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 online, 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, 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. 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).

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

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

The length of the key and the complexity of the algorithm determines the strength of the encryption algorithm. The key is measured in bits, and for every bit the number of possible key sequences is doubled, resulting in dramatically stronger encryption as the number of bits increases. 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. Today, the most advanced forms of encryption software have a key length of 1,052-bits.

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. 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. PaDoover 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).


5 See id.

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

7 See FBI Report, supra note 4, at 2.


9 See Stender, supra note 2, at 294; see also High Tech Dictionary (visited Oct. 18, 1998) c9html?lookup=863>. Algorithm is defined as a "set of instructions for solving a problem. Named after Al-Khwarizimi, 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.


15 See High Tech Dictionary (visited Oct. 18, 1998) c9http://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).


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

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 and the Export Administration Act, issued Executive Order 13,026 entitled "Administration of Export Controls on Encryption Products." This particular Order focuses on the export of encryption technology. The Administration’s policy originally 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 seamless.

By authenticating a message, the probability of forgery and repudiation is significantly diminished. Certifying the integrity of a message confirms that a message has not been altered in any way during transit.

A. Key Escrow Systems

The Clinton Administration proposed a key recovery or key escrow system as a way to balance the “needs for information security against the needs of law enforcement and to a lesser extent national security.” Key escrow encryption systems provide encryption key codes to a trusted third party that stores the keys for the users of such technology. These codes allow the holder of the keys to decrypt any encrypted message. Under this law, encryption key codes on all encryption software shipped internationally would deemed the export of data scrambling technology to be a serious threat to national security and foreign policy. The Order authorizes the Secretary of Commerce to issue licenses to manufacturers of encryption technology on a case-by-case basis. In addition, the Order promotes the use of a key recovery management infrastructure — a long-standing cornerstone of the government’s policy.

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 (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).

1999] Decrypting the Politics 195
be provided to the trusted third parties.36 These third parties could release the codes to predetermined authorized parties87 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 exports89 under the authority of the Arms Export Control Act40 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-use53 encryption software from the DoS to both the Commerce Department64 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).
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. Matsusura & George B. Delta, Export Controls on the Internet, 10 No.3 J. Proprietary Rs. 2, 3 (1998) (defining dual-use technologies as those which serve both military and non-military purposes).
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).
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).
59 See id.
divided into ten general categories and numerous sub-categories. As of March 1998, the Commerce Control List included over 200 sub-categories of controlled goods and approximately 100,000 specific goods.

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." The licensing policy was divided into four distinct groups. The first group dealt with the distribution of mass-market encryption software. In order to obtain a license, the BXA must have conducted a one-time review of the software. Only 40-bit encryption software was eligible for such a license after a seven day review under this policy.

The second group represented the exportation requirements of key escrow or key recovery software and commodities. Similar to the first group, this software was subject to a one-time review by the BXA in order to receive its license.

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) or other material/information required to decrypt cipher text . . . are maintained after export or reexport as required by the EAR." If the software received a favorable recommendation, then manufacturers of encryption software were not limited to any particular key length, and they would have been permitted to export their products to nearly all destinations throughout the world.

The third licensing method concerned non-recovery encryption items with up to a 56-bit key length. 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." In addition, exporters must have submitted an acceptable time frame and business plan to the BXA for review. The exporter had a two-year transition period to "develop, produce, and/or market encryption items and services with recoverable features." The permit needed to be renewed every six months; the renewal process was dependent on how well the applicant adhered to the time frame technology will not provide adequate security because researchers have cracked 56-bit codes in 36 hours with a machine that only cost $250,000.

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").

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

See id. at 68,573; see also Center for Democracy and Technology (visited Nov. 19, 1998) (explaining that 40-bit and even 56-bit encryption technology will not provide adequate security because researchers have cracked 56-bit codes in 36 hours with a machine that only cost $250,000).
of the detailed plan submitted by the company. The fourth method handled other encryption issues. The policy in effect prior to the issuance of this rule remains the regulatory scheme for all other encryption products. Exporters may apply for a license through the BXA, but each application will be reviewed on a case-by-case basis.

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: (1) law enforcement organizations concerned with gathering evidence of criminal activity, such as the Federal Bureau of Investigation ("FBI") or the police; and (2) interests concerned with gathering intelligence information concerning national security, such as the National Security Agency ("NSA"). 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. 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. A question arises as to what extent the government should accommodate law enforcement organization's wants.

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. The Aldrich Ames case and Ramzi Yousef case are often cited as examples of criminals who have used encryption technology as a means to avoid revealing their criminal activity.

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

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. Presently, domestic use of the strongest encryption technology is permitted without any key recovery system in place. The FBI is pressuring the Clinton Administration to mandate such systems for both domestic and commercial airliners.

---

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.
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 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 1995 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.)
The FBI asserts four main reasons for its policy. First, the key to the encryption algorithm will remain in the hands of the FBI or a trusted third party, thereby providing users with the knowledge that their communications will not be subject to unauthorized disclosure to law enforcement officials or illegal "hacker-type" attack. Second, a specific legal process must be followed to seize the encrypted information. Third, a lawful investigation could be conducted without the knowledge of the suspects. Fourth, law enforcement officials at the state, local and federal levels have the technical ability to immediately decrypt electronically encrypted information. 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.

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. 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.”

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

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. 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.

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. These changes include: the replacement of the term “key escrow” with the term “key recovery.” The concept of a “trusted third party” was also expanded to allow 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.

See CRS Report, supra note 99.

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

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).

See CRS Report, supra note 99 (stating that some detractors of the program referred to it as “Clipper II”).

See id.

See id.

See id. (explaining that the term “key escrow” was identified with government control of the keys whereas “key

---

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.

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." These proposed changes were eventually implemented through President Clinton's November 15, 1996, Executive Order.

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. In the letter, the Vice President also hinted that the possibility of relaxing the export controls existed. In April 1998, the Secretary of Commerce and the Undersecretary of Commerce 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 recovery" would be identified as a way to recover lost, stolen, or corrupted keys).

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").

See Exec. Order No. 13,026, supra note 1, at 58,767.


See CRS Report, supra note 99.

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.)

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.


See id.

See id.

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 Paks, 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 financial institutions. Banks that conduct international transactions are now allowed to use the most powerful encryption technology available without a key recovery system in place. 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 . . . ," In July 1998, this policy was extended to include securities firms. 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.

One of the most dramatic policy changes occurred on September 16, 1998. Vice President Gore announced that the licensing requirements implemented only two years ago by the BXA had been totally restructured. 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. Surprisingly, the Administration also elimi-
nated the requirement that companies create and implement a key recovery system. For those companies that do choose to export key recovery technology, it is no longer necessary to report information to a key recovery agent.

The new policy allows other sectors to use any bit and any length encryption technology in their routine business operations worldwide. These sectors include insurance companies, health and medical organizations, subsidiaries of U.S. firms and on-line merchants. 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

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).

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

See Press Briefing, supra note 132, at 6.

See id.

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).

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).

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).

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).


See id.

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") (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).

See Dinh, supra note 14, at 391.

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.

See Aarons, supra note 18, at 21.

See Dinh, supra note 14, at 391.

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 Brokarts’ 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 Brokarts’ 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 manufacturers of encryption software have all “benefit[ed] from this unintended consequence of U.S. encryption policy.” See id.

150 See Goodwin, supra, note 149, at 2.


153 See Baker, supra note 8, at 300.

154 See Evans, supra note 60, at 490.

155 See id.


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). See OECD Report, supra note 141, at 222.

161 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).

162 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 bills184 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 Development189 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-
proach," (i.e. key escrow systems). 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. 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 Administra-

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).