Ads in Encryption Battle*, WALL ST. J., July 21, 1998, at A16.

[182] *See id.* The ad campaign will include TV commercials on a few local stations in metropolitan areas and the cable stations CNN, CNBC, and MSNBC. *See id.* The campaign will also place ads in national newspapers and put information on the Internet. *See id.*

[183] *See id.* To influence citizens' views on encryption policy, Americans for Computer Privacy have enlisted the services of Goddard-Claussen, the creator of the original Harry and Louise health-care ads that helped destroy President Clinton's 1993 health-care initiative. *See id.*; *see also* Rajiv Chandrasekaran, *Harry and Louise Have a New Worry: Encryption*, WASH. POST, July 28, 1998 at E1.

[184] *See* FBI Report, *supra* note 3, at 7 (describing and commenting on bills dealing with encryption in the 105th Congress).

[185] *See* Simons, *supra* note 181 at A16; *see also* Press Briefing, *supra* note 132, at 3 (indicating that the ACP was a key player in shaping the new policy implemented on September 16, 1998).

[186] *See* Ralph T. King and John Simons, *Industry Group's Method May Break a Long Impasse With FBI*, WALL ST. J., July 13, 1998, at A16.

[187] *See id.* The information is accessible at certain points, referred to as "private doorbells" or routers, that direct the information to a particular point. *See id.* As the data travels from point A to point B, it is encrypted. *See id.* The information can be retrieved if the address of the sender or receiver is known, because the routers can be "programmed to pull out the message to or from a specific address." *See id.*

[188] *See id.*; *see also* Press Briefing, *supra* note 132, at 7 (stating that the Clinton Administration endorsed this type of encryption technology and is allowing for its export to "deal with the development of local area of wide area networks and the transmission of e-mail and other data networks.")

[189] *See* OECD Report, *supra* note 141; *see also* John Markoff, *U.S. Rebuffed in Global Proposal For Eavesdropping on the Internet*, N.Y. TIMES, March 27, 1997, at A1.

[190] *See* Jennifer L. Schnecker, *EU Seen Rejecting U.S. Encryption Plan*, WALL ST. J., Oct. 8, 1998, at 2.

[191] *See id.*

proach," (i.e. key escrow systems).[192] Even members of President Clinton's own party are openly opposing the Administration's policy and believe that the EU policy will influence the United States.[193] As on-line transactions become increasingly more commonplace, a standardized encryption policy will provide the security demanded by foreign nations if they are to expand their international transactions with U.S. businesses.

## VI. CONCLUSION

The original encryption policy implemented through President Clinton's Executive Order will continue to undergo significant modifications, as exemplified by the September 1998 changes. The software industry will continue to maintain constant political pressure on the Clinton Administration to further deregulate the encryption technology serving commercial purposes. As encryption becomes more ubiquitous, law enforcement and national security entities will be forced to adapt to changing technology. Prohibiting such beneficial technology is not and will not be a viable option for the Administration to pursue. Law enforcement organizations have managed to respond to rapid technological change in the past, and should be encouraged to continue to adapt to new technologies, but should not be allowed to impede on the development of a profitable U.S. based market in advanced encryption technology. These changes will provide the business community and the software industry with more than mere profits. It will provide them with the security needed to flourish in a competitive global market place.

[192] *See id.* (stating that the EU is not opposed to law enforcement having limited access to data, but having the key codes stored in escrow where U.S. security or law enforcement agencies could gain access labels the technology as unsecure).

[193] *See id.* (quoting Representative Zoe Lofgren (D-Calif.) as stating that she admires the EU position and believes that the U.S. policy is flawed).