1995

A Puzzle Even the Codebreakers Have Trouble Solving: A Clash of Interests over the Electronic Encryption Standard

Sean Flynn

A PUZZLE EVEN THE CODEBREAKERS HAVE TROUBLE SOLVING: A CLASH OF INTERESTS OVER THE ELECTRONIC ENCRYPTION STANDARD

SEAN M. FLYNN*

I. INTRODUCTION

On February 9, 1994, when the National Institute of Standards and Technology (NIST) announced the federal Escrowed Encryption Standard (EES),[1] the simmering debate over encryption policy in the United States boiled over. Public interest groups argued that the standard would jeopardize an individual's right to privacy. U.S. multinationals voiced concerns that the government would undercut private encryption technology and limit their choice of encryption products for sensitive transmissions. Computer software groups claimed that EES lacked commercial appeal and would adversely affect their ability to compete. Pitted against these concerns were those of the law enforcement and national security communities, which countered that the interests of national security required the adoption of EES.

A quick study[2] of EES reveals little that would explain this uproar. The NIST issued EES as an encryption methodology for use in its government information processing[3] pursuant to the Computer Security Act of 1987.[4] The EES is intended to supersede the existing government standard, Data Encryption Standard (DES), which has been in use since 1977 and is very popular.[5] The new standard's methodology is classified, but the government has stated that it represents the state of the art in security protection. The catch in this positive scenario is that the government keeps a backdoor key that will allow it to decrypt encrypted messages.

So why did an obscure and seemingly insignificant announcement cause so much commotion? Upon closer examination, one discovers that

---

* B.A., Duke University, 1990; J.D., Georgetown University Law Center, anticipated 1996.

1. Approval of Federal Information Processing Standards Publication 185, Escrowed Encryption Standard (EES), 59 Fed. Reg. 5997 (1994) [hereinafter Approval of EES].

2. The specifics of the EES are examined in greater detail in Part II.C.

3. Approval of EES, 59 Fed. Reg. at 5998.

4. 15 U.S.C. § 278g-3(a)(5) (1994).

5. OFFICE OF TECHNOLOGY ASSESSMENT, INFORMATION SECURITY AND PRIVACY IN NETWORK ENVIRONMENTS 121–22 (1994).

encryption, though still obscure to many, is a hot commodity in the information age. It is the silver shield that protects personal, financial, trade, and national security information. And, until recently, the government has enjoyed a monopoly over its development and use. Viewed from this perspective, the NIST announcement was seen by many as a government attempt to maintain its monopoly to the detriment of potential users and private developers.

The ensuing clash of interests has created an impasse. Encryption users and privacy advocates refuse to accept the government's EES standard. For its part, the government maintains stringent export controls to undermine the development of feasible alternative standards and to deny software producers economies of scale.

This Note will undertake a number of examinations. First, it will review the government's role in cryptography. Second, it will study EES in detail. Third, it will explore how the EES scheme works with other aspects of the government's encryption policies to trigger legal, economic, and political concerns. Fourth, it will survey the alternatives to EES. Finally, it will suggest how the interests in the current policy debate may achieve an accommodation that would sufficiently address privacy and competitiveness concerns, on the one hand, while meeting national security and law enforcement concerns on the other.

II. A QUICK CRYPTOGRAPHY PRIMER

A. *What is Cryptography?*

Before proceeding further into this complex area, it may be useful to go over some fundamentals. At its base, cryptography is the practice of transforming a message into gibberish (encryption), transmitting it, and transforming it back into "plaintext" (decryption) at the other end.[6] Though once the province of spies, diplomats, and generals as a device to protect sensitive communications, encryption has moved gradually into the mainstream. With the increasing prevalence of networked computing[7] and its increasing vulnerability to tamper-

6. *See, e.g.*, BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY 1–2 (1994).

7. Andrew Johnson Laird, President of Johnson-Laird, Inc., estimated that there are more than 3.2 million "host" computers on the Internet as of July 1994, an increase of 81% from the previous year. Andrew Johnson Laird, Exploring Cyberspace: The Good, The Bad, and The Ugly, *in* 8th Ann. Advanced Computer L. Inst. 390 (Mar. 23–24, 1995) (unpublished manuscript, reproduced by Continuing Legal Education Division of Georgetown University Law Center) (on file with *Law and Policy in International Business*). Estimates of the number of Internet users range from 2 million to 25 million. *Id.* at 391. If electronic money were to become legal tender on the Internet, it would

ing,[8] cryptography has become a valued tool both for businesses and consumers in the protection of proprietary and personal information.

Properly employed, cryptography can perform three distinct functions: (1) authenticate the sender by means of a unique "signature"; (2) protect the confidentiality of the message during transmission and in storage; and (3) assure the integrity of the message through encrypting a digest.[9] In general, the method by which the message is transformed into and out of gibberish is the "algorithm." Each particular encryption is achieved by plugging a string of numbers, or a "key," into the algorithm and then applying the result to the message. Decryption works by running the encrypted message back through the algorithm-key combination.[10] The strength of a cryptographic system is gauged by the length of its key and the complexity of its algorithm.[11]

Traditionally, cryptographic schemes used a single key; the sender encrypted and the receiver decrypted the message with the same key.[12] This system has an inherent weakness: the key must necessarily be distributed to all communicants; the more widely distributed the key, the more likely the possibility that it could fall into the wrong hands. In response to this problem, two researchers at Stanford University created a two-key scheme called "public key."[13] In a public key system, one key, which is posted publicly, encrypts the message; the second key, which is kept secret, decrypts it. Although the keys are mathematically related, each functions in only one direction and, thus, both are needed to complete the encryption-decryption chain of events.[14] Since public key algorithms are cumbersome to calculate, it would be inconvenient to use them for the entire message. In practice, parties use public key schemes

---

produce a "virtual economy" as large as that of the Netherlands. *Electronic Money: So Much for the Cashless Society*, ECONOMIST, Nov. 26, 1994, at 21, 22.

8. Illicit and widespread activities on the Internet include copyright and trademark infringement, theft of trade secrets, software pirating, harassment, and unauthorized entry onto systems by hackers. Laird, *supra* note 7, at 411–20.

9. OFFICE OF TECHNOLOGY ASSESSMENT, *supra* note 5, at 39.

10. SCHNEIER, *supra* note 6, at 1–2.

11. *Id.* at 129.

12. *Id.* at 3.

13. Whitfield Diffie, a mathematician and computer scientist, and Martin E. Hellman, a professor of electrical engineering, created the public key scheme at Stanford University and published their findings in 1976. Steven Levy, *The Cypherpunks vs. Uncle Sam*, N.Y. TIMES, June 12, 1994, Sec. 6, at 47–48. Shortly after the researchers published their findings, three mathematicians at M.I.T.—Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman—implemented a public key system of encryption, which became known by their initials, RSA. *Id.* at 48.

14. SCHNEIER, *supra* note 6, at 29–30.

to exchange a session key and a single-key algorithm.[15] Thus, public key facilitates on the spot creation and secure distribution of the unique session key.

B. *The Federal Government's Preeminent Role in Cryptography*

It is a testament to both the importance and complexity of cryptography that the National Security Agency (NSA),[16] a part of the Department of Defense, has until recently been the sole source of advanced cryptographic know-how in the United States.[17] The NSA has two national missions: to collect foreign signals intelligence and to provide secure information systems to protect classified and unclassified government information and communication.[18] Thus, the government is not only a developer of cryptography technology, it is a user and a regulator of encryption products as well. These multiple roles give the government varying levels of insight into cryptography in the United States. In its roles as regulator and user, the government is able to monitor the current state of encryption technology. In its roles as developer and federal standard-setter, the government is able to influence the development of cryptography in this country.[19] If all of these functions were properly coordinated, the potential would exist for the government to impose its own standards on the marketplace while discouraging other standards.[20] This potential is one of the reasons that government processing standards are not mandated for government agencies.[21]

---

15. *Id.* at 30–31.

16. The NSA was created by a presidential memorandum on October 24, 1952 to monitor and decode transmissions considered relevant to national security. This memorandum and the agency's mission have been cloaked in official secrecy for more than 40 years. John Perry Barlow, *Decrypting the Puzzle Palace*, 7 COMMUN. OF ACM 25, 25 (1992).

17. JAMES BAMFORD, THE PUZZLE PALACE 344 (1982). Although administered by the Department of Defense, the NSA is responsible to the Director of Central Intelligence, who sets objectives, needs, and priorities for the intelligence community. NATIONAL SECURITY AGENCY, BROCHURE (on file with *Law and Policy in International Business*).

18. Exec. Order No. 12333, 46 Fed. Reg. 59,941 (1981). Under the Executive Order, the Federal Bureau of Investigation is responsible for the collection of foreign intelligence and counterintelligence within the United States, while the Central Intelligence Agency has this responsibility abroad. *Id.*

19. It is because of the potency of the three complementary roles of government that the NSA's part in developing the EES scheme is so controversial.

20. This assumes that there is a commercial need for the type of government standard established. As I will explain later, key escrow must have a commercial appeal to succeed.

21. *Hearing on Communications and Computer Surveillance, Privacy and Security Before the Subcomm. on Technology, Environment and Aviation of the House Comm. on Science, Space and Technology*, 103d Cong., 2d.

Otherwise, the government might set the new standard through its immense purchasing power.

1. Setting Federal Standards

The Brooks Act authorizes the Department of Commerce to research and recommend data processing standards for the federal government.[22] Pursuant to this authority, the Department of Commerce issued the government's first encryption standard, the Data Encryption Standard, for use in protecting unclassified computer data and communications.[23]

Although the DES algorithm was developed by IBM, it had been submitted to the NSA for approval.[24] After reviewing the algorithm, the agency recommended certain modifications. Once IBM complied with these recommendations,[25] the standard was approved by the Department of Commerce in 1977.[26] Thus, the NSA's hand was visible in the process of standard setting from the beginning. Critics charged that the NSA was purposefully weakening encryption that was to be made available to the public.[27] This provided a basis for future suspicions concerning the NSA's role in the development of encryption.

The DES was quickly adopted by industry both in the United States and abroad.[28] Today, there are at least 267 products available in the

---

Sess. 12 (1994) [hereinafter *House Clipper Hearing*] (statement of James K. Kallstrom, Special Agent in Charge, New York Field Div., Federal Bureau of Investigation).

22. 40 U.S.C. § 759(d) (1988).

23. NAT'L BUREAU OF STANDARDS, U.S. DEP'T OF COMMERCE, FEDERAL INFO. PROCESSING STANDARD PUBLICATION NO. 46, DATA ENCRYPTION STANDARD (Jan. 15, 1977) (on file with *Law and Policy in International Business*) [hereinafter FIPS PUB. NO. 46].

24. Strong versions of encryption are barred from export by the United States Munitions List, which is administered by the Department of State's Office of Defense Trade Controls. SCHNEIER, *supra* note 6, at 449. However, since the Office of Trade Controls defers to the NSA on matters of cryptography, developers of encryption products send their products to the NSA for review. *Id.* at 452.

25. BAMFORD, *supra* note 17, at 347.

26. FIPS PUB. NO. 46, *supra* note 23.

27. The Senate Select Committee on Intelligence investigated the allegation that the NSA watered down DES and concluded that the agency "did not tamper with the design of the algorithm in any way. IBM invented it . . . and concurred that the agreed upon key size was more than adequate for all commercial applications for which the DES was intended." SENATE SELECT COMM. ON INTELLIGENCE, 95TH CONG., 2D SESS., UNCLASSIFIED SUMMARY: INVOLVEMENT OF THE NSA IN THE DEVELOPMENT OF THE DATA ENCRYPTION STANDARD 4 (Comm. Print 1978).

28. The DES algorithm has become the standard for electronic transfers in the banking and financial communities. OFFICE OF TECHNOLOGY ASSESSMENT, *supra* note 5, at 121.

United States that employ DES and some 164 products that employ DES spread across 25 countries.[29] However, the standard is now more than twenty years old. Though it has been re-approved every five years since its introduction, the NIST stated it will consider replacing DES in its 1998 review.[30]

The Computer Security Act of 1987 called for a new federal encryption standard and laid the principal responsibility for developing future encryption standards on the NIST.[31] However, a Memorandum of Understanding between the NSA and the NIST effectively undermined the Computer Security Act's division of responsibilities such that NIST agreed to rely on the NSA to generate the new encryption technology.[32] Thus, in 1991 when AT&T informed the NSA that it was developing a voice-encryption product with DES technology,[33] the agency already was working on a sophisticated encryption algorithm with a backdoor key as a successor to DES.

This scheme became the Escrowed Encryption Standard, and its hardware version for voice communication was dubbed the Clipper chip.[34] Since Clipper is the result of the NIST standard-setting process, it is unsurprising that the agency considered the interests and concerns of other government agencies when developing the scheme.[35] The Clipper chip was designed both to incorporate the strengths of the latest NSA algorithm[36] and to provide authorized law enforcement officials

---

29. Trusted Information Systems & Software Publishers Association, Encryption Products Database Statistics (Dec. 1994) (on file with *Law and Policy in International Business*) [hereinafter Encryption Products Statistics].

30. Revision of Federal Information Processing Standard 46-1, Data Encryption Standard, 58 Fed. Reg. 69,347 (1993).

31. The NIST is authorized to develop standards for computer security and privacy, 15 U.S.C. § 278g-3(a) (1994); with the assistance of the National Security Agency, § 278g-3(c); and to implement those standards, § 278g-3(b).

32. Memorandum of Understanding (MOU) between the Director of the National Institute of Standards and Technology and the Director of the National Security Agency concerning the Implementation of Public Law 100-235 2 (Mar. 24, 1989). The MOU provides that the NIST will request NSA assistance on all cryptographic matters, including research, development, evaluation, and endorsement. In addition, a working group composed of members from each agency must review all cryptographic matters prior to public disclosure. *Id.* at 3.

33. Michael L. Rozansky, *Taking a Byte Out of Crime*, HOUS. CHRON., July 31, 1994, at 2F.

34. The hardware version of EES for data communication is called "Capstone." OFFICE OF TECHNOLOGY ASSESSMENT, *supra* note 5, at 65.

35. *See House Clipper Hearing*, *supra* note 21, at 40 (Statement by Raymond G. Kammer, Deputy Director, NIST).

36. Skipjack, the latest algorithm, is contended to be "16 million times tougher to crack than the previously endorsed system." Rozansky, *supra* note 33, at 2F.

with a backdoor key to decrypt messages.[37]

Pointing out the disadvantages of DES and dangling the prospect of export approval for products utilizing Clipper,[38] the NSA suggested that AT&T incorporate the yet-to-be-announced Clipper chip into its product. For AT&T, this was a chance to use next generation technology in its product and to win early export approval. After all, the DES was a single-key system with all the inherent key management shortcomings, and it was well over twenty years old. For the NSA, this was an opportunity to commercialize a standard that would give the government access to encrypted messages. Although the agency was still years ahead of the state of the art technology publicly available,[39] the number of strong encryption products available in the United States had exploded. Thus, in April 1993, AT&T was persuaded by the government to use the Clipper chip in its Surity 3600, a mass-market voice scrambling box.[40]

Since the Clipper chip and EES are voluntary technology,[41] the government must rely on widespread acceptance for the scheme to be effective. To this end, federal officials pointed mainly to the security provided by EES.[42] As one Department of Justice official declared, "We are confident . . . of the quality and strength of key-escrow encryption as embodied in this chip, and we believe it will become increasingly attractive to the private sector as an excellent, easy-to-use method of protecting sensitive personal and business information."[43] Nonetheless,

---

37. Approval of EES, 59 Fed. Reg. at 5998. The Clipper chip and EES utilize the classified Skipjack encryption/decryption algorithm. For Clipper, the algorithm and the protected backdoor gateway are placed on a computer chip that is designed to prevent modification or reverse engineering. OFFICE OF TECHNOLOGY ASSESSMENT, *supra* note 5, at 65.

38. *U.S. Sets New Licensing Procedures for Encryption-Capable Exports*, 11 Int'l Trade Rep. (BNA) 212–13 (Feb. 9, 1994) [hereinafter *New Licensing Procedures*].

39. The NSA employs more mathematicians than any other employer and purchases more computer hardware than any other buyer. SCHNEIER, *supra* note 6, at 439.

40. Rozansky, *supra* note 33, at 2F. However, impatient with the government's progress, AT&T introduced an earlier version of their Surity 3600 that made use of a third-party proprietary encryption algorithm. Brad Brass, *AT&T Unveils First Clipper Device on GSA Schedule*, FED. COMPUTER WK., May 9, 1994, at 24, 29.

41. *Id.*

42. "[W]e sought to develop a technology which provides very strong protection for government information requiring confidentiality protection." *House Clipper Hearing*, *supra* note 21, at 42 (statement of Raymond G. Kammer, Deputy Director, NIST).

43. Statement of Jo Ann Harris, Asst. Attorney General, Criminal Division of the Department of Justice, Before the Subcomm. on Technology and the Law of the Comm. on the Judiciary of the United States Senate, May 3, 1994, at 3 (concerning Key Escrow Encryption Program) (on file with *Law and Policy in International Business*).

the only significant purchase of products using the scheme has been an order of nine thousand phones by the Department of Justice.[44] Although many explanations may exist for the commercial failure of the Surity 3600, it is reasonable to conclude that the private sector is reluctant to embrace the EES.

2. Government Purchases

The government created the market for encryption with the development of DES;[45] despite the explosion in telecommunications and the increasing demand for privacy protection, the U.S. government remains the largest purchaser of telecommunication products in the world.[46] Since the government is thus the largest user of encryption, critics of the EES and Clipper scheme fear that the government will harness this enormous purchasing power and forcibly establish the Clipper as a de facto standard.[47] At the moment, however, use of EES and the Clipper chip remains optional for government agencies.[48]

In fact, many agencies have not adopted the standard, choosing to wait for an industry standard to emerge.[49] Although the government could make EES mandatory for government agencies, there are good policy reasons for not doing so. For instance, some agencies, such as the Federal Reserve System, are working with industry to create industry-specific standards.[50] Moreover, not all attempts to establish a government-wide standard have been successful.[51] In the current belt-

---

44. Rozansky, *supra* note 33, at 2F. It has been suggested that these phones comprised all of the units manufactured with the Clipper Chip and that the government wanted to get them off the market. Interview with Ken Mendelson, former Counsel to Congressman Jack Brooks (D-Tex.), Chairman of the House Judiciary Committee, in Washington, D.C. (Mar. 29, 1995). Mr. Mendelson is now General Counsel at Trusted Information Systems, a computer security company that has developed a commercial key escrow system as an alternative to Clipper.

45. In 1977, the National Bureau of Standards (now NIST), solicited proposals for the first Federal Information Processing Standard (FIPS) to protect unclassified government documents. IBM submitted the winning algorithm and DES was born. BAMFORD, *supra* note 17, at 344–49. Prior to that time, encryption software was limited to classified documents. *See id.* at 345.

46. Nina Schuyler, *Bugs in the System*, CAL. LAW., July 1994, at 45–46 (comments of Marc Rotenberg, Director of Elec. Privacy Info. Ctr.).

47. *Id.*

48. Approval of EES, 59 Fed. Reg. at 5998.

49. OFFICE OF TECHNOLOGY ASSESSMENT, *supra* note 5, at 131.

50. *Id.* The Federal Reserve System remains committed to the banking industry's DES-based standard. *Id.* (citing Interview with Marianne Emerson, Asst. Dir., Div. of Info. Resources Management, Bd. of Governors of the Fed. Reserve System (Apr. 17 & June 23, 1994)).

51. As a result of the government's attempt to establish a standard for communications between computer networks, agencies must use two different standards: one to communicate with

tightening mood within government, agency heads remain understandably reluctant to make any significant commitment to—and thus investment in—products utilizing Clipper or EES.

3. Export Controls

Currently, export of cryptographic products is restricted by the Arms Export Control Act[52] and the Export Administration Act,[53] which collectively authorize export control of scientific and technical data and are administered, respectively, by the Department of State[54] and the Department of Commerce.[55] Although the two acts may overlap in their jurisdictions, the stricter Arms Export Control Act and its regulations, the Defense Trade Regulations,[56] govern in application. Under this regime, the Office of Defense Trade Controls (DTC)[57] determines whether an encryption product belongs on the highly restricted United States Munitions List (USML).[58]

According to the governing statute, the USML could apply to all "[i]nformation [s]ecurity [s]ystems and equipment, cryptographic devices, software, and components specifically designed or modified therefore."[59] In practice, however, the Director of the DTC defers to the NSA, which in fact decides whether an encryption product is covered by the USML.[60] Although the DTC will consider applications for export licenses on a case-by-case basis, items on the USML are rarely exported.[61] The practical result of this system is that strong encryption products[62] are barred from export.

During the Cold War, the United States coordinated its export regulations with other members of the Coordinating Committee for

---

the commercial and international worlds and one to communicate with other government agencies. *Id.* at 131–32.

52. Arms Export Control Act, Pub. L. No. 90-629, 82 Stat. 1320 (codified as amended in scattered sections of 22 U.S.C.).

53. 50 U.S.C. app. §§ 2401–2420 (1988).

54. Exec. Order No. 11,958, 42 Fed. Reg. 4311 (1977).

55. Exec. Order No. 12,002, 42 Fed. Reg. 35,623 (1977).

56. 22 C.F.R. §§ 120–30 (1995).

57. The Office of Defense Trade Controls resides in the Bureau of Politico-Military Affairs at the Department of State. 22 C.F.R. § 120.12 (1995).

58. 22 C.F.R. § 121.1 (1995).

59. *Id.* § 121.1, Category XIII(b).

60. *See* SCHNEIER, *supra* note 6, at 449.

61. *Id.*

62. Strong encryption includes DES and EES. *See* OFFICE OF TECHNOLOGY ASSESSMENT, *supra* note 5, at 115 n.5.

Multilateral Export Controls (COCOM), an organization set up to prevent sensitive technologies from falling into the hands of the Eastern Bloc.[63] Under COCOM, any member could effectively veto the decision of another member to re-export a sensitive technology or product.[64] With the dissolution of the Eastern Bloc, COCOM's *raison d'être* disappeared. It was formally dissolved at the end of March 1994.[65] The United States and other former members of COCOM agreed to replace it with a new multilateral organization, the focus of which would be on restricting strategic trade with "rogue" countries and hot spots.[66] Thus, in COCOM's wake, the United States continues to maintain strict export controls on a host of technologies, including encryption.

Since other countries with software industries have less restrictive export controls,[67] and the United States has no import controls on encryption products, DES products are readily imported into the United States from a number of countries,[68] even though they cannot be re-exported. The Clinton Administration considered lifting restrictions on cryptography exports, but the President "determined that vital national security and law enforcement interests compel maintaining appropriate control of encryption."[69] In other words, export controls are the trump card with which the administration can continue to influence the development and use of encryption technology.

It now seems that export controls, once an instrument of foreign relations and military strategy, are used as instruments of domestic regulation.[70] In theory, export restrictions will deter a potential devel-

---

63. 15 C.F.R. § 768.1(a)(1) (1995).

64. *Id.*

65. *U.S., Allies Making "Slow" Progress Toward Setting Up Post-COCOM Regime*, 12 Int'l Trade Rep. (BNA) 533, 534 (Mar. 22, 1995).

66. *Id.*

67. After examining the relevant laws of many former COCOM members and some non-COCOM countries, the Department of Justice found that most do not restrict the importation of encryption products. U.S. DEP'T OF JUSTICE, CLIPPER CHIP REPORT IN RESPONSE TO SENATE REPORT 103-109 14 (1995) (on file with *Law and Policy in International Business*) [hereinafter CLIPPER CHIP REPORT].

68. "We know that companies in Australia, Denmark, Germany, Israel, South Africa, Sweden, Switzerland, and the United Kingdom are freely shipping DES products to the U.S. . . . with no more then [sic] a few days of government export control delay, if any." Statement of Stephen T. Walker, President of Trusted Information Systems, Inc., Before the Subcomm. on Technology and the Law of the Comm. on the Judiciary of the United States Senate, May 3, 1994, at 18 (on file with *Law and Policy in International Business*).

69. Statement by Martha Harris, Deputy Asst. Sec. for Political-Military Affairs, Encryption—Export Control Reform (Feb. 4, 1994).

70. Statement of Whitfield Diffie, Distinguished Engineer of Sun Microsystems, Inc., Before

oper of a strong encryption product from developing a product that does not utilize the EES because sales of the product would be limited to the domestic market.[71] The export controls have a chilling effect on the U.S. software industry: some companies are forced to develop a weak version for export; others refuse to develop cryptographic products because of the added expenses; and the rest face a dampened demand for their products since potential foreign customers see no point in requesting strong cryptography from U.S. companies unable to export it.[72] Strong encryption is already widely available overseas, however, and can be imported into this country.[73]

B. *The Clipper Chip Scheme*

The Escrowed Encryption Standard is a voluntary encryption standard that employs the secret Skipjack algorithm with a backdoor through which law enforcement authorities have access to encrypted messages.[74] When devices employing the Clipper chip communicate with each other, they operate similarly to a public key scheme that creates a session key. Each message contains the Law Enforcement Access Field (LEAF), a special field that carries the chip's identification number.[75] The identification number corresponds to the backdoor decryption key, which is split into two components and stored in escrow and which is used to decrypt the session key.[76]

When law enforcement officials encounter messages encrypted with the Clipper chip, they can retrieve the chip's identification numbers from the LEAFs by running the message through a special device.[77] By

---

the Subcomm. on Technology and the Law of the Comm. on the Judiciary of the United States Senate, May 3, 1994, at 3 (on file with *Law and Policy in International Business*). The appropriateness of using export controls in this manner is outside the scope of this Note. *See* Charles L. Evans, Comment, *U.S. Export Controls 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 L. & COM. REG. 469 (1994).

71. Although the DES is barred from export, the government has approved the EES for export. *New Licensing Procedures*, *supra* note 38, at 212–13.

72. Statement of Stephen T. Walker, *supra* note 68, at 21.

73. A survey found 889 encryption products available across 26 countries, 431 of them using DES. In the United States, 487 encryption products are available, 267 using DES. Encryption Products Statistics, *supra* note 29. Note that the author of this survey is the Software Publishers Association, the software industry's trade group, and that the survey does not indicate whether such encryption products are mass-marketed or user-friendly.

74. Approval of EES, 59 Fed. Reg. at 5998.

75. *Id.* at 6003.

76. *Id.*

77. NATIONAL SECURITY AGENCY, SYSTEM SPECIFICATIONS FOR THE KEY ESCROW SYSTEM 2 (June 30, 1994) (on file with *Law and Policy in International Business*).

presenting the identification numbers to the escrow agents, they can obtain the two components of each chip's decryption key.[78] After piecing the keys together, they can decrypt the session key by running the encrypted versions back through the special device with the key.[79]

The NIST announced EES as part of its mandate to develop and publish Federal Information Processing Standards.[80] Shortly after the announcement, the Department of Justice selected the NIST and the Automated Systems Division of the Department of the Treasury as escrow agents[81] and published rules for the release of the decryption key component pursuant to an authorized wiretap under Title III of the Omnibus Crime Control and Safe Streets Act of 1968,[82] state wiretap statutes, and the Foreign Intelligence Surveillance Act.[83] The procedures provide that in the event that EES encryption is encountered during a court-approved wiretap, the agency must deliver to the escrow agents a certificate containing the source, scope, and duration of the wiretap authorization, and the identification number of the Clipper chip.[84] The agency must ensure that the key component numbers are transferred by secure means and returned upon expiration of the authority or completion of the intercept.[85] In addition, all federal agencies involved in the EES process—the NIST, the Department of Justice, and the Automated Systems Division of the Department of Treasury—have instituted certain security measures, known as the Key Escrow Security System Policy, to govern all computer, communications, physical, and technical security as well as administrative and procedural security measures and personnel training.[86]

Despite this high level of procedural protection, there are no remedies for unauthorized disclosures of the keys. Although the Electronic Communications Privacy Act of 1986[87] prohibits unauthorized intercep-

---

78. *Id.*

79. *Id.*

80. Approval of EES, 59 Fed. Reg. at 6002. For a more detailed discussion of the standard's development see *supra* Part II.

81. CLIPPER CHIP REPORT, *supra* note 67, at 3.

82. 18 U.S.C. §§ 2510 *et seq.* (1994).

83. 50 U.S.C. §§ 1801–29 (1988).

84. U.S. DEP'T OF JUSTICE, AUTHORIZATION PROCEDURES FOR RELEASE OF ENCRYPTION KEY COMPONENTS IN CONJUNCTION WITH INTERCEPTS PURSUANT TO TITLE III 1–2 (Feb. 4, 1994) (on file with *Law and Policy in International Business*) [hereinafter AUTHORIZATION PROCEDURES].

85. *Id.* at 2.

86. KEY ESCROW WORKING GROUP, KEY ESCROW SECURITY POLICY 2 (Nov. 8, 1994) (draft) (on file with *Law and Policy in International Business*).

87. 32 U.S.C. §§ 2510–2521 (1994).

tion and disclosure of electronic communications[88] and provides for a civil remedy,[89] and the Stored Wire and Electronic Communications and Transactional Records Access Act of 1986[90] prohibits unauthorized access to and disclosure of stored communications[91] and provides for a civil remedy,[92] there are no additional protections or penalties in the event of disclosure of the key components by escrow agents or government officials.[93] A possible reason for this void has been presented by the Department of Justice, which has expressed doubt that the improper disclosure of the two key components causes any damage or that such a disclosure would impinge upon any privacy right.[94]

III. GOVERNMENT ENCRYPTION POLICY AND ITS OPPONENTS

Taken alone, Clipper may not have been so objectionable. However, when viewed in combination with the existing strict export regime, Clipper raises some fundamental legal, economic, and political concerns.

A. *Protecting Privacy*

1. Privacy in Electronic Communications

At the heart of the Clipper chip debate is the issue of privacy.[95] As the information age gives way to cyberspace, more and more transactions occur electronically, sending more and more intimate and revealing information through electronic pipelines.[96] Businesses and private citi-

---

88. 32 U.S.C. §§ 2511, 2516–17 (1994).

89. 18 U.S.C. § 2520 (1994).

90. 18 U.S.C. § 2701-10 (1994).

91. 18 U.S.C. § 2701-02 (1994).

92. 18 U.S.C. § 2707 (1994).

93. CLIPPER CHIP REPORT, *supra* note 67, at 10–11. Indeed, the Department of Justice believes that its strict physical and procedural security measures make such disclosure virtually impossible. *Id.* at 10.

94. *Id.*

95. For more detailed treatment of privacy and the Clipper chip, see Jaleen Nelson, Comment, *Sledge Hammers and Scalpels: The FBI Digital Wiretap Bill and its Effect on Free Flow of Information and Privacy*, 41 U.C.L.A. L. REV. 1139 (1994); Mark I. Koffsky, Comment, *Choppy Waters in the Surveillance Data Stream: The Clipper Scheme and the Particularity Clause*, 9 HIGH TECH. L.J. 131 (1994); and Timothy B. Lennon, Comment, *The Fourth Amendment's Prohibitions on Encryption Limitation: Will 1995 Be Like 1984?*, 58 ALB. L. REV. 467 (1994).

96. One example of the ease of entering cyberspace is Microsoft's inclusion of an icon in Windows 95 that instantly connects users to its on-line service, the Microsoft Network. Kevin Reichard, *The Microsoft Network: The One-Click Connection to Win 95 Applications*, PC MAGAZINE, Oct. 10, 1995, at 42.

zens alike want to protect sensitive communications from impostors and from prying eyes.[97] With encryption, senders can ensure that their documents are confidential and free from tampering, and recipients can ensure that the documents and the sender are authentic.

Although "the right to be let alone"[98] is firmly entrenched in our common law, the Supreme Court in 1967 first recognized a privacy interest in electronic communication in *Katz v. United States*.[99] *Katz* held that an individual has a reasonable expectation of privacy in phone conversations and that the Fourth Amendment requires that, in order to tap phone conversations, law enforcement officials must show probable cause that a criminal activity is being or will be committed, limit the scope and duration of the invasion, and be subject to judicial oversight.[100] In response to this decision, Congress enacted Title III of The Omnibus Crime Control and Safe Street Act of 1968,[101] creating procedural safeguards and judicial oversight for wiretapping. However, since electronic communication was not widespread in 1967, the Court never addressed the question of whether individuals had an enforceable expectation of privacy in their data communication. To resolve the issue, Congress passed the Electronic Communications Privacy Act of 1986,[102] recognizing a privacy interest in electronic data communication and extending procedural safeguards to protect that interest.[103]

2. Privacy Concerns Generated by Clipper

Citing this privacy interest against unreasonable searches and seizures of electronic communications,[104] privacy advocates and business people express three concerns about the Clipper scheme: (1) that it is the first step to government monitoring of all communications; (2) that it unfairly presupposes that everyone using the scheme is a criminal; and (3) that it may not offer adequate protection.

First, some fear that EES leads down a slippery slope where, at the bottom, government would have access to all private communica-

---

97. For example, e-mail is as public as a postcard. Vic Sussman, *Policing Cyberspace*, U.S. NEWS & WORLD REP., Jan. 23, 1995, at 54, 57 (quoting cryptographer Bruce Schneier).

98. Olmstead v. United States, 277 U.S. 438, 478 (1928)(Brandeis, J., dissenting).

99. 389 U.S. 347 (1967). *Katz* overruled *Olmstead*. *Id.* at 353.

100. *Id.* at 354–59.

101. 18 U.S.C. §§ 2510–21 (1994).

102. Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. §§ 2510–21).

103. S. REP. NO. 541, 99th Cong., 2d Sess. 3 (1986), *reprinted in* 1987 U.S.C.C.A.N. 3555, 3557.

104. While the First, Third, Fifth, and Fourteenth Amendments have been held to implicate a privacy interest, this Note is limited to a brief consideration of the Fourth Amendment.

tions.[105] Since both the FBI and the NSA have a history of controversial wiretapping,[106] it is especially troublesome that the Department of Justice refuses to discuss publicly the circumstances under which the NSA may have access to the components outside of FISA.[107] Perhaps Justice Louis Brandeis, privacy's most ardent advocate, was prescient in 1928 when he wrote:

> Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home . . . . Can it be that the Constitution affords no protection against such invasions of individual security?[108]

For its part, the government has repeatedly declared that use of the Clipper chip is voluntary[109] and that there are neither plans to mandate for private use a particular type of cryptography nor to criminalize the private use of a particular type of cryptography.[110] Law enforcement agencies assert that they have no desire to achieve continuous surveillance of transaction information access[111] but simply wish to maintain

---

105. "[It] comes down to one simple question: Do you have the right to keep a phone call or a computer transmission private? The government says no." John Mintz & John Schwartz, *Chipping Away at Privacy?*, WASH. POST, May 30, 1993, at H1 (quoting Jim Bidzos, president of RSA Data Security).

106. The NSA and its legal regime are discussed in more detail in Part II.B. For a chronicle of intrigue and arrogance, see generally BAMFORD, *supra* note 17. For an account of the FBI's controversial history of wiretapping, see ATHAN G. THEOHARIS & JOHN STUART COX, THE BOSS: J. EDGAR HOOVER AND THE GREAT AMERICAN INQUISITION (1988).

107. "Whether, and under what conditions, agencies of the U.S. intelligence community may have access to escrowed key components other than in conjunction with FISA intercepts could only be discussed in a classified document" because the sources and methods of intelligence gathering are "sensitive to national security." CLIPPER CHIP REPORT, *supra* note 67, at 4. The Justice Department maintains, however, that U.S. intelligence will act only in compliance with Executive Order 12333 (United States Intelligence Activities, Dec. 4, 1981), and they will not target U.S. citizens anywhere in the world. *Id.* at 4–5.

108. *Olmstead*, 277 U.S. at 474 (Brandeis, J., dissenting).

109. Approval of EES, 59 Fed. Reg. at 6001; Letter from Albert Gore, Vice President of the United States, to Maria Cantwell, U.S. House of Representatives 1–2 (July 20, 1994) (available on Internet from EEF (mech@eff.org)) [hereinafter Letter from Albert Gore]; Statement of Jo Ann Harris, *supra* note 43, at 3.

110. Approval of EES, 59 Fed. Reg. at 5998.

111. "I don't want that [kind of] access—I don't need it." John Schwartz & John Mintz, *Clinton Plan For Wiretaps Taps Fears*, WASH. POST, Apr. 4, 1994, Washington Business at 17, 22 (quoting FBI Director Louis J. Freeh).

their ability to monitor voice communication.[112] Even the Federal Bureau of Investigation has stated that it is willing to accept additional safeguards on wiretaps of data transmission.[113]

Nevertheless, the possibility exists that the government may try to impose the EES standard by use of its vast direct buying power and its indirect influence through government contracts. In the event of a failure to impose such standards, the government may try to restrict competing technology. Indeed, the administration has made rumblings in the past about restricting cryptography technology[114] if law enforcement becomes overwhelmed by non-Clipper technologies.

Second, privacy advocates object to the assumption implicit in EES, namely that everyone is a potential criminal. Since the government holds possession of the keys needed to decrypt messages even before probable cause of criminal activity has been established, Clipper treats everyone—innocent and guilty alike—as a criminal.[115] Moreover, since the government can detect when EES is employed, it might be tempted to infer nefarious activity from its very use (the idea being that only someone with something to hide would use encryption). Thus, there exists the danger that mere use of encryption may be raised to establish probable cause.

In response to this objection, the government counters that, since agents must obtain a court order to perform a wiretap operation, Clipper does not affect substantive privacy rights.[116] The current wiretap law permits the government to translate or decode intercepts as necessary.[117] From this point of view, the escrow arrangement and release procedures function only to verify existing authorization and to

---

112. "Law enforcement is interested in voice communications 99 percent of the time." Schuyler, *supra* note 46, at 48 (quoting Kent Walker, Asst. U.S. Attorney in San Francisco).

113. Schwartz & Mintz, *supra* note 111, at 22.

114. FBI Director Freeh raised the possibility of restricting all encryption schemes that the government was unable to crack. *FBI on the Line*, Digital Media, Nov. 7, 1994, *available in* LEXIS, News Library, CURNWS File.

115. "[I]t is like [the government is] saying that every single communication in this country regardless of how it is conducted and regardless of where it is conducted and who conducts it may involve a criminal plot." *Privacy Expert Says Block the Clipper Chip*, Newsbytes News Network, June 27, 1994, available in LEXIS, News Library, CURNWS File (quoting Marc Rotenberg, Director of the Elec. Privacy Info. Ctr.).

116. CLIPPER CHIP REPORT, *supra* note 67, at 10.

117. A Department of Justice official testified that wiretap statutes permit the translation or decoding of authorized wiretaps. Statement of Jo Ann Harris, *supra* note 43, at 7. The statute defines "contents" to include "any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8) (1994).

prevent unauthorized release.[118] Nevertheless, the government has failed to address the perception of presumed guilt that Clipper introduces into the mix and has left open the possibility that the fact that an idividual employs encryption may be used to build a case for probable cause of criminal activity.

Third, some question the wisdom of relying on a secret and untested algorithm, in that the Clipper chip may offer a false sense of security. Although the Clipper has received high praise from a group of five independent evaluators,[119] a scientist recently discovered a flaw[120] that would allow sophisticated programmers to bypass the government's backdoor access and superencrypt data.[121] In this case, the flaw works to the advantage of privacy users, but it illustrates the concern stemming from reliance on a chip that remains untried and untested by private users.

Thus, given the above issues with regard to privacy concerns generated by Clipper, it is not unlikely that there are a number of potential users who would shy away from the technology on privacy grounds alone.

B. *A Competitive Software Industry*

Unlike objections prompted by privacy concerns, which are essentially legal in nature, the software industry's objections are economic and, thus, very political.[122] While the government may have a legitimate interest in influencing the development of strong cryptography in the long term, the short term side-effects of this policy may have disastrous consequences for the U.S. software industry. A software industry group claims that export controls could cause the U.S. software industry to lose as much as nine billion dollars in revenues.[123] Given that the market is already thriving without large-scale U.S. participation,[124] restricting

---

118. *See generally* AUTHORIZATION PROCEDURES, *supra* note 84.

119. Ernest F. Brickell et al., Skipjack Review Interim Report: The Skipjack Algorithm 1 (July 28, 1993) (*reprinted in House Clipper Hearing*, *supra* note 21, at 127).

120. A technical consideration of the Clipper chip is beyond the scope of this Note. For further discussion of the technical capacity of the Clipper chip, *see, e.g.*, Stephanie Stahl, *Flaw Discovered in Clipper Chip*, INFORMATIONWEEK, June 20, 1994, at 28.

121. Schuyler, *supra* note 46, at 48.

122. U.S. Representative Cantwell (D-Wash.), whose district includes the home of Microsoft, sponsored a bill to loosen export restrictions. 140 CONG. REC. H5548 (daily ed. July 12, 1994) (statement of Rep. Cantwell).

123. Bob Violino, *Encryption Triggers Conniption*, INFORMATION WEEK, Feb. 7 1994, at 15.

124. Irrespective of U.S. export controls, a booming international market for cryptography

U.S. software companies simply undercuts their overall competitiveness. In response, some companies are forced to develop two products: one for the domestic market with strong encryption technology and one for the market abroad with a weaker technology.[125] Other companies simply do not export their products.[126]

In essence, the government is competing head-to-head with domestic cryptography developers. With the introduction of EES and its classified algorithm, the government has become the software industry's most fierce competitor.[127] The government's goal, according to some, is nothing less than preventing the widespread adoption of an international, compatible, easy-to-use, strong public key system.[128]

EES has failed to add value to the market for encryption products. Since the EES algorithm is classified, the standard has had little effect on the pace of cryptographic innovation. In the long term, the lack of variety in encryption products may slow the overall pace of improvements in the technology.[129] Furthermore, Clipper did not start out strongly[130] and has failed to achieve wide acceptance.[131] There are several explanations for this failure. First, other technologies, such as a combination of DES and RSA,[132] are emerging as competing standards.[133] Second, potential users are concerned about privacy and the

---

does exist. The Software Publishers' Association found 889 products—431 of them with DES—across 26 foreign countries. Encryption Products Statistics, *supra* note 29.

125. For example, Lotus Development Corp., the fourth largest U.S. software company, needed to develop a weaker version of its Notes e-mail package for export. James Coates, *A Diverse Group of Critics Hopes to Clip U.S. Code Plan*, CHI. TRIB., Mar. 28, 1994, Sec. 4, at 1, 2. By contrast, Netscape decided to market a 40-bit encryption scheme worldwide rather than design a stronger version for the United States. Graeme Browning, *Code Words*, NATIONAL J., Oct. 21, 1995, at 2589–90.

126. Of 487 encryption products identified by the Software Publishers' Association, 267 employ DES and, therefore, they cannot be exported. Encryption Products Statistics, *supra* note 29.

127. "For almost 10 years, I've been going toe to toe with [the NSA]. The success of [my] company is the worst thing that can happen to them. To them, we're the real enemy, we're the real target." Levy, *supra* note 13, at 50 (quoting D. James Bidzos, Director of RSA Data Security).

128. *Id.*

129. OFFICE OF TECHNOLOGY ASSESSMENT, *supra* note 5, at 130.

130. Of the 298 individual comments submitted following announcement of the EES proposal, nearly all opposed adoption of the standard. Approval of EES, 59 Fed. Reg. at 5998.

131. IBM and the International Chamber of Commerce have come out against the Clipper Chip. Rozansky, *supra* note 33, at 2F.

132. The Internet Task Force is developing an encryption standard that combines DES with RSA public key technology. Mitch Wagner, *E-Mail Encryption Standard Readied*, ELECTRONIC ENGINEERING TIMES, Feb. 6, 1995, *available in* WESTLAW, Elengt File.

133. As stated in one source in March 1995, "RSA's encryption is fast moving to becoming a standard—or at least the basis for one." Daniel S. Levine, *On-Line Commercial Traffic Seeks Route to 'Net Gains*, S.F. BUS. TIMES, Mar. 17, 1995, at A7, *available in* WESTLAW, Bus-date File.

security of key escrow and of a classified algorithm.[134] Finally, technological uncertainty may cause firms to wait and see which standard emerges as the market leader.[135] With EES, the government has failed both to spur innovation of encryption technology and to offer an acceptable alternative to existing products.

C. *Public Safety/National Security Interest*

The Supreme Court has held that the executive branch has a constitutional duty to "apprehend and obtain conviction of those who have violated criminal statutes of the United States"[136] and "to protect our Government against those who would subvert or overthrow it by unlawful means."[137] To this end, the government asserts that wiretapping is an invaluable tool in solving and preventing crimes.[138] While acknowledging the need to protect the privacy of information, law enforcement officials[139] are concerned that a significant criminal element may be able to use encryption to cover its activities.[140] Computer crime is wide-ranging and includes white collar embezzlement, financial theft, pilfered services, drug smuggling,[141] terrorism, and child pornography.[142] Moreover, should digital cash become a reality without safeguards to track financial transactions, money launderers, terrorists, and organized crime will be able to move cash freely and talented counterfeiters could have a field day.[143]

---

134. OFFICE OF TECHNOLOGY ASSESSMENT, *supra* note 5, at 130 n.38.

135. *Id.* at 130.

136. United States v. Valenzuela-Berual, 458 U.S. 858, 863 (1982).

137. United States v. United States District Court, 407 U.S. 297, 310 (1972).

138. According to the Department of Justice, over the past decade, more than 22,000 convictions have resulted from court-approved surveillance. Statement of Jo Ann Harris, *supra* note 43, at 1.

139. These include officials at the Treasury Department's Financial Crimes Enforcement Network, the Justice Department's Criminal Division, the Federal Bureau of Investigation, and banking regulators including the Federal Reserve. Benjamin Wittes, *The Dark Side of Digital Cash*, LEGAL TIMES, Jan. 30, 1995, at 1, 24.

140. Although no hard numbers exist for the amount of computer crime, experts at the Federal Law Enforcement Training Center would begin estimates in the billions of dollars. Sussman, *supra* note 97, at 55.

141. The challenge posed by strong encryption is especially prevalent in drug cases where wealthy drug dealers can afford to purchase sophisticated cryptography. In 1993, 75% of court-authorized wiretaps and bugs were approved for narcotics investigations. Jonathan Erickson, *Who's That Tapping at Your Back Door?*, DR. DOBB'S J., Nov. 1994, at 6.

142. Sussman, *supra* note 97, at 56.

143. Wittes, *supra* note 139, at 1, 24. Stanley Morris, Director of the Treasury Department's Financial Crimes Enforcement Network, asserts that safeguards are "very, very high priority." *Id.*

Scott Charney, chief of the Justice Department's computer crimes unit, summed up law enforcement's dilemma:

> People do want the ability to engage in transactions with the understanding that these transactions aren't subject to surveillance . . . . This may be good for 99 percent of people, because 99 percent of people are law abiding and need privacy protections. But what about the others?[144]

Additionally, the FBI has warned that new encryption technology is making it more difficult to tap phones[145] and that easy access to strong encryption by the criminal element would pose "an extremely serious threat to the public safety and national security."[146] Law enforcement agencies thus distinguish between the availability of encryption for the sophisticated programmer and encryption for the novice; their primary concern is that standardized and easy-to-use encryption may become widely available.[147] The administration's encryption policy is effective in addressing this concern to the extent that it discourages the development of strong, user-friendly, affordable, and accessible encryption.

The NSA also has a very real interest in keeping the lid on what could quickly become Pandora's box.[148] The National Security Agency has two missions: (1) to gather signal intelligence and (2) to develop encryption technology to protect U.S. government classified information.[149] Strong encryption that is readily available and easy to use may make the NSA's first mission more difficult.

At first glance, the NSA's experience and expertise[150] should make it uniquely qualified to develop strong encryption technology that meets the twin goals of protecting the privacy of users and allowing law enforcement to monitor criminal communications. There is fear, however, that the concerns and agenda of the NSA are driving the entire

---

144. *Id.*

145. Erickson, *supra* note 141, at 6.

146. *House Clipper Hearing, supra* note 21, at 13 (statement of James Kallstrom).

147. Stewart A. Baker, *Don't Worry, Be Happy: Why Clipper Is Good for You*, WIRED, June 1994, at 130, 132.

148. Statement of Vice Admiral J. M. McConnell, Director, NSA, Before the Subcomm. on Technology and the Law of the Comm. on the Judiciary of the United States Senate, May 3, 1994, at 5 (on file with *Law and Policy in International Business*).

149. Baker, *supra* note 147, at 133. However, the NSA's charter document, a seven-page memorandum signed by President Truman, remains classified. BAMFORD, *supra* note 17, at 1.

150. The NSA has more expertise in cryptography than any other organization in the United States. Baker, *supra* note 147, at 133.

U.S. encryption policy.[151] Currently, the agency plays a large role in export controls by determining whether an encryption product should be on the USML. In addition, pursuant to an agreement with the NIST, the NSA plays a significant role in setting federal processing standards.[152] Both prongs of the administration's current policy cater to the NSA's concerns. First, strict export controls help prevent encryption of foreign communications that would jeopardize the NSA's ability to monitor signal intelligence.[153] Second, Clipper might lead to an international encryption standard[154] to which NSA would have the backdoor keys.

IV. CLIPPER CHIP AND EXPORT CONTROLS CANNOT ACHIEVE GOVERNMENT'S GOALS

The administration needs to realize that its twin policies of Clipper Chip promotion and strict export controls are flawed and are doomed to fail because of strongly held legal and economic objections.

First, the Clipper scheme poses serious privacy and technical concerns. The Clipper may be the first step on a slippery slope to greater government intrusion. Given the history of surveillance by the FBI and NSA, the agencies' roles in developing EES and Clipper raise suspicions about the chip's reliability and the access to the backdoor decryption key. In addition, employment of Clipper may be used to infer probable cause. Moreover, there are doubts about a product that has not been subjected to trial by the market.

Second, the policy of strict export controls undercuts the ability of U.S. software developers to compete. Export controls prevent U.S. software developers from including strong encryption in their products and put them at a competitive disadvantage with their international rivals. Moreover, the restrictions prevent encryption developers from participating in a lucrative market.

Third, as a result of these concerns and the lack of a clear standard, Clipper has not been embraced by private users. People will not entrust the intimate details of their lives or confidential financial information to an algorithm that is classified. Not only is performance an issue,[155] but users of encryption, especially foreign users, will question whether

151. Interview with Ken Mendelson, *supra* note 44.

152. *See supra* Part II.B.1 (discussing standard setting).

153. Levy, *supra* note 13, at 49–50.

154. *Id.* at 49, 51.

155. Notwithstanding the findings of the five evaluators. *See supra* note 119 and accompanying text.

privacy is really protected by encryption technology that was developed by the super-secret NSA.[156]

V. IN SEARCH OF A SOLUTION

There are four possible outcomes to the current situation. First, the government may try to impose a standard by executive fiat. Second, the government may stick to its policy and software developers will continue to operate under the current encryption regime. Third, there may be a legislative solution. Fourth, all sides may reach an informal accommodation. For the most part, both the opponents and the supporters of the Clipper scheme are warily eyeing each other to see who is going to make the first move, though one public interest group opposed to the strict export controls has filed suit against the government seeking their removal.[157]

A. *Resolution Through Executive Action*

In general, the Clinton administration has taken a conciliatory approach. In a letter to U.S. Representative Cantwell, Vice President Gore indicated that the administration was willing to sit down with the software industry to reach a mutually acceptable solution for data encryption.[158] To that end, the Interagency Working Group on Encryption and Telecommunications Policy[159] (IWG) was created to consider the economic significance of a change in the federal encryption standard and to adjust the administration's approach appropriately.[160] The IWG has been working with industry, the private sector, privacy advocates, and members of Congress to come up with alternatives to the Clipper scheme; those alternatives include new technologies, alternative escrow

156. "If you're a foreigner, assuming you have no bad intentions, are you going to feel secure knowing that the U.S. government can read your mail anytime they want?" *Security, Privacy and Reliability Issues Important to GII*, Daily Executive Rep. (BNA), Feb. 14, 1995, S-7, S-9 (quoting Jim Burger, Director of Government Affairs for Apple Computer).

157. The Electronic Frontier Fund (EFF) has filed a suit against the federal government seeking to lift export controls on encryption software. David Johnson, Chairman, EFF, Address at the 8th Ann. Advanced Computer L. Inst. (Mar. 23, 1995).

158. Letter from Albert Gore, *supra* note 109, at 2.

159. The IWG consists of representatives from the National Security Council, White House Office of Science and Technology Policy, National Economic Councils, Departments of Commerce, Justice, State and the Treasury, NIST, Office of Management and the Budget, FBI, NSA, Central Intelligence Agency, U.S. Customs Service, Federal Communications Commission, and the Office of the Vice President. CLIPPER CHIP REPORT, *supra* note 67, at 16.

160. *House Clipper Hearing*, *supra* note 21, at 48 (statement of Raymond G. Kammer, Deputy Director, NIST).

agents, and a government standard for data encryption.[161] Currently, the IWG is circulating a working paper that purportedly recommends alternatives to EES such as commercial escrow and the use of published algorithms.[162]

Nevertheless, although the administration has said it will not seek legislation restricting the use of cryptographic products in the United States,[163] the FBI Director has already raised the specter of such a possibility.[164] Moreover, in the wake of the bombing of the federal building in Oklahoma in early 1995, the administration may take a harder line with wiretaps and encryption. Most recently, it proposed legislation to allow emergency wiretaps of suspected terrorists; this proposal, however, was rejected by the Senate.[165]

B. *Status Quo*

The government cannot maintain its current monopoly in cryptographic technology. In fact, a good argument can be made that many significant advances in cryptography occurred outside of government, including DES and public key.[166] As the need for cryptography steadily grows,[167] so does the number of cryptography producers.[168] The cryptography genie is out of the bottle, and it is doubtful that government can put him back in.

1. Public Key Without Escrow

Public key standards[169] have proliferated across cyberspace, thanks to the success of RSA Data Security and Pretty Good Privacy (PGP). RSA

---

161. CLIPPER CHIP REPORT, *supra* note 67, at 16.

162. Interview with Dorothy E. Denning, Georgetown University Department of Computer Science, Member of Evaluation Committee for EES, in Washington, D.C. (Mar. 24, 1995).

163. *House Clipper Hearing*, *supra* note 21, at 47 (statement of Raymond G. Kammer, Deputy Director, NIST). "You can use whatever encryption you want to in the United States." *Security, Privacy and Reliability*, *supra* note 156, at S-9 (quoting Mike Nelson, Spec. Asst., White House Office of Science and Technology Policy).

164. *FBI on the Line*, *supra* note 114.

165. Helen Dewar & Kenneth J. Cooper, *Senate Rejects Clinton Proposal to Allow Terrorist Case Wiretaps*, WASH. POST, May 27, 1995, at A11.

166. Interview with Ken Mendelson, *supra* note 44.

167. New technologies expose new vulnerabilities to fraud, hackers, corporate espionage, eavesdropping, and foreign industrial espionage. Karen L. Casser, Address at the 8th Ann. Advanced Computer L. Inst. (Mar. 23, 1995).

168. According to the Encryption Products Database Standard, 889 software and encryption products are available worldwide. Encryption Products Statistics, *supra* note 29.

169. *See supra* Part II.A. (discussing public key cryptography).

holds the patents for the original public key algorithms, while PGP incorporates some of these algorithms in its code.[170] By virtue of their power, RSA-based public key algorithms are currently emerging as the standard.[171]

In April 1995, three of the largest on-line information companies and two major Internet software providers agreed to a security standard for transactions on the Internet.[172] The agreement consolidates two currently incompatible standards and will allow Internet users to communicate with one another using the same encryption scheme.[173] PGP, developed by amateur cryptographer Zimmerman and completed by mid-1991, was placed on the Internet by one of his friends and is now available for use by anyone with a modem and a computer.[174]

Notwithstanding their popularity and appeal, RSA-based algorithms face a major hurdle in the form of continued opposition on the part of the federal government.[175] Since they would qualify as strong encryption technology, these algorithms are barred by the USML from export and only the weaker, 40-bit versions are exportable.[176] It seems all but certain that in order to obtain an export license, public key algorithms will have to provide for some type of backdoor access.

2. International Clipper

Hewlett-Packard is working on a hardware encryption scheme that would give encryption users a choice of technologies while allowing a national government to access encrypted messages within its borders.[177] According to the plan, each country would issue an electronic card to

---

170. OFFICE OF TECHNOLOGY ASSESSMENT, *supra* note 5, at 124–25; SCHNEIER, *supra* note 6, at 436. It is alleged that Zimmerman used proprietary RSA algorithms without permission. Levy, *supra* note 13, at 60.

171. Levine, *supra* note 133, at A7. Despite an open invitation, prestige, and a cash prize, no one has yet broken RSA's code. *Id.*

172. Peter H. Lewis, *Accord is Reached on a Common Security System for the Internet*, N.Y. TIMES, Apr. 11, 1995, at D5. The companies are American Online, Compuserve, IBM, Netscape Technologies, and Enterprise Integration Technologies. *Id.*

173. *Id.*

174. John Schwartz, *Privacy Program: An On-Line Weapon?*, WASH. POST, Apr. 3, 1995, at A1, A13. Zimmerman may be indicted for violation of U.S. export laws. *Id.*

175. Some experts believe the government will pressure RSA to create a backdoor for law enforcement. Levine, *supra* note 133, at A7.

176. A 40-bit key encryption program developed by RSA for Netscape was recently cracked in eight days. Browning, *supra* note 125, at 2590.

177. Jill Gambon, *The Business of Security*, INFORMATION WEEK, Apr. 10, 1995, at 64, 65.

anyone wishing to encrypt his or her communications.[178] The card would contain all of the cryptographic standards approved for use within that country and would give the user the choice of which standard to employ.[179] When the user transmitted a message, the card would stamp the message, much like a postage stamp.[180] By examining the stamped message, the government could determine how the message was encrypted and then proceed to decrypt it.[181]

Although Hewlett-Packard's scheme offers more options than the Clipper scheme and is designed to work internationally, it has one major drawback: the government would be intimately involved. Arguably, this scenario is more intrusive than Clipper because a government would have unfettered access to all encrypted communications and would have the power to select the range of encryption technologies available.

3. Commercial Key Escrow

There are several companies working on commercial key escrow systems, including Banker's Trust, Trusted Information Systems, and AT&T.[182] A commercial key escrow system functions much like Clipper, with two notable exceptions: (1) the system is not limited to any one encryption algorithm and (2) the government does not retain possession of the decryption keys. However, the government would have access to the decryption key after presenting a court authorization to install a wiretap.[183]

In the Trusted Information Systems (TIS) scheme, for example,[184] companies or individuals would deposit the decryption key for their encryption products with a bonded or licensed commercial agent, where it would be held in trust under rigid safeguards.[185] Each encrypted communication would carry a field containing the identification of the escrow agent and a copy of the decryption key, the latter also en-

178. *Id.*

179. *Id.*

180. Elizabeth Corcoran, *Three Ways to Catch a Code*, WASH. POST, Mar. 16, 1995, at B11, B12.

181. *Id.*

182. Trusted Information Systems and AT&T have software proposals while Bankers Trust has proposed an international system with encryption hardware. Dorothy E. Denning, *The Case for "Clipper,"* TECH. REV., July 1995, at 48, 54–55.

183. Interview with Ken Mendelson, *supra* note 44.

184. Although all commercial key escrow systems have commercial escrow, allow for government access, and are not limited to a particular algorithm, they vary enough to be confusing. In the interest of clarity, this Note will examine how one particular system, TIS, operates.

185. Interview with Ken Mendelson, *supra* note 44.

crypted.[186] The whole arrangement resembles a locked box with an address on the outside and a key on the inside.[187] By retrieving the escrow agent's identification and presenting the proper identification or authority, the individual or company could obtain the decryption key.[188] Since the individual or business users of the commercial escrow system would have entered into a contract with the commercial key agent, the agent would be bound by contract law[189] and thus liable for unauthorized disclosure and use of the key.[190]

Commercial key escrow addresses many of the concerns in the current debate. The government would not have possession of the decryption keys, and access would be administered by a neutral third party. The system is not limited to one algorithm, encouraging software companies to develop new algorithms and allowing users to choose whichever method best suits them. For its part, government would have access to keys uncovered during a valid wiretap. Nevertheless, users of commercial key would be ceding to the government the right to decrypt their communications if the government finds probable cause. For some privacy advocates, even this line is one that should not be crossed.[191]

C. *Resolution through Legislative Action*

It would be an understatement to say that the EES announcement was quietly received in the halls of Congress. Although there have been some hearings, few bills on the subject have been introduced since the announcement, as the Democratic Congress appeared reluctant to make any substantive changes to the government's encryption policy. As noted above,[192] the Republican Congress rejected an administrative proposal to expand the authority of law enforcement agencies to make wiretaps. It seems that the current Congress will continue to let the

---

186. Corcoran, *supra* note 180, at B12.

187. *Id.*

188. Interview with Ken Mendelson, *supra* note 44.

189. *See* Robert L. Dunne, *Deterring Unauthorized Access to Computers: Controlling Behavior in Cyberspace through a Contract Law Paradigm*, 35 JURIMETRICS J. 1, 12 (1994) (suggesting contract law is more appropriate than criminal law for controlling low level illegal acts).

190. Interview with Ken Mendelson, *supra* note 44. Although most of the elements could be implemented under existing law, the system could benefit from legislation to lock in legal rights, obligations, and remedies. Interview with Beryl Howell, Senior Counsel to Senator Patrick Leahy, Senate Judiciary Subcommittee on Antitrust, Business Rights, and Competition, Washington, D.C. (Mar. 23, 1995).

191. The Electronic Frontier Fund and Electronic Privacy Information Center are both in this camp.

192. *See supra* Part V.A.

White House make initiatives and be content to defeat the proposals or to enact implementing legislation.[193]

In May 1995, both the House and the Senate convened hearings to question representatives of the NSA, NIST, and the Department of Justice on the details of Clipper as well as to solicit expert opinion from private industry.[194] In July 1994, Representative Maria Cantwell (D-Wash.), whose congressional district includes Redmond, the home of Microsoft, proposed an amendment to the Export Administration Act that would have eased the export controls on encryption software.[195] In exchange for dropping the proposed amendment, Vice President Gore promised that the administration would work with industry to come up with an alternative to Clipper for high speed data transmission and pointed out that the administration supported a five-month policy review and two studies on export controls.[196] Upon closer examination, however, the Vice President's letter did not offer anything new but simply restated the administration's current encryption policy.[197] Also in July, Senator Patrick Leahy (D-Vt.) attached language to the Senate Report for the Justice Department's annual budget instructing the Attorney General to answer ten detailed questions on the Clipper scheme.[198]

Perhaps the most comprehensive legislative proposal, the Encryption Standards and Procedures Act of 1994,[199] was offered by Representative

---

193. Beryl Howell believes that legislation will eventually be necessary to implement commercial key escrow or a mandatory government standard, particularly to address the issue of how law enforcement and intelligence agencies obtain access to escrowed keys. Interview with Beryl Howell, *supra* note 190. In contrast, Stewart A. Baker believes that legislation is by no means inevitable and probably unnecessary. Interview with Stewart A. Baker, former General Counsel to the NSA, in Washington, D.C. (Mar. 23, 1995).

194. *Hearing on the Administration's "Clipper" Chip Key Escrow Program Before the Subcomm. on Technology and the Law of the Senate Judiciary Comm.*, 103rd Cong., 2d Sess. (1994); *Hearing on Communications and Computer Surveillance, Privacy and Security Before the Subcomm. on Technology, Environment & Aviation of the House Comm. on Science, Space and Technology*, 103d Cong., 2d Sess. (1994).

195. H.R. 3937, 103d Cong., 2d Sess., 140 CONG. REC. H5548 (1994).

196. Letter from Albert Gore, *supra* note 109. When Senator Leahy asked about the administration's policy review at the subcommittee hearing, he was told there had only been a few meetings. Statement of Sen. Patrick Leahy on Vice President Gore's Clipper Chip Letter, July 21, 1994 (on file with *Law and Policy in International Business*) [hereinafter Statement of Sen. Leahy].

197. Statement of Sen. Leahy, *supra* note 196. The letter stated that Clipper remained the voluntary federal standard for voice communication, that the administration would work with industry to develop a key escrow system for data communicaiton, and that there would be no restrictions on encryption products currently exportable. Letter from Albert Gore, *supra* note 109.

198. S. REP. NO. 309, 103d Cong. 2d Sess. 22–23 (1994).

199. H.R. 5199, 103d Cong., 2d Sess. (1994).

George Brown, Jr. (D-Cal.).[200] Finding that the value of encryption technology to the security and protection of private communications conflicts with the importance of wiretapping to provide for the public safety and national security, the bill would have required the NIST to hold an open rule-making process so that all interested parties could influence the final standard.[201] The bill, which was referred to the House Committee on Science, Space, and Technology, was never reported out of committee.

D. *Informal Accommodation*

All sides—law enforcement, privacy advocates, the computer industry, and individual and business users—have compelling interests in the current debate triggered by Clipper. At the moment, the debate is at an impasse, but the proliferation of encryption products and the increasing demand for strong, exportable cryptography are driving all parties toward compromise. For that reason, discussions between government and privacy advocates, the computer industry, and business are taking place behind the scenes, and a few proposals are in circulation.[202]

One proposed accommodation would entail an encryption scheme including some access for law enforcement agencies, procedural safeguards—preferably administered by a neutral third party and supplemented by legal remedies—and an unclassified algorithm suitable for export. In this way, government would obtain access to encrypted communications when authorized, privacy advocates could rely on meaningful safeguards and remedies, and the computer software and hardware industries would be free to compete abroad. The only drawback to this scheme may be that the current unclassified algorithms are not as complex as the EES, and therefore the cryptographic protections they provide are not as extensive.[203] However, new and more complex algorithms will arise as the need for them becomes more acute.

VI. CONCLUSION

Succinctly stated, Clipper is a commercial failure, although the current policy continues to postpone the day when strong encryption

---

200. Then Chairman, Subcommittee on Technology, Environment, and Aviation of the House Committee on Science, Space, and Technology.

201. 140 CONG. REC. E2118 (daily ed. Oct. 6, 1994) (statement of Rep. Brown).

202. Interview with Dorothy Denning, *supra* note 162.

203. Dorothy E. Denning, Crime and Crypto on the Information Superhighway (forthcoming in J. CRIM. JUST. EDUC.).

prevails both in the United States and abroad. Gradually, the private market is eroding the NSA's monopoly on cryptography technology. However, the government still wields enormous clout as the largest user of encryption technology, through administration of export controls, and by issuing federal standards.

Having given the private sector notice that it will aggressively pursue its interests, the federal government should sit down with business, the software and hardware industries, and privacy advocates and attempt to reach a compromise. This compromise scheme must be viable, voluntary, and marketable here and abroad.[204] It will probably include some form of commercial escrow, proprietary algorithm, and public key. The administration has already indicated its preference for a compromise involving commercial key escrow,[205] and there are in circulation several proposals involving commercial key escrow.[206]

A public key system that includes a strong yet exportable algorithm and a commercial escrow component is such a compromise. The government would continue to review encryption products as it does currently[207] but would make exceptions for certain algorithms with key escrow provisions. At a minimum, DES should be licensed for export in return for government access to commercially escrowed keys.[208] Since DES is already widely available abroad, the government would only be acknowledging the existing state of the encryption technology market. It would still be able to prevent the most powerful cryptographic products from becoming freely available overseas.

The proposed cryptography system is a pragmatic solution that addresses most concerns without favoring one side over the other. By privatizing the function of key escrow, relying on contract liability concepts, and enacting strict penalties for disclosure, the compromise addresses the legal concerns of privacy advocates while allowing law enforcement officials to access encrypted messages when authorized to do so. By avoiding limitation to a particular algorithm and loosening export restrictions for algorithms with escrow, the compromise would give software developers the opportunity to offer sophisticated encryption products here and abroad while safeguarding national security.

---

204. An area that merits further examination is how the United States policy on cryptography will interact with foreign users, other governments, and their legal regimes.

205. Letter from Albert Gore, *supra* note 109.

206. Interview with Dorothy Denning, *supra* note 162.

207. Interview with Ken Mendelson, *supra* note 44.

208. Denning, Mendelson, and Howell each stressed that this would be a minimum requirement for establishment of a workable commercial escrow. Interview with Dorothy Denning, *supra* note 162; Interview with Ken Mendelson, *supra* note 44; Interview with Beryl Howell, *supra* note 190.

Finally, by excepting certain pre-approved escrow algorithms with commercial escrow from the rigid export regime, the compromise would encourage the development of secure encryption products while enabling the NSA to keep abreast of cryptography expertise.

EPILOGUE

On August 17, 1995, the NIST announced a proposal to allow export of strong encryption software products that employ up to 64-bit keys as long as the products include a third-party escrow scheme.[209] The agency invited industry representatives to discuss escrow issues in workshops scheduled for September 6 and 7.[210]

On September 21, 1995, in a speech to the International Cryptography Institute, FBI Director Louis French asserted that encryption is a "public safety issue" and cited several cases ranging from a plan to assassinate the Pope to child pornography on the Internet where encryption has hampered the efforts of law enforcement authorities. He declared that unless Congress decides to revamp Fourth Amendment law, his agency will continue to hold out for court-authorized access to encrypted records and communications.[211]

On November 7, 1995, a computer industry coalition of 37 companies broke off negotiations with the government, indicating that the administration was too inflexible to reach a compromise. This group, which includes America Online, Apple Computer, AT&T, Eastman Kodak, Microsoft, and Novell, pledged to present its own proposal to the White House and to Congress in the next six months.[212]

---

209. *Commerce's NIST Announces Process for Dialogue on Key Escrow Issues*, NIST Release No. 95-24, Aug. 17, 1995.

210. Memorandum for Registrants for the Sept. 6–7, 1995 Key Escrow Issues Meeting, NIST, Aug. 25, 1995.

211. Louis J. Freeh, Speech Before the International Cryptography Institute, Washington, D.C., Sept. 21, 1995.

212. John Markoff, *Industry Group Rebuffs U.S. on Encryption*, N.Y. TIMES, Nov. 8, 1995, at D5.