Fordham International Law Journal

Volume 19, *Issue* 1 1995 *Article* 7

Personal Data Security: Divergent Standards in the European Union and the United States

Amy Fleischmann*

*

Personal Data Security: Divergent Standards in the European Union and the United States

Amy Fleischmann

Abstract

This Note argues that the U.S. Government should discontinue all attempts to establish EES as the de facto encryption standard in the United States because the economic disadvantages associated with widespread implementation of EES outweigh the advantages this advanced data security system provides. Part I discusses the EU's legislative efforts to ensure personal data security and analyzes the evolution of encryption technology in the United States. Part II examines the methods employed by the U.S. Government to establish EES as the de facto U.S. encryption standard. Part III argues that the U.S. Government should terminate its effort to establish EES as the de facto U.S. encryption standard and institute an alternative standard that ensures continued U.S. participation in the international marketplace.

NOTE

PERSONAL DATA SECURITY: DIVERGENT STANDARDS IN THE EUROPEAN UNION AND THE UNITED STATES

*Amy Fleischmann**

INTRODUCTION

The amount of personal data[1] processed[2] on computer networks is approaching staggering proportions.[3] This growing dependence on information systems raises personal data security[4] concerns among computer users.[5] Responding to these con-

* J.D. Candidate, 1996, Fordham University.

1. Common Position (EC) No. 1/95, O.J. L 93/01 (1995) [hereinafter 1995 Directive No. 1/95]. The Directive form of the Common Position, which was adopted July 24, 1995, remains unpublished. *Council Definitively Adopts Directive on Protection of Personal Data*, European Commission Press Release, July 24, 1995 [hereinafter *Council Definitively Adopts Directive on Protection of Personal Data*] (on file with *Fordham International Law Journal*). The 1995 Directive defines "personal data" as:

> [A]ny information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

1995 Directive No. 1/95, *supra*, art 2(a), O.J. L 93/01, at 7 (1995).

2. 1995 Directive No. 1/95, *supra* note 1, art. 2(b), O.J. L 93/01, at 7 (1995). The 1995 Directive defines "processing of personal data" as:

> [A]ny operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

Id.

3. *See* Lance J. Hoffman et al., *Cryptography Policy*, COMMUNICATIONS OF THE ACM, Sept. 1994, at 109, 110 [hereinafter *Cryptography Policy*] (describing exponential increase in processed data); JOEL KURTZMAN, THE DEATH OF MONEY 30-31 (1993) (stating that Solomon Brothers annually trades approximately US$2 trillion worth of securities and runs equivalent of total U.S. bank holdings through company's computer networks); G.B.F. Niblett, *Computers and Privacy*, *in* PRIVACY, COMPUTERS AND YOU 17, 17 (B.C. Rowe ed., 1972) (suggesting that reasons for growth of technology include desire for efficiency and urge to achieve maximum production with minimum effort).

4. LANCE J. HOFFMAN, MODERN METHODS FOR COMPUTER SECURITY AND PRIVACY 2 (1977). "Data security is the protection of data against accidental or intentional destruction, disclosure, or modification." *Id.*

5. *See* Hilary E. Pearson, *Data Protection in Europe*, COMPUTER LAWYER, Aug. 1991, at

cerns, the European Union[6] ("EU") and the U.S. Government are implementing data security measures within their respective jurisdictions.[7]

The European Union relies on legislation to foster personal data security on computer networks.[8] On July 24, 1995, the European Union adopted the European Community's[9] ("EC")

24, 24 (stating that individuals in Europe and United States are concerned about data privacy because of increased use of computerized databases); Paige Amidon, *Widening Privacy Concerns*, ONLINE, July 1992, at 64, 64 (concluding that almost 80% of U.S. citizens are concerned about computer-related privacy issues).

6. Treaty Establishing the European Community, Feb. 7, 1992, [1992] 1 C.M.L.R. 573 [hereinafter EC Treaty], *incorporating changes made by* Treaty on the European Union, Feb. 7, 1992, O.J. C 224/1 (1992), [1992] 1 C.M.L.R. 719, 31 I.L.M. 247 [hereinafter TEU]. The TEU, *supra*, amended the Treaty Establishing the European Economic Community, Mar. 25, 1957, 298 U.N.T.S. 11, 1973 Gr. Brit. T.S. No. 1 (Cmd. 5179-II) [hereinafter EEC Treaty], *as amended by* Single European Act, O.J. L 169/1 (1987), [1987] 2 C.M.L.R. 741 [hereinafter SEA], *in* TREATIES ESTABLISHING THE EUROPEAN COMMUNITIES (EC Off'l Pub. Off. 1987). Until 1995, the twelve European Union ("EU") Member States were Belgium, Denmark, France, Germany, Greece, Spain, Ireland, Italy, Luxembourg, the Netherlands, Portugal, and the United Kingdom. TEU, *supra*, pmbl. On January 1, 1995, Austria, Finland, and Sweden became EU Member States. *Sweden, Finland and Austria Join European Union*, S.F. CHRON., Jan. 2, 1995, at A8. GEORGE A. BERMANN ET AL., CASES AND MATERIALS ON EUROPEAN COMMUNITY LAW 2-18 (1993). The TEU, which became effective on January 1, 1993, superceded EC treaties and established the European Union. *Id.* at 16. An economic crisis in the mid-1970's and problems within the European Community in the 1980's, including political differences regarding reform of common agricultural policy and EC financial problems, emphasized the importance of creating a unified Europe. *Id.* at 13-14. In response, community leaders developed the TEU. *Id.* at 13. TEU provisions are divided into two categories: economic and monetary union and political union. *Id.* at 16. Economic and monetary coordination is scheduled to occur in several stages. *Id.* at 16-17. The first stage involves creation of the European Monetary Institute ("EMI") to coordinate the activities of the central banks. *Id.* at 17. The second stage requires creation of independent central banks in Member States that do not currently possess them, elimination of excessive deficits, and the formation of a plan for complete monetary union. *Id.* The third stage entails creating a European System of Central Banks. *Id.* By 1999, a single currency is scheduled to replace the national currencies. *Id.* The TEU is considered a crucial step towards European political integration, as it will expand the Community sphere in a variety of areas including immigration, justice, and health. *Id.* at 17-18.

7. *See* 1995 Directive No. 1/95, *supra* note 1, pmbl., O.J. L 93/01, at 1 (1995) (outlining comprehensive plan to ensure personal data protection and free movement of personal data within European Union). *See also Statement of the Press Secretary*, The White House Office of the Press Secretary, Feb. 4, 1994 (on file with *Fordham International Law Journal*) [hereinafter *Statement of the Press Secretary*] (describing Escrowed Encryption Standard as encryption standard that provides advanced computer data security).

8. *See* 1995 Directive No. 1/95, *supra* note 1, art. 17(1), (2), O.J. L 93/01, at 12 (1995) (mandating that EU Member States implement technical measures to protect personal data security).

9. BERMANN, *supra* note 6, at 2. The European Community ("EC") preceded the EU. *Id.* The EC consisted of several Communities, including: the European Coal and

Amended Proposal for a Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data ("1995 Directive").[10] Article 17 of the 1995 Directive[11] ("Article 17") addresses personal data security and requires data controllers[12] to implement state of the art[13] security measures when processing personal data.[14]

Steel Community, the European Economic Community, the European Defense Community, and the European Political Community. *Id.* at 2-6. The EC was initially created as a means to integrate the European economic market and increase the European standard of living. *Id.* at 2. During its thirty-five year tenure, however, the EC also fostered political, social, and cultural integration. *Id.*; *see supra* note 6 (presenting twelve EC Member States).

10. *See* 1995 Directive No. 1/95, *supra* note 1, arts. 6-18, O.J. L 93/01, at 8-13 (1995) (outlining data controller's affirmative duties and prohibitions regarding personal data processing and discussing data transfers to third party countries). The EU's Council of Ministers adopted an earlier draft of the 1995 Directive on February 20, 1995. *EU Council Approves Standards for Protections of Data Privacy*, BNA INT'L BUS. & FIN. DAILY, Feb. 24, 1995, *available in* LEXIS, BNA Library, Int'l Bus. & Fin. Daily File [hereinafter *EU Council Approves Standards for Protections of Data Privacy*]. The Council of Ministers then adopted a modified version of this early draft on July 24, 1995. *Council Definitively Adopts Directive on Protection of Personal Data*, *supra* note 1.

11. 1995 Directive No. 1/95, *supra* note 1, art. 17(1), (2), O.J. L 93/01, at 12 (1995). Article 17 provides, in relevant part:

> 1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss and against unauthorized alteration, disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Having regard to the state of the art and the costs of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.
> 2. The Member States shall provide that the controller must, where the processing is carried out on his behalf, choose a processor who provides sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out and must ensure compliance with those measures.

Id.

12. *Id.* art. 2(d), O.J. L 93/01, at 7 (1995). The 1995 Directive defines "controller" as:

> [A]ny natural or legal person, public authority, agency or other body who processes personal data or causes it to be processed and who decides what is the purpose and objective of the processing, which personal data are to be processed, which operations are to be performed upon them and which third parties are to have access to them.

Id.

13. Commission of the European Communities, Amended Proposal for a Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, Explanatory Memorandum, COM (92) 422 Final (Oct. 1992) [hereinafter 1992 Proposal Explanatory Memorandum] (defining "state of the art" as appropriate technical measures to protect data).

The U.S. Government, in contrast, responds to personal data security concerns with the development of encryption[15] technology.[16] The Escrowed Encryption Standard[17] ("EES") represents the U.S. Government's current attempt to alleviate data security concerns in the United States.[18] EES features key escrow technology,[19] which guarantees advanced data security and allows U.S. Government agencies to intercept data communications for law enforcement purposes.[20] The U.S. Government seeks to establish EES as the *de facto* encryption standard in the United States.[21]

This Note argues that the U.S. Government should discontinue all attempts to establish EES as the *de facto* encryption standard in the United States because the economic disadvantages

---

14. 1995 Directive No. 1/95, *supra* note 1, art. 17(1), (2), O.J. L 93/01, at 12 (1995).

15. *See* U.S. CONGRESS, OFFICE OF TECHNOLOGY ASSESSMENT, INFORMATION SECURITY AND PRIVACY IN NETWORK ENVIRONMENTS 113 (1994) [hereinafter OTA] (defining encryption as method by which contents of message are concealed).

16. *See* Ira S. Rubenstein, *Export Controls on Encryption Software, in* COPING WITH U.S. EXPORT CONTROLS 177, 182 (PLI COM. LAW AND PRACTICE COURSE HANDBOOK SERIES No. A4-4458, 1994) (discussing how computers equipped with encryption technology that allow users to transform computerized data into form which is incomprehensible to all unauthorized users).

17. Jaleen Nelson, *Sledge Hammers and Scalpels: The FBI Digital Wiretap Bill and Its Effect on Free Flow of Information and Privacy*, 41 UCLA L. REV. 1139, 1140 (1994). The Escrowed Encryption Standard ("EES") is comprised of two components, the Clipper Chip and the Capstone Chip. *Id.* The Capstone Chip encrypts high-speed data transmissions, whereas the Clipper Chip encrypts low-speed data and voice conversations. *Id.*

18. *Statement of the Press Secretary*, *supra* note 7.

19. OTA, *supra* note 15, at 173. Chip-specific keys required to access encrypted communications are held in escrow, allowing a party to retrieve a key from the escrow agent and decrypt the encrypted information. *Id.* The National Institute of Technology estimated that establishing key escrow technology in EES cost US$14 million, and annual operating costs for the agents holding the keys in escrow approaches US$16 million. *Id.*

20. *Statement of the Press Secretary*, *supra* note 7. Key escrow technology permits law enforcement and other agencies to conduct legally authorized wiretaps. *Id.* Consequently, key escrow technology will allow agencies to intercept incriminating communications processed over telephones and modems by potential terrorists, drug dealers, and other criminals. *Id.*

21. *See Cryptography Policy*, *supra* note 3, at 109 (explaining how U.S. Government employs export controls to eliminate competing devices from U.S. encryption market); James Fallows, *Open Secrets: Why the So-Called Clipper Chip - Vilified As A Threat to the Privacy of Electronic Communications - Is Not Worth Losing Sleep Over*, ATLANTIC MONTHLY, June 1994, at 50 (stating that U.S. Government's purchasing power is so great that it possesses ability to influence types of technology available on U.S. encryption market).

associated with widespread implementation of EES outweigh the advantages this advanced data security system provides. Part I discusses the EU's legislative efforts to ensure personal data security and analyzes the evolution of encryption technology in the United States. Part II examines the methods employed by the U.S. Government to establish EES as the *de facto* U.S. encryption standard. Part II also presents the advantages and disadvantages associated with the widespread implementation of EES. Additionally, Part II discusses recent developments in the U.S. Government's quest to ensure data security in the United States. Part III argues that the U.S. Government should terminate its effort to establish EES as the *de facto* U.S. encryption standard and institute an alternative standard that ensures continued U.S. participation in the international marketplace. This Note concludes that the successful establishment of EES as the *de facto* U.S. encryption standard will prevent the United States from actively participating in the international marketplace.

I. *EU AND U.S. DATA SECURITY STANDARDS*

The European Union and the United States approach the issue of personal data security differently.[22] The European Union develops legislation to ensure personal data security.[23] These legislative efforts culminated in a state of the art standard for the protection of personal data.[24] The U.S. Government does not rely upon legislation to protect data processed over computer networks.[25] Instead, to achieve this goal, the U.S. Government advocates the development of encryption technology.[26] The most recently released U.S. encryption standard features key escrow technology.[27]

---

22. *See supra* notes 8-14 and accompanying text (discussing EU legislative efforts to ensure security of personal data processed on computer networks); *supra* notes 15-20 and accompanying text (discussing U.S. Government development of encryption technology).

23. *See* Herald D.J. Jongen & Gerrit A. Vriezen, *The Council of Europe and the European Community, in* DATA TRANSMISSION AND PRIVACY 140-155 (Dennis Campbell & Joy Fisher eds., 1994) (examining various EU legislative efforts regarding personal data protection).

24. 1995 Directive No. 1/95, *supra* note 1, art. 17(1), O.J. L 93/01, at 12 (1995).

25. *Statement of the Press Secretary, supra* note 7.

26. *See supra* notes 18-20 and accompanying text (discussing most recently released encryption technology in United States).

27. *Statement of the Press Secretary, supra* note 7.

A. *Development of the EU's Personal Data Security Standard*

In the late 1960's, governmental bodies within the European Union[28] determined that the rights and obligations associated with computerized personal data required governmental regulation.[29] In the 1970's, several EU Member States independently adopted national data protection legislation.[30] Each of the national initiatives included a data security provision, however, these provisions created incompatible data security standards that obstructed the free transfer of personal data among EU Member States.[31] In the early 1980's, two EU entities[32] drafted international documents in an attempt to harmonize national data protection laws, including national data security provisions.[33] These international efforts, however, failed to create uniformity among existing national laws.[34] Article 17, the European Union's most recent legislation concerning data security, attempts to harmonize Member States' national data security provisions.[35]

---

28. *See* A.C.M. NUTGER, TRANSBORDER FLOW OF PERSONAL DATA WITHIN THE EC 20 (Computer/Law Series No. 6, 1990) (naming Organization for Economic Cooperation and Development ("OECD") and Council of Europe ("COE") as two governmental bodies concerned with personal data protection).

29. Jongen & Vriezen, *supra* note 23, at 140.

30. *Id.* Between 1974 and 1979, Austria, Denmark, France, Germany, Luxembourg, Norway, and Sweden enacted general data protection laws. *Id.*

31. *See* Organization for Economic Co-Operation and Development: Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980 O.E.C.D. Doc C (80) 58 Final at 17 (Oct. 1980), 20 I.L.M. 422, 430 [hereinafter OECD Guidelines] (explaining that general differences among national legislations included scope of legislation, implementation of principles outlined in legislation, and method of enforcement); Pearson, *supra*, note 5, at 24 (stating that incongruous legislation prevented data flows between European countries and, consequently, had significant ramifications on public and commercial institutions in Europe).

32. *See* NUTGER, *supra* note 28, at 20 (discussing attempts by the Organization for Economic Co-Operation and Development and the Council of Europe to harmonize national data protection laws).

33. OECD Guidelines, *supra* note 31, 1980 O.E.C.D. Doc C (80) 58 Final, 20 I.L.M. 422; Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, April 21,1981, Europ. T.S. No. 108, 20 I.L.M. 317 (1981) [hereinafter COE Convention].

34. *See Council Adopts Common Position on Protection of Personal Data Directive*, European Commission Press Release, Feb. 21, 1995 [hereinafter *Council Adopts Common Position on Protection of Personal Data Directive*] (on file with *Fordham International Law Journal*) (stating that international documents did not adequately rectify incompatibilities among national legislation).

35. 1995 Directive No. 1/95, *supra* note 1, art. 17(1), (2), O.J. L 93/01, at 12 (1995).

1. National Data Security Provisions

In 1968, the Council of Europe's[36] ("COE") Parliamentary Assembly[37] asked the Council of Ministers[38] ("Ministers") to determine whether any existing international agreement addressed personal privacy[39] in the context of data processing.[40] The Ministers found that earlier agreements did discuss privacy issues, but did not consider personal privacy in the context of data processing.[41] This finding led to the adoption of Resolutions (73)22[42] and (74)29.[43] These Resolutions recommended that EU Member States implement data protection measures.[44]

---

36. D. LASOK & J.W. BRIDGE, INTRODUCTION TO THE LAW AND INSTITUTIONS OF THE EUROPEAN COMMUNITIES 9 (3d ed. 1982). The COE consists of a Consultive Assembly comprised of parliamentary delegates from each of the COE Member States, a Committee of Ministers, and a Secretariat. *Id.*; *see* Pearson, *supra* note 5, at 29 n.1 (explaining that COE is intergovernmental body within EU created in 1948 to promote unification among European nations); BERMANN, *supra* note 6, at 4 (stating that COE is comprised of twenty-six Member States).

37. *See* LASOK & BRIDGE, *supra* note 36, at 9 (explaining that Parliamentary Assembly is component of COE and consists of parliamentary delegates of Member States).

38. *Id.* The Parliamentary Assembly and the Council of Ministers are both components of the COE. *Id.* CLIVE ARCHER & FIONA BUTLER, THE EUROPEAN COMMUNITY STRUCTURE AND PROCESS 29 (1992). The Council of Ministers, formally titled the Council of the European Communities, is the EU's legislative, decision-making body. *Id.* The Council of Ministers is the only EU institution whose members directly represent national governments. RICHARD MAYNE, THE INSTITUTIONS OF THE EUROPEAN COMMUNITY 17 (1968).

39. HOFFMAN, *supra* note 4, at 2. "Privacy is a concept which applies to an individual. It is the right of an individual to decide what information (s)he wishes to share with others and also what information (s)he is willing to accept from others." *Id.*

40. *See* Jongen & Vriezen, *supra* note 23, at 140 (explaining that Parliamentary Assembly was primarily concerned with whether European Human Rights Convention (EHRC) provided for personal privacy protection by means of modern science and technology).

41. *See* NUTGER, *supra* note 28, at 20 (1990) (noting that European Convention on Human Rights, adopted by COE on November 4, 1950, and International Covenant on Civil and Political Rights, adopted by United Nations on December 19, 1966, were two international agreements that considered individual privacy rights, but not with regard to data processing); OECD Guidelines, *supra* note 31, 1980 O.E.C.D. Doc C (80) 58 Final at 18, 20 I.L.M. 431 (stating that Committee's inquiry revealed that existing law provided inadequate protection of privacy rights with regard to automated data banks).

42. Resolution on the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Private Sector, Res. (73)22, Council of Europe, Comm. of Ministers, 224th mtg. (1973) [hereinafter Resolution (73)22].

43. Resolution on the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Public Sector, Res. (74)29, Council of Europe, Comm. of Ministers, 224th mtg. (1974) [hereinafter Resolution (74)29].

44. *See* Resolution (73)22, *supra* note 42 (establishing principles of data protection for private sector); Resolution (74)29, *supra* note 43 (establishing principles of data

Following the adoption of Resolutions (73)22 and (74)29, several EU Member States enacted data protection legislation.[45] All of the national data protection laws included provisions addressing personal data security.[46] These national security provisions, however, mandated disparate data security requirements.[47]

These provisions' conflicting requirements impeded the ability of computer users in the European Union to transfer computerized information across national borders.[48] EU Member States that maintained stringent security laws often prohibited data transfers to Member States possessing inadequate[49]

---

protection for the public sector). The Ministers adopted the private sector Resolution on September 26, 1973, and the public sector Resolution on September 20, 1974. SIMON CHALTON & SHELAGH GASKILL, DATA PROTECTION LAW 1147 (1988). *See* OECD Guidelines, *supra* note 31, 1980 O.E.C.D. Doc C (80) 58 Final at 19, 20 I.L.M. 431 (discussing Resolutions (73)22 and (74)29's recommendation that COE Member States implement measures regarding obtaining of data, quality of data, rights of individuals to be informed about data, and data processing activities); Jongen & Vriezen, *supra* note 23, at 140 (explaining that Resolutions (73)22 and (74)29 established minimum standards of data protection).

45. *See* Draft Explanatory Report on the Draft Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Council of Europe, CJ-CD (80) 1, Addendum (Jan. 1980), *reprinted in* 19 I.L.M. 299, 300 [hereinafter COE Convention Explanatory Report] (noting that COE Member States possessed discretion regarding method by which they implement Resolutions, and that most Member States elected to enact legislation); Jongen & Vriezen, *supra* note 23, at 140 (listing Austria, Denmark, France, Germany, Luxembourg, Norway, and Sweden as countries that possess data protection laws, and noting that Portugal and Spain include data protection as fundamental rights in their Constitutions).

46. *E.g.*, NUTGER, *supra* note 28, at 64. Section 6 of the German personal data processing act, the Bundesdatenschutzgesetz ("BDSG"), provides: "There is an obligation on all persons involved in processing data within the scope of the BDSG to implement technical and organizational measures to ensure that the act is complied with." *Id.* Section 29 of the French data processing act, the Loi relative à l'informatique, aux fichiers et aux libertés ("LIFL"), states: "Any person processing personal data or ordering such processing thereby shall undertake, vis-à-vis the persons concerned to see that all necessary precautions are taken to protect the data and in particular to prevent these from being distorted, damaged or disclosed to unauthorized third parties." *Id.* at 95.

47. *Id.* at 64.

> The German legislator has chosen not to tie the measures to be taken to a particular state of technology. Data security is seen as a process that is [amenable] to improvement with the result that the latest state-of-the-art technology can be viewed as the point of departure.

Id. By contrast, the LIFL does not make any reference to the state of technology to be implemented. *Id.* at 95.

48. *Council Adopts Common Position on Protection of Personal Data Directive*, *supra* note 34.

49. *See Modification of the Commission's Proposal on Data Protection*, INFORMATION, Oct.

data security requirements.[50] The French government, for instance, prohibited the Italian car maker, Fiat, from transferring employee data from the company's French subsidiary to its headquarters in Italy.[51] The French Government prohibited the transfer because it considered Italian data security requirements inadequate.[52]

2. International Initiatives

While preparing Resolutions 73(22) and 74(29), the Ministers advised the COE that the national data protection laws required reinforcement from a binding, international data protection agreement.[53] In 1976, pursuant to the Ministers' recommendation, the COE instructed the Ministers to prepare a Convention[54] ("COE Convention") on personal data protection.[55] In 1980, the Ministers completed a draft of the Convention,[56] and, in 1981, the final version of the Convention opened

---

23, 1992 *available in* LEXIS, News Library, ARCNWS file (explaining that some EU Member States do not possess data protection legislation); DATA TRANSMISSION AND PRIVACY viii (Dennis Campbell & Joy Fisher eds., 1994). Belgium did not adopt data protection legislation until 1992. *Id.*

50. *Council Adopts Common Position on Protection of Personal Data Directive*, *supra* note 34; *see* Emma Tucker, *EU States Harmonise on Data Protection*, FIN. TIMES, Feb. 23, 1995, at 1, 14 (stating that varying data protection laws limit cross-border provision of financial products, including mortgages and life insurance policies); COE Convention Explanatory Report, *supra* note 45, at 302. Even if two Member States possess similar data protection laws, problems may arise regarding which nation has jurisdiction and which national law applies. *Id.*

51. *Banks Oppose EC Plans to Protect Personal Privacy*, REUTERS, Mar. 31, 1993, *available in* LEXIS, NEXIS Library, News File.

52. *Id.* The French and Italian governments reached a compromise after Fiat guaranteed that it would protect the transferred information. *Id.*

53. Alexander D. Roth, *Introduction* to Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, 19 I.L.M. 282 (1980) [hereinafter COE Introductory Note]. The Ministers suggested that the COE create a binding international agreement following the enactment of the national laws. *Id.*; *see* BERMANN, *supra* note 6, at 3 (stating that although COE does not possess legislative power, it produces international documents on variety of subjects adopted by COE Member States).

54. CHALTON & GASKILL, *supra* note 44, at 1147. The COE Convention established basic data protection principles. *Id.* The COE Convention is binding upon its signatories, who are obligated to incorporate the COE Convention's principles into their national laws. *Id.*

55. COE Convention Explanatory Report, *supra* note 45, at 302. The Ministers developed the Convention in collaboration with the OECD. *Id.*

56. CHALTON & GASKILL, *supra* note 44, at 1147. The Ministers considered two models for the COE Convention. *Id.*

The first was based on reciprocity: data processing in Country A which related

for signature.[57] The COE Convention's data security provision required the implementation of security measures incorporating state of the art technology.[58]

In 1978, the Organization for Economic Cooperation and Development[59] ("OECD") also attempted to eliminate conflicts among the national data protection laws.[60] The OECD organized a Group of Experts on Transborder Data Barriers and Privacy Protection[61] ("Transborder Experts") to formulate a set of international data protection guidelines ("OECD Guidelines").[62]

---

to individuals living in Country B would be required to be carried out according to the laws of Country A and vice versa. The second possibility was the promulgation of data protection principles common to all party states.

Id. The Ministers chose to implement the second option. *Id.*

57. Jongen & Vriezen, *supra* note 23, at 140. The Committee of Ministers approved the COE Convention on December 17, 1980. *Id.* The Convention opened for signature on January 28, 1981. *Id.* COE Convention, *supra* note 33, Europ. T.S. No. 108, at 11, 19 I.L.M. at 299. Austria, Denmark, France, Federal Republic of Germany, Ireland, Luxembourg, Norway, Spain, Sweden, and the United Kingdom have ratified the Convention. *Id.* Belgium, Cyprus, Greece, Iceland, Italy, Netherlands, Portugal, and Turkey have signed but not ratified the Convention. *Id.* Finland, Liechtenstein, Malta, San Marino, and Switzerland have not signed the Convention. *Id.*

58. COE Convention, *supra* note 33, Europ. T.S. No. 108, at 4, 20 I.L.M. at 317. Article 7 provides that: "[A]ppropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination." *Id.* The Convention requires that data security measures be based on the current state of the art in the field of data security methods and techniques. COE Convention Explanatory Report, *supra* note 45, at 310.

59. BERMANN, *supra* note 6, at 4. The OECD was originally named the Organization for European Economic Cooperation ("OEEC"). *Id.* In 1948, the Marshall Plan's recipient nations created the OEEC in order to facilitate the administration of the Marshall Plan. *Id.* In 1960, Canada and the United States became members of the OEEC, at which time it was renamed the OECD. *Id.* The OECD is primarily concerned with instituting policies regarding the European economy. *Id.*

60. OECD Guidelines, *supra* note 31, at 15, 20 I.L.M. at 422.

61. *Id.* Justice Michael Kirby, Chairman of the Australian Law Reform Commission, chaired the Group of Experts on Transborder Data Barriers and Privacy Protection ("Expert Group"). *Id.* at 5, 20 I.L.M. at 426. A Symposium, held in Vienna in 1977, supplied the Expert Group with the information necessary to formulate a set of data protection guidelines. *Id.* at 19, 20 I.L.M. at 444. The Symposium provided opinions from a variety of sectors, including government, industry, and users of international communication networks. *Id.*

62. *Id.* at 15, 20 I.L.M. at 422. The OECD Guidelines consisted of eight principles, all intending to facilitate the protection of data processing. *Id.* at 15, 20 I.L.M. at 430. These principles address: limitations on collection, data quality, purpose specification, use limitation, openness, individual participation, accountability, and security safeguards. *Id.* at 10-11, 20 I.L.M. at 426; *see* Hon. Justice Michael Kirby, *Legal Aspects of Transborder Data Flows*, 11 COMPUTER/L.J. 233, 233 (1991) (noting OECD Guidelines are voluntary because OECD does not possess enforcement power).

On September 23, 1980, OECD Member States[63] adopted the OECD Guidelines, which became the European Union's foundation for uniformity in the protection of personal data.[64] The OECD Guidelines included a provision devoted to personal data security.[65] This provision recommended that computer users implement "reasonable safeguards" to protect personal data.[66]

The security provisions in both the COE Convention and the OECD Guidelines failed to harmonize national personal data security requirements.[67] These international provisions did not replace existing national data security requirements.[68] Rather, Member States altered national security provisions to include the general data security objectives outlined in the COE Convention and the OECD Guidelines.[69] Members States independently determined which security measures satisfied the COE and the OECD objectives.[70] Discrepancies among national data security laws persisted because Member States did not require the implementation of identical security measures to

---

63. OECD Guidelines, *supra* note 31, at 2, 20 I.L.M. 422. OECD Member States include: Australia, Austria, Belgium, Canada, Denmark, Finland, France, the Federal Republic of Germany, Greece, Iceland, Ireland, Italy, Japan, Luxembourg, the Netherlands, New Zealand, Norway, Portugal, Spain, Sweden, Switzerland, Turkey, the United Kingdom, and the United States. *Id.*

64. Kirby, *supra* note 62, at 233.

65. OECD Guidelines, *supra* note 31, at 10, 20 I.L.M. at 425. The Security Safeguards Principle reads: "Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data." *Id.*

66. *Id.* at 31, 20 I.L.M. at 444. The OECD Guideline's Explanatory Memorandum defines "reasonable safeguards" as:

> Such safeguards include physical measures (locked doors and identification cards, for instance), organisational measures (such as authority levels with regard to access to data) and, particularly in computer systems, informational measures (such as enciphering and threat monitoring of unusual activities and responses to them).

Id.

67. Jongen & Vriezen, *supra* note 23, at 150; *see* Amelia Torres, *Belgium Speeds Up Work on Plans to Protect Privacy*, REUTERS, Sept. 20, 1993, *available in* LEXIS, News Library, ARCNWS file (reporting that COE and European Commission officials believe that COE Convention does not allow for free movement of data in single market, nor does it possess legal provisions to solve conflicts).

68. COE Introductory Note, *supra* note 53, 19 I.L.M. at 282 (1980).

69. CHALTON & GASKILL, *supra* note 44, at 1147.

70. Jongen & Vriezen, *supra* note 23, at 141. The manner in which the signatories to the COE Convention implement the basic principles of the COE Convention is left to their discretion. *Id. See also* CHALTON & GASKILL, *supra* note 44, at 1147 (examining recommended OECD Guidelines).

achieve the general objectives outlined in the COE Convention and the OECD Guidelines.[71]

3. Article 17

In 1990, the Commission of the European Communities[72] ("Commission") responded to persisting disparities[73] among national data protection laws, such as incompatible data security requirements, by issuing a comprehensive data protection proposal ("1990 Proposal").[74] The 1990 Proposal, however, encountered severe criticism from various sectors within the European Union.[75] Opposition to the 1990 Proposal prompted drafters to

---

71. *See supra* note 46 and accompanying text (discussing various methods adopted by EU Member States to achieve general objectives outlined in COE Convention and OECD Guidelines).

72. ARCHER & BUTLER, *supra* note 38, at 24. Seventeen Commissioners serve on the Commission. *Id.* The Commissioners do not advocate their national interest. *Id.* The Commission proposes legislation, while the Council of Ministers decides whether to implement the Commission's proposed legislation. *Id.* at 29. The Commission was kept apprised of the COE's activities while the COE prepared the COE Convention. *Id.* The Commission supervised the harmonization of national legislation regarding the data security problems of individual residents of the Member States. *Id.*

73. *See* Jongen & Vriezen, *supra* note 23, at 150 (explaining that EU legislation is justified only when national laws are not harmonized); Commission of the European Communities: *Communication from the Commission to the European Parliament Pursuant to the Second Subparagraph of Article 189 B (2) of the EC Treaty*, SEC (95) 303 Final at 1 (Feb. 1995) [hereinafter *Communication from the Commission to the European Parliament*] (concluding that harmonization of data security laws is necessary to address disparities among national laws, and to satisfy data-exchange requirements imposed by completion of internal market).

74. Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data, COM (90) 314 Final (Sept. 1990) [hereinafter 1990 Proposal]; Jongen & Vriezen, *supra* note 23, at 150. In 1982, the COE adopted a resolution recommending that the European Community formulate a directive regarding personal data in the anticipation of the COE Convention's inability to foster uniformity among national data protection legislation. *Id.* The 1990 Proposal is the product of this recommendation. *Id.*; *see EU Council Approves Standards for the Protections of Data Privacy*, *supra* note 10 (reporting that 1990 Proposal intended to provide regulatory framework enabling free movement of personal data across EU borders).

75. Louella Miles, *Feeling the Draft*, MARKETING, May 30, 1991, at 16. Newspapers criticized the 1990 Proposal for creating severe restrictions on indirect and classified advertising. *Id.* Computer manufactures criticized the 1990 Proposal for encouraging manual manipulation of data. *Id.* The British Bankers' Association criticized the 1990 Proposal, stating that it could undermine the world's cash flow. *Id.*; *see* Andrew Hill, *Brussels Acts to Dispel Fears Over Data Processing*, FIN. TIMES, Oct. 24-25, 1992, at A2 (explaining that human rights organizations raised objections to 1990 Proposal, claiming that directive would provide European governments with *carte blanche* regarding personal data); *Banks Oppose EC Plans to Protect Personal Privacy*, *supra* note 51 (stating that EC Banking Federation criticized 1990 Proposal as poorly designed for responsible

amend[76] the original version and create a more lenient and less restrictive directive.[77] The drafters' efforts ultimately resulted in the 1995 Directive.[78]

Article 17 bestows upon the data controller responsibility for ensuring the security of processed personal data.[79] Article 17 mandates that data controllers accomplish this task by implementing security measures that incorporate state of the art technology.[80] Article 17, however, neglects to specify those technologies that satisfy this state of the art standard.[81] Each EU Member State must independently determine which security measures satisfy Article 17's state of the art standard.[82] All EU Member States, however, must obey the criteria outlined in Article 17.[83] Because all EU Member States require data controllers to obey Article 17's state of the art standard, incompatible data security requirements will be eliminated, thereby facilitating data flow across national borders.[84]

---

lending, efficiency of payment systems, and combating financial fraud); Jongen & Vriezen, *supra* note 23, at 151 (characterizing 1990 Proposal as extreme and bureaucratic; favoring protection of privacy at expense of public policy objectives, including freedom of information).

76. *Communication from the Commission to the European Parliament*, *supra* note 73. Two of the most significant amendments are the exclusion of the distinction between data protection rules in the public and private sector, and the procedures regarding supervisory authority. *Id.*; *see* 1995 Directive No. 1/95, *supra* note 1, O.J. L 93/01 (1995) (presenting 1995 Directive).

77. 1995 Directive No. 1/95, *supra* note 1, O.J. L 93/01 (1995).

78. *Council Adopts Common Position on Protection of Personal Data Directive*, *supra* note 34. The 1995 Directive is intended to act as a regulatory measure that will guarantee the free movement of personal data. *Id.*

79. 1995 Directive No. 1/95, *supra* note 1, art. 17(1), (2), O.J. L 93/01, at 12 (1995). The responsibility for ensuring security of processed personal data also applies to other persons who participate in personal data processing. *Id.*

80. *Id.*; *see supra* note 13 (discussing state of art).

81. 1995 Directive No. 1/95, *supra* note 1, art. 17, O.J. L 93/01, at 12 (1995).

82. *EU/Internal Market: Council Agreement on Data Protection Directive Confirmed (With Abstention by United Kingdom), Even Though the Common Position Must Be Verified in Swedish and Finnish*, EUROPE, Feb. 10, 1995, at 6 [hereinafter *EU/Internal Market*]; 1995 Directive No. 1/95, *supra* note 1, art. 17, O.J. L 93/01, at 12 (1995). "Having regard to the state of the art and the costs of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected." *Id.*

83. 1995 Directive No. 1/95, *supra* note 1, art. 17, O.J. L 93/01, at 12 (1995); *see EU/Internal Market*, *supra* note 82, at 6 (stating that EU Member States must transpose criteria outlined in Article 17 into national data protection laws within three years following adoption of 1995 Directive).

84. *See* Jongen & Vriezen, *supra* note 23, at 139 (noting that EU data security law

B. *U.S. Encryption Technology*

The U.S. Government seeks to ensure personal data security through the development of encryption technology.[85] In 1977, the U.S. Government endorsed the Data Encryption Standard[86] ("DES") as a government-sponsored encryption standard.[87] Shortly thereafter, scientists developed Rivest-Shamir-Adelman[88] ("RSA"), an alternative encryption device to DES.[89] Although DES and RSA enjoy international popularity among members of the private sector,[90] the U.S. Government suspects that widespread availability of DES and RSA endangers national security.[91] In 1993, in an attempt to alleviate national security concerns, the U.S. Government adopted EES as a government-sponsored encryption standard.[92]

1. The Evolution of Encryption Technology in the United States

For centuries, military leaders, diplomats, and spies have practiced the art of cryptography[93] to prevent enemies from obtaining confidential[94] information.[95] Cryptography consists of

---

will harmonize national data security laws, thereby eliminating need to restrict data flows for privacy protection reasons).

85. *See supra* notes 18-20 and accompanying text (discussing EES as most recently released U.S. encryption standard).

86. OTA, *supra* note 15, at 121. DES, an encryption device, was the first government-sponsored encryption product. *Id.*

87. *Id.*

88. Fallows, *supra* note 21, at 46. Rivest-Shamir-Adelman, RSA, was developed in 1978, and is named after its inventors, Ronald Rivest, Adi Shamir and Leonard Adelman. *Id.*

89. OTA, *supra* note 15, at 120.

90. *See* Rochelle Garner, *Clipper's Hidden Agenda*, OPEN COMPUTING, Aug. 1994, at 54 (reporting that international finance and banking communities encrypt data with DES and RSA encryption systems); Eric Hirschhorn & David Payton, *Uncle Sam's Decoder Ring*, WASH. POST, June 25, 1992, at A23 (reporting that encryption is routine business precaution); Stewart A. Baker, *Don't Worry Be Happy*, *in* BUILDING IN BIG BROTHER 295, 299 (Lance J. Hoffman ed., 1994) (noting that development of encryption technology is expensive because of time-consuming process of testing strength of algorithm for bugs and weaknesses).

91. *See* James Daly, *Security Pros, Clinton Clash over Encryption Standards*, COMPUTERWORLD, Jan. 1994, at 79 (stating that U.S. Government fears RSA and DES may prevent U.S. security agencies from intercepting non-U.S. communications).

92. OTA, *supra* note 15, at 117.

93. *See* HOFFMAN, *supra* note 4, at 42 (explaining "cryptography" is Greek word for "hidden writing").

94. *See* OTA, *supra* note 15, at 112 (defining confidentiality as secrecy of contents).

two components: encryption[96] and decryption.[97] Encryption involves converting information into an unreadable form, while decryption operates to reconvert the information into an understandable language.[98] Encryption and decryption are accomplished using mathematical algorithms[99] that convert and reconvert information.[100] Although algorithms do not prevent access to the message, they do prevent unauthorized persons from understanding the message's contents.[101] The more complex the algorithm, the more difficult it is to determine the algorithm's formula and decrypt the information.[102]

Whereas algorithms in manual cryptosystems code information with simple formulas, computer-based algorithms code computerized data with keys.[103] A key consists of a series of bits.[104]

"Confidentiality is a concept which applies to data. It is the status accorded to data which has been agreed upon between the person or organization furnishing the data and the organization receiving it and which describes the degree of protection to be provided." HOFFMAN, *supra* note 4, at 2.

95. *See* HOFFMAN, *supra* note 4, at 42-43 (stating that Spartans in fifth century B.C. and Venice's ruling body in sixteenth century, both employed cryptographic techniques to conceal messages from adversaries); Rubenstein, *supra* note 16, at 182 (explaining that Julius Caesar protected messages by substituting every letter in word with letter that is three letters later in alphabet). To illustrate Caesar's code, the string:

ZHBQHHGBPRUHBVQRZBIRUBEHWWHUBVNLLQJ

is the encrypted version of the message:

WE NEED MORE SNOW FOR BETTER SKIING

HOFFMAN, *supra* note 4, at 43.

96. OTA, *supra* note 15, at 112. The encrypted, unintelligible version of the information is often referred to as ciphertext. *Id.*

97. *Id.* The decrypted, understandable version of the information is often referred to as plaintext. *Id.*

98. *See Cryptography Policy*, *supra* note 3, at 109 (describing encryption and decryption as inverse operations).

99. BUILDING IN BIG BROTHER: THE CRYPTOGRAPHIC POLICY DEBATE 14 (Lance J. Hoffman ed., 1994) [hereinafter BUILDING IN BIG BROTHER]. Mathematical algorithms comprise the technique or rules selected for encryption. *Id.* The algorithm selected determines "how simple or how complex the process of transformation will be." *Id.*; *see* John Markoff, *Big Brother and the Computer Age*, N.Y. TIMES, May 6, 1993, at D1 [hereinafter *Big Brother and the Computer Age*] (defining algorithm as mathematical formula on which encoding system is based).

100. *See* OTA, *supra* note 15, at 113 (defining algorithm as technique by which original input is transformed into form that is unintelligible without knowledge of secret information).

101. Rubenstein, *supra* note 16, at 182. Algorithms scramble the messages. *Id.*

102. *See* OTA, *supra* note 15, at 112 (stating that strength of algorithm depends upon number of steps, storage, and time necessary to break code and read encrypted message, without prior knowledge of formula on which algorithm is based).

103. BUILDING IN BIG BROTHER, *supra* note 99, at 14. A key is a secret value that acts as a password. *Id.* The key is incorporated into the algorithm to convert the infor-

Each bit is comprised of a string of zeros and ones.[105] A computer user must input the appropriate key into the algorithm to encrypt and decrypt data.[106] The strength of the algorithm and the amount of bits included in the key[107] determine the amount of protection afforded by the encryption technology employed.[108]

Computer database networks that lack effective security devices are susceptible to unauthorized intrusion,[109] interception,[110] and misuse.[111] Unauthorized acquisition of personal data, which generally occurs for pecuniary reasons[112] or as a

---

mation into an unreadable form. *Cryptography Policy*, *supra* note 3, at 109. The algorithm and the key are collectively titled a cryptosystem. OTA, *supra* note 15, at 113. Keys, which are generated randomly, encrypt and decrypt data. Daniel Pearl, *Encryption - Software Plan Presented Using 'Keys" Held by Escrow Agents*, WALL ST. J., Aug. 18, 1995, at A3.

104. Pearl, *supra* note 103, at A7.

105. *The Impact on America's Software Industry of Current U.S. Government Munitions Export Controls: Hearings Before the Subcomm. on Economic Policy, Trade and Environment of the House Comm. on Foreign Affairs*, 103d Cong., 1st Sess. 8 (1993).

106. *Id.*

107. *Id.* "Longer key lengths mean more possible keys for an intruder to try and thus imply greater security." *Id.*

108. *Id.*; BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY: PROTOCOLS, ALGORITHMS AND SOURCE CODE IN C 129 (1994); Charles L. Evans, Comment, *U.S. Export Control of Encryption Software: Efforts to Protect National Security Threaten the U.S. Software Industry's Ability to Compete in Foreign Markets*, 19 N.C.J. INT'L L. & COM. REG. 469 n.36 (1994). If a key possesses two bits, four possible key combinations exist: 00, 01, 10, 11. *Id.* If a key possesses three bits, eight possible key combinations exist. *Id.*

109. Michael D. Scott, *United States*, *in* DATA TRANSMISSION AND PRIVACY 487, 501 (Dennis Campbell & Joy Fisher eds., 1994). "Intrusion" is "the wrongful entering upon, seizing or taking possession of another's property." *Id.* Examples of computer-related intrusions include: unauthorized access to individual databases, unauthorized removal of data from computer systems, and unauthorized interception of data transmissions. *Id.*

110. *See id.* at 502 (presenting interception as equivalent to eavesdropping, and noting that examples of interception include: unauthorized access of computer-based data by person at computer site, unauthorized access of computer-based data from remote location, and interception of information communicated between computer and terminal or another computer).

111. *See id.* at 503 (explaining that information is misused when it was revealed for specific purpose and individual or entity to whom information was revealed uses it for unauthorized purpose).

112. Jerome Lobel, *Third Decade of Concern*, COMPUTERWORLD, Feb. 8, 1982, at 32. For example, access to banks' computer systems facilitates wire fraud and theft from computerized accounts. *Id.* Additionally, access to welfare agencies' computer systems allows people to illegally receive welfare payments. *Id.* A study released by the National Center for Computer Crime Data found that theft of money and services accounts for 70% of computer crimes. Michael Alexander, *Hacker Stereotypes Changing*, COMPUTERWORLD, Apr. 3, 1989, at 101.

game or challenge,[113] creates potentially devastating consequences[114] both to society at large and to the individual whose personal data is involved.[115] Computer-based encryption technology minimizes the likelihood of unauthorized acquisition.[116]

2. Entities Responsible for U.S. Encryption Standards

The U.S. Government segregates computerized data into two categories for purposes of determining the governmental entity responsible for protecting the data.[117] The National Security Agency[118] ("NSA") controls one category, classified data.[119] The Brooks Act[120] authorizes the U.S. Department of Commerce to control and create processing standards for the other category, "unclassified but sensitive" data.[121] The U.S. De-

---

113. TIME LIFE BOOKS, COMPUTER SECURITY 19 (Understanding Computers No. 8, 1986) [hereinafter UNDERSTANDING COMPUTERS]. A high school student broke into a university computer system and destroyed data "just for the fun of it." *Id.* In 1983, approximately twelve youths calling themselves the 414s, after the Milwaukee, Wisconsin area code, broke into more than sixty computer networks. JEROME LOBEL, FOILING THE SYSTEM BREAKERS 1 (1986).

114. *See Weekend Edition*, National Public Radio, Jan. 3, 1993, *available in* LEXIS, News Library, NPR File [hereinafter *Weekend Edition*] (identifying computerized theft, industrial espionage, electronic vandalism, and forgery as potential consequences of unprotected personal data).

115. *See* GEOFF L. SIMMONS, PRIVACY IN THE COMPUTER AGE 27 (1982) (explaining that disclosure of personal data may affect person's employment prospects, marriage, treatment in courts, credit ratings, and public reputation).

116. *See* Lobel, *supra* note 112, at 33 (explaining that encryption protects data while data is processed).

117. OTA, *supra* note 15, at 141.

118. National Security Act of 1947, Exec. Order No. 12,333, 46 C.F.R. 59941 (1981), *reprinted in* 50 U.S.C. §§ 401-32 (1988 & Supp. V 1993), *and in* 61 Stat. 495 (1947). The National Security Act of 1947 authorized the creation of the National Security Agency ("NSA"). *Id.* The U.S. Department of Defense oversees and controls NSA activities. *Id.* The NSA is concerned primarily with intelligence operations. *Id.*

119. BNA, COMPUTER DATA SECURITY: A LEGAL AND PRACTICAL GUIDE TO LIABILITY, LOSS PREVENTION, AND CRIMINAL & CIVIL REMEDIES 32 (1989) [hereinafter COMPUTER DATA SECURITY]. The Computer Security Act of 1987 ("Computer Security Act") defines "classified data" as "information which has been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy." Computer Security Act of 1987, 15 U.S.C. § 278g-3 (1988 & Supp. V 1993) [hereinafter Computer Security Act].

120. Federal Property and Administrative Services Act of 1949, ch. 288, § 111, 79 Stat. 1127 (1965) (codified as amended at 40 U.S.C. § 759(f) (1982)). The Brooks Act of 1965 authorized the Commerce Department to create computer systems research programs, and to formulate federal computer security standards for "unclassified but sensitive" information. OTA, *supra* note 15, at 133.

121. OTA, *supra* note 15, at 135. Computer Security Act, 15 U.S.C. § 278g-3. The Computer Security Act defines "sensitive information" as:

partment of Commerce delegates this duty to the National Institute of Science and Technology ("NIST").[122] NIST develops Federal Information Processing Standards ("FIPS").[123] FIPS influence U.S. Government agencies' decisions regarding which encryption technology to employ.[124] FIPS also facilitate the exchange of encrypted data among computer users.[125]

The Computer Security Act of 1987[126] ("Computer Security Act") reinforces and clarifies NIST and NSA duties regarding data security.[127] The Computer Security Act charges the NSA with the responsibility of protecting classified data processed on computer networks.[128] The Computer Security Act further mandates that NIST must create all U.S. security standards and guidelines for sensitive but unclassified computer systems.[129] The Computer Security Act provides that NIST may receive technical assistance from the NSA, but the NSA must only assist NIST in an advisory capacity.[130] NIST possesses final authority regarding the development of standards and guidelines for sensitive but unclassified data.[131]

> [A]ny information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled . . . but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy."

Id.

122. OTA, *supra* note 15, at 136. The National Institute of Science and Technology ("NIST") was originally named the National Bureau of Standards ("NBS"). *Id.* NBS established a program for computer security in 1973. *Id.* The NBS security program led to the adoption of DES as a Federal Information Processing Standard ("FIPS"). *Id.* Currently, FIPS are created by the NIST Computer Systems Laboratory. *Id.*

123. *Id.* at 129. NIST has published dozens of FIPS. *Id.* at 136. The most recently published FIPS is EES. *Id.*

124. *Id.*

125. *Id.*

126. Computer Security Act, 15 U.S.C. § 2789-3. COMPUTER DATA SECURITY, *supra* note 119, at 35. Rep. Dan Glickman (D-Kan) introduced The Computer Security Act on Jan. 6, 1987 as H. R. Res. 145. *Id.*

127. Computer Security Act, 15 U.S.C. § 2789-3; OTA, *supra* note 15, at 138.

128. OTA, *supra* note 15, at 138.

129. *See* Computer Security Act, 15 U.S.C. at § 3(3) (explaining that NIST must also help private sector organizations apply results of NIST computer security activities).

130. *Id.* at § 2(b)(1); *see* OTA, *supra* note 15, at 146 (explaining that NIST may consult NSA computer system technical security guidelines to extent that guidelines are consistent with NIST requirements).

131. OTA, *supra* note 15, at 145.

3. DES

The U.S. Government adopted DES as the first federal encryption standard to protect sensitive but unclassified computerized data.[132] In January 1977, NIST published DES as a FIPS,[133] and the U.S. Government endorsed DES as the official Government standard in July of the same year.[134] When the U.S. Government initially endorsed DES, encryption experts considered the DES algorithm unbreakable.[135] The National Bureau of Standards[136] ("NBS"), however, anticipated that future technological advancements might diminish DES's ability to provide adequate security.[137] NIST, therefore, required that the effectiveness of DES be evaluated every five years.[138] Despite growing concern regarding DES's ability to protect computerized information,[139] in 1993, NIST reaffirmed DES as the national standard until its reevaluation in 1998.[140]

---

132. *Id.* at 121. Scientists working for the International Business Machines Corporation developed DES specifically to protect information considered unclassified but sensitive to U.S. national security. *Id.*

133. *Id.* at 136. NBS, under the authority of the Brooks Act of 1965, adopted DES as a FIPS. *Id.*

134. *Id.* at 121.

135. Daly, *supra* note 91, at 79.

136. *See supra* note 122 (discussing creation and function of NBS).

137. NATIONAL BUREAU OF STANDARDS, FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, 46-1: DATA ENCRYPTION STANDARD 1, 4 (1977). Modern computers are able to launch "brute attacks" on DES in attempts to break DES code. *Id.* The more modern the computer used to launch the attack, the faster it can break DES codes. *Id.*

138. *Id.* NIST conducts the evaluations of DES. *Id.*

139. *Cryptography Policy*, *supra* note 3, at 110. "[T]he security of DES in the future is worrisome to some scientists, who contend that advances in technology will soon make it possible to break DES by 'brute force,' using a powerful computer to try every possible combination of keys until the correct key is discovered." *Id.*

140. *See* BUILDING IN BIG BROTHER, *supra* note 99, at 38 (stating that although NIST reaffirmed DES in 1993, NIST indicates that it might not reaffirm DES as national standard in 1998). The acting director of NIST, Dennis Branstead, stated that:

> Last year, NIST formally solicited comments on the recertification of DES. After reviewing those comments, and the other technical inputs that I have received, I plan to recommend to the Secretary of Commerce that he recertify DES for another five years. I also plan to suggest to the Secretary that when we announce the recertification we state our intention to consider alternatives to it over the next five years. By putting that announcement on the table, we hope to give people an opportunity to comment on orderly technological transitions. In the meantime, we need to consider the large installed base of systems that rely upon this proven standard.

SCHNEIER, *supra* note 108, at 223.

The DES algorithm, which possesses a 56-bit key,[141] is a single key[142] encryption algorithm.[143] In a single key system, every computer user participating in the particular communication employs the same key to encrypt and decrypt the data.[144] The authorized users must protect the key because any computer user who obtains the key used to encrypt the data can employ the same key to decrypt the data.[145] Because the degree of security afforded by DES depends upon how well the authorized computer users protect the key,[146] the possibility of lost, stolen, and counterfeit keys constitutes an inherent vulnerability in the DES system.[147]

4. RSA

In 1977, Ronald Rivest, Adi Shamir, and Leonard Adelman developed RSA, an alternative encryption device to DES.[148] Although the U.S. Government never endorsed RSA as a government-sponsored encryption standard,[149] the system enjoys international popularity.[150] Banks in Europe and Australia employ

---

141. UNDERSTANDING COMPUTERS, *supra* note 113, at 19. The algorithm breaks down information into sections of eight characters and then encrypts each section using a particular key. *Id.* DES's 56 bit key possesses 10^{17} possible values. Kurt Kleiner, *Cracking into the World of Whispers*, NEW SCIENTIST, Sept. 18, 1993, at 14. *See supra* note 104 (discussing components and function of keys and bits).

142. *See* BUILDING IN BIG BROTHER, *supra* note 99, at 19 (explaining that single key is also referred to as private key, symmetric key, or secret key).

143. Rubenstein, *supra* note 16, at 184.

144. BUILDING IN BIG BROTHER, *supra* note 99, at 19. If the key to encrypt the data is 0101, then the key to decrypt the data is also 0101. *Id.*

145. MORRIE GASSER, BUILDING A SECURE COMPUTER SYSTEM 258 (1988). "Because keys get stale after repeated use [the greater the amount of information encrypted with a given key, the easier it is to figure out the key and break the code], it is important to change keys periodically [an interval called a *cryptoperiod*]." *Id.*

146. BUILDING IN BIG BROTHER, *supra* note 99, at 19.

147. Fallows, *supra* note 21, at 46. "The need for two or more people to agree ahead of time on a key created problems that have been the stuff of spy novels and war histories for hundreds of years." *Id.*

148. OTA, *supra* note 15, at 220. In 1982, the inventors of RSA, Ronald Rivest, Adi Shamir, and Leonard Adelman, formed RSA Data Security, Inc., and obtained an exclusive license for their invention from the Massachusetts Institute of Technology, which had been assigned rights to the invention. *Id.*

149. *Id.* NIST claims that its desire to issue royalty-free FIPS prevented it from endorsing RSA as a government-sponsored encryption standard because RSA was developed by members of the private sector. *Id.*

150. Murray Slovick, *The Big Brother Chip*, POPULAR MECHANICS, Sept. 1994, at 116, 117.

RSA,[151] and over four million copies of RSA exist worldwide.[152]

The RSA system eliminates the need for computer users who exchange encrypted information to share secret keys,[153] the primary drawback associated with the DES single key system.[154] The RSA algorithm accomplishes this task by employing two mathematically related keys to encrypt and decrypt computerized data.[155] RSA's two key system[156] involves a private key and a public key.[157] To create the keys, a computer user must choose two prime numbers.[158] The public key, which equals the product of two 155-digit prime numbers,[159] may be used by any computer user to encrypt data.[160] The encrypted data, however, can only be decrypted by the holder of the private key, which consists of the original prime numbers.[161] Although the numbers employed to create the private key, theoretically, could be determined, the process would take hundreds of years.[162]

---

151. Garner, *supra* note 90, at 55.

152. Slovick, *supra* note 150, at 117.

153. Rubenstein, *supra* note 16, at 184.

154. Fallows, *supra* note 21, at 46. The inventors of RSA developed the encryption device based on the ideas included in a paper proposed by two Stanford University scientists, Whitfield Diffie and Martin Hellman. *Id.* Diffie and Hellman's paper proposed a cryptographic system that would eliminate the vulnerabilities associated with a single key system. *Id. See supra* note 147 and accompanying text (discussing vulnerability associated with DES single key system).

155. *See* Rubenstein, *supra* note 16, at 183 (explaining that because two keys are mathematically related, one key can encrypt information and other key can decrypt information, and vice-versa).

156. *See* BUILDING IN BIG BROTHER, *supra* note 99, at 19 (noting that two key system is also referred to as asymmetric key or public key system).

157. *See* Rubenstein, *supra* note 16, at 184 (explaining that two key system allows computer users to publish public key in directory while keeping private key private). The two key system incorporated into RSA allows computer users to employ the system for activities such as filing tax returns or using a credit card number for on-line shopping. Slovick, *supra* note 150, at 117.

158. Fallows, *supra* note 21, at 48; *see* Kleiner, *supra* note 141, at 14 (defining prime numbers as numbers possessing only two factors).

159. Kleiner, *supra* note 141, at 14.

160. Fallows, *supra* note 21, at 48.

161. *See id.* (stating that it is impossible to discern original prime number comprising secret key with only knowledge of public key).

162. *Id.* "Finding the factors of such a 200-digit number on a modern top-speed computer would require not milliseconds or minutes but at least several centuries. The task is, in computer terms, "computationally infeasible." *Id.*; *see* Slovick, *supra* note 150, at 117 (explaining that businesses are attracted to RSA because of system's security).

5. EES

The Clinton Administration released EES in April 1993[163] to protect unclassified but sensitive data.[164] NIST approved EES as a FIPS in February 1994.[165] EES consists of two components, the Clipper Chip[166] and the Capstone Chip.[167] Both components of EES are tamper-proof chips that incorporate the SKIPJACK algorithm.[168] All computer users participating in data communications encrypted with EES technology must possess a chip containing the SKIPJACK algorithm.[169] The sending party's chip encrypts the data, and the receiving party's chip decrypts the data.[170]

EES chips feature key escrow technology.[171] This technology allows law enforcement agencies to intercept voice and data communications.[172] Each EES chip possesses an identification number[173] that constitutes the chip-unique key.[174] Each chip-unique key is broken into two components.[175] Each component of a particular key is separately escrowed.[176] The U.S. Department of Treasury[177] holds one component of the key in escrow,

---

163. *Statement of the Press Secretary*, *supra* note 7.

164. OTA, *supra* note 15, at 117.

165. *Id.*; *Statement of the Press Secretary*, *supra* note 7. The Commerce Secretary approved EES as a FIPS Standard. *Id.* *See supra* notes 122-25 and accompanying text (discussing creation and function of FIPS).

166. Fallows, *supra* note 21, at 48.

167. *See* Kleiner, *supra* note 141, at 14 (explaining that Clipper Chip encrypts voice communications and Capstone Chip encrypts data communications); OTA, *supra* note 15, at 117 (stating that VLSI Logic produces these chips, and Mykotronx programs these chips with algorithms and keys).

168. Dorothy Denning, *The U.S. Key Escrow Encryption Technology*, *in* BUILDING IN BIG BROTHER 111, 112 (Lance J. Hoffman ed., 1994). SKIPJACK, which was designed by the NSA, is a single-key encryption algorithm. *Id.* SKIPJACK employs an 80-bit key. *Id.*

169. *Id.* at 114-15.

170. Kleiner, *supra* note 141, at 14.

171. *Id.*

172. OTA, *supra* note 15, at 117.

173. Fallows, *supra* note 21, at 48. The U.S. Government maintains a master list of identification numbers for every EES chip sold. *Id.*

174. *Communications and Computer Surveillance, Privacy and Security: Hearings Before the Subcomm. on Technology, Environment, and Aviation of the House of Representatives Comm. on Science, Space and Technology*, 103d Cong., 2d Sess. 3 (1994) (statement of Clinton C. Brooks, Special Assistant to the Director, NSA) [hereinafter Brooks].

175. Denning, *The U.S. Key Escrow Encryption Technology*, *in* BUILDING IN BIG BROTHER, *supra* note 168, at 111-12.

176. Brooks, *supra* note 174, at 3.

177. THE UNITED STATES GOVERNMENT MANUAL 1993/1994, at 492 (1994). The Treasury Department, which was created on September 2, 1789, formulates and recom-

and the U.S. Department of Commerce[178] holds the other component in escrow.[179] Constructing the chip-unique key necessary to decrypt the data requires the retrieval of the key's components from both escrow agents.[180]

II. *U.S. GOVERNMENT EFFORTS TO ESTABLISH EES AS THE DE FACTO U.S. ENCRYPTION STANDARD*

U.S. Government efforts to establish EES as the *de facto* encryption standard in the United States requires the promotion of EES technology and the elimination of competing encryption devices from the U.S. encryption market.[181] The successful establishment of EES as the *de facto* U.S. encryption standard will be advantageous for computer users and the U.S. Government.[182] Computer users will enjoy the most advanced data security system available to date,[183] and the U.S. Government will

---

mends economic, financial, and tax polices. *Id.* The Treasury Department also acts as the U.S. Government's financial agent and issues all U.S. coins and currency. *Id.*

178. *Id.* at 154-55. The Commerce Department was reorganized into its current form on March 4, 1913. *Id.* The Commerce Department creates and administers a variety of programs to facilitate international trade, economic growth, and technological advancement. *Id.*

179. Department of Justice, *Attorney General Makes Key Escrow Encryption Announcements*, Feb. 4, 1994 (on file with *Fordham International Law Journal*) [hereinafter *Key Escrow Announcment*]. Specifically, the Commerce Department's NIST and the Treasury Department's Automated Systems Division are the two agencies responsible for holding the keys in escrow. *Id.* "The two escrow agents were chosen because of their abilities to safeguard sensitive information, while at the same time being able to respond in a timely fashion when wiretaps encounter encrypted communications." *Id.* *But see* Garner, *supra* note 90, at 54 (criticizing choice of elected agents as violation of checks and balances system because both agencies are members of Executive Branch).

180. Denning, *The U.S. Key Escrow Encryption Technology*, *in* BUILDING IN BIG BROTHER, *supra* note 168, at 112. Whitfield Diffie stated:

> The effect is very much like that of the little key hole in the back of the combination locks used on the lockers of schoolchildren. The children open the lock with the combinations, which is supposed to keep the other children out, but the teachers can always look in the lockers by using the key.

Fallows, *supra* note 21, at 48-49.

181. Nina Schuyler, *Bugs in the System: The FBI Wants to Monitor Traffic on the Digital Superhighway*, CAL. LAW., July 1994, at 45, 46 (1994) (citing Marc Rotenberg, director of Electronic Privacy Information Center in Washington, DC).

182. *Statement of the Press Secretary*, *supra* note 7. "[EES] will provide Americans and government agencies with encryption products that are more secure . . . than others readily available today—while at the same time meeting the legitimate needs of law enforcement." *Id.*

183. *See* Brooks, *supra* note 174, at 4 (advocating widespread implementation of EES technology to enable computer users to take advantage of benefits offered by this technology).

reap the benefit of enhanced law enforcement capabilities.[184] Despite these advantages, however, the successful establishment of EES as the *de facto* U.S. encryption standard will also engender economic disadvantages for international businesses and U.S. encryption manufacturers.[185] In response to criticisms[186] concerning the disadvantages attributed to EES technology, the U.S. Government plans to develop a proposal for an alternative encryption standard.[187]

A. *U.S. Government Tactics*

Clinton Administration officials stress that all U.S. Government agencies and members of the private sector may implement EES on a purely voluntary basis.[188] Allowing optional implementation of EES, however, impedes the U.S. Government's goal of establishing EES as the *de facto* encryption standard in the United States.[189] The U.S. Government aims, therefore, to ensure voluntary implementation of EES by employing its market influence to promote EES technology[190] and by manipulating export controls to eliminate competing devices from the U.S. encryption market and to facilitate the export of EES.[191]

---

184. *See supra* note 20 and accompanying text (describing EES technology).

185. *Communications and Computer Surveillance, Privacy and Security: Hearings Before the Subcomm. on Technology, Environment and Aviation of the House of Representatives Comm. on Science, Space and Technology*, 103d Cong., 2d Sess. 3 (1994) (statement of Mr. Rohrabacher) [hereinafter Mr. Rohrabacher]. "[EES technology] is the wrong direction that we shouldn't be heading to." *Id.*

186. John Markoff, *U.S. to Urge A New Policy On Software*, N.Y. TIMES, Aug. 18, 1995, at D1 [hereinafter *U.S. to Urge a New Policy on Software*]. "[T]echnology executives have opposed the Government's data-scrambling policy because it restricts export of other types of data-security systems, which is seen as an impediment to sales of American computer products overseas." *Id.*

187. *Id.*

188. *Questions and Answers about the Clinton Administration's Encryption Policy*, The White House Office of the Press Secretary, Feb. 4, 1994, [hereinafter *Questions and Answers about the Clinton Administration's Encryption Policy*] (on file with *Fordham International Law Journal*). The U.S. Government continues to stress that it developed EES for voluntary use by Government agencies and the private sector. *Id. But see* Schuyler, *supra* note 181, at 45 (citing Kent Walker, assistant U.S. Attorney in San Francisco) (explaining that there is no requirement everyone use only EES; permitting use of another encryption device in addition to EES).

189. Garner, *supra* note 90, at 54.

190. *Id.*; *see* Fallows, *supra* note 21, at 50 (discussing how U.S. Government uses market influence to make EES *de facto* standard in United States).

191. *See* Garner, *supra* note 90, at 54 (speculating that U.S. Government uses EES technology to justify maintenance of export controls).

1. Manipulation of the U.S. Encryption Market

As the single largest purchaser of computer equipment in the world,[192] the U.S. Government possesses the ability to influence the U.S. encryption market by promoting widespread implementation of EES technology.[193] In 1994, NIST approved EES as a FIPS.[194] This approval allows U.S. Government agencies to insist that all Government purchases of computer equipment include EES technology.[195] The U.S. Government's substantial buying power and its demand for EES technology forces encryption software manufacturers who desire large Government contracts[196] to produce EES products.[197] Large U.S. Government purchases of EES technology reduces the price of this system,[198] and, in turn, promotes private sector demand for EES.[199] Mass production and affordable prices of EES technology promote widespread implementation of EES.[200]

---

192. Schuyler, *supra* note 181, at 45-46 (citing Marc Rotenberg, Director of Electronic Privacy Information Center in Washington, D.C.). COMPUTER DATA SECURITY, *supra* note 119, at 32. "The federal government spent about 1.6 percent of its fiscal 1986 budget on automated data processing equipment and services—more than 415 billion." *See* Fallows, *supra* note 21, at 50 (explaining that second only to U.S. Government, banks and credit-card companies purchase most encryption technology).

193. *NIST Announces Voluntary Escrowed Encryption Standard to Promote Secure Telecommunications*, U.S. DEP'T OF COM. NEWS, Feb. 4, 1994, at 2.

194. *See supra* notes 123-25 and accompanying text (describing purpose of FIPS).

195. *NIST Announces Voluntary Escrowed Encryption Standard to Promote Secure Telecommunications*, *supra* note 193. The approval of EES as a FIPS enables U.S. Government agencies to demand that American telecommunications and computer manufacturers include key escrow technology in all equipment purchased by the agencies. *Id.* If EES had not been approved as a FIPS, the "[a]gencies would have to formally waive DES requirements if they wanted to employ escrow encryption techniques." *Id.*

196. *See* Slovick, *supra* note 150, at 117 (stating that AT&T, presently only supplier of EES technology, already received orders of 8,000 EES chips from Department of Justice, and 20,000 chips from Department of Defense).

197. *See* Fallows, *supra* note 21, at 50 (stating that if U.S. encryption software manufacturers produce key escrow technology because it is only type of encryption technology that U.S. Government will implement, then key escrow technology will eventually crowd out competing products in the United States).

198. *See* Robert Lee Hotz, *Computer Code's Security Privacy Watchdogs*, L.A. TIMES, Oct. 4, 1993, at A1 (reporting that each Clipper Chip costs US$26).

199. John Perry Barlow, *Jackboots on the Infobahn*, *in* BUILDING IN BIG BROTHER 307, 312 (Lance J. Hoffman eds., 1994). "By purchasing massive numbers of [EES technology], [the U.S. Government] intend[s] to induce an economy of scale which will make [EES technology] cheap while the export embargo renders all competition either expensive or nonexistent." *Id.*

200. *See* Fallows, *supra* note 21, at 50 (arguing that EES technology will eventually crowd out competing encryption devices).

2. Manipulation of the U.S. Encryption Export Controls

The U.S. Government promotes the implementation of EES technology by restricting the export of competing encryption products, such as DES and RSA, and by facilitating the export of EES technology.[201] The U.S. Government considers "strong"[202] encryption products, such as DES and RSA, "inherently military in character."[203] The State Department is responsible for controlling the export of these products.[204] All items within the State Department's jurisdiction, including DES and RSA, appear on the United States Munitions List ("USML").[205] Exporters must obtain a munitions license to export any item included on the USML.[206] Munitions licenses require specific approval and must be applied for on a case-by-case basis.[207] These stringent controls effectively render DES and RSA non-exportable.[208] Encryption software manufacturers' inability to export DES and RSA has compelled many U.S. manufacturers to terminate production of these products.[209] This decrease in the production of

---

201. *See supra* note 191 and accompanying text (stating that U.S. Government manipulates U.S. encryption export controls to promote widespread implementation of EES).

202. SCHNEIER, *supra* note 108, at 7. "An algorithm is considered computationally . . . strong, if it cannot be broken with available (current or future) resources. Exactly what constitutes 'available resources' is open to interpretation." *Id.*; *see* OTA, *supra* note 15, at 156 n.135 (defining "strong" encryption as encryption systems that possess 1,024 bit keys and provide same degree of security as DES and RSA).

203. OTA, *supra* note 15, at 151.

204. *Id.* Specifically, the Office of Defense Controls, a component of the State Department, administers the export controls for items considered "inherently military in character." *Id.*

205. 22 U.S.C. § 2778(a)(1) (1988 & Supp. V 1993); OTA, *supra* note 15, at 151.

206. OTA, *supra* note 15, at 151.

207. *Id.*

208. *Id.* at 156. In 1992, the U.S. Government modified encryption export controls. *Id.* at 156-57. The 1992 modification relaxed controls for encryption systems possessing moderate encryption capabilities. *Id.* at 156. Systems with moderate encryption capabilities, such as RC2 and RC4, possess 40-bit keys. *Id.* at 156-57. This modification did not affect stringent controls on DES and RSA because these encryption devices possess strong encryption capabilities. *Id.* at 157.

209. OTA, *supra* note 15, at 157. Responding to the 1992 modification of encryption export controls, financially stable U.S. encryption software manufacturers produce two versions of encryption systems, strong versions that are eligible for sale in the United States and versions with moderate encryption capabilities for sale in non-U.S. nations. *Id.* U.S. computer software firms that do not possess the economic resources to manufacture two versions of each encryption system, however, only manufacture moderately secure encryption systems that qualify for sale in both the United States and non-U.S. destinations. *Id.*; *Weekend Edition*, *supra* note 114 (quoting reporter, Daniel

DES and RSA reduces their availability in the U.S. encryption market.[210]

The U.S Government defends stringent export controls on DES and RSA with claims that international availability of these strong encryption devices will endanger U.S. national security.[211] Despite stringent controls regulating the export of these encryption devices, commentators argue that the strongest encryption system available, EES, may be freely exported.[212] Governmental permission to export EES technology, in conjunction with the virtual embargo[213] on DES and RSA, suggests that the U.S. Government is manipulating export controls in an effort to establish EES as the *de facto* encryption standard in the United States.[214]

B. Potential Advantages of EES

Widespread implementation of EES technology will benefit computer users and the U.S. Government.[215] The U.S. Government maintains that computer users who employ EES technol-

---

Hinerfeld). "[A]lthough numerous companies such as Apple, Microsoft and IBM have licensed RSA's cryptographic software for an array of new products, they must use it in a weakened form." *Id.*; *see* Fallows, *supra* note 21, at 49 (noting that production of two versions of all equipment is costly and complicated).

210. *See Weekend Edition*, *supra* note 114 (concluding that decreased availability of strong encryption devices in United States shortchanges domestic computer users). DOMINICK SALVATORE, MICROECONOMICS 47 (2d ed. 1994). "[A]n increase in supply . . . results in . . . higher . . . quantity. A decrease in supply has the opposite effect." *Id.*

211. *Encryption-Export Control Reform*, U.S. Department of State, Feb. 4, 1994 (statement of Dr. Martha Harris, Deputy Assistant Secretary of State for Political Military Affairs). "The President has determined that vital U.S. national security and law enforcement interests compel maintaining appropriate control of encryption." *Id.*

212. Brooks, *supra* note 174, at 5-6. "[T]he Administration agreed at the urging of industry that key escrow encryption products would be exportable." *Id.* at 6.

213. OTA, *supra* note 15, at 157. In order to export any item on the USML, including DES and RSA, a munitions license must be obtained as well as specific approval for the item's export, which is granted on a case-by-case basis. *Id.* The export of USML products is strictly regulated and licenses are difficult to obtain. *Id.*

214. Garner, *supra* note 90, at 54. *But see* OTA, *supra* note 15, at 159.

> Our announcement regarding the exportability of key escrow encryption products has caused some to assert that the Administration is permitting the export of key escrow products while controlling competing products in order to force manufacturers to adopt key escrow technology. These are arguments without foundation . . . we are not using or intending to use export controls to force vendors to adopt key escrow technology.

Id.

215. *See supra* notes 182-84 and accompanying text (discussing how widespread implementation of EES will provide advantages to computer users).

ogy possess unrivaled data security.[216] Additionally, the key escrow technology incorporated into EES enhances U.S. Government law enforcement capabilities by allowing Government agencies to intercept crime-related data communications.[217]

1. Advanced Data Security

The Clinton Administration asserts that EES technology offers computer users the most advanced data security currently available on the international encryption market.[218] Although the U.S. Government refuses to publicly divulge information regarding SKIPJACK, the mathematical algorithm incorporated into EES technology,[219] the NSA and NIST employed encryption experts[220] to independently evaluate the algorithm's security.[221] These experts issued a joint report that discussed the SKIPJACK algorithm.[222]

The experts, who based their evaluation of SKIPJACK's security on the algorithm's ability to overcome "brute force attacks,"[223] concluded that the secrecy surrounding SKIPJACK

---

216. *Questions and Answers About the Clinton Administration's Encryption Policy*, *supra* note 188. "[EES technology] will provide Americans with encryption products that are more secure . . . than others readily available today." *Id.*

217. *Statement of the Vice President*, The White House Office of the Vice President, Feb. 4, 1994 (on file with *Fordham International Law Journal*).

218. *See Questions and Answers about the Clinton Administration's Encryption Policy*, *supra* note 188 (noting that EES technology guarantees most advanced security available to date).

219. Denning, *The U.S. Key Escrow Encryption Technology*, *in* BUILDING IN BIG BROTHER, *supra* note 168, at 112. "The algorithm was designed by the National Security Agency and is classified in order to prevent someone from implementing it in software or hardware without providing the law enforcement access feature, thereby taking advantage of the government's strong algorithm while rendering encrypted communications immune from lawful government surveillance." *Id.*

220. Ernest F. Brickell, et al., *SKIPJACK Review: Interim Report*, *in* BUILDING IN BIG BROTHER, 119, 119-20 (Lance J. Hoffman ed., 1994). Members of the expert group included: Ernest F. Brickell, Dorothy E. Denning, Stephen T. Kent, David P. Maher, and Walter Tuchman. *Id.*

221. Denning, *The U.S. Key Escrow Encryption Technology*, *in* BUILDING IN BIG BROTHER, *supra* note 168, at 112.

222. *Id.* at 112-13. The experts issued their joint report in July 1993. *Id.*

223. Brickell et al., *SKIPJACK Review: An Interim Report*, *in* BUILDING IN BIG BROTHER, *supra* note 220, at 122. Attacks constitute attempts to determine either the key employed to encrypt the data or the message in its readable form. *Id.* A brute force attack is also called an exhaustive search. *Id.* A brute force attack occurs when a computer user "tries all possible keys" until one is found that decrypts the data. *Id.* The amount of time required to perform a brute force attack is directly related to the length of the keys. *Id.* A hypothetical, future, supercomputer costing US$50 million would

does not conceal any weakness within its algorithm.[224] The report also confirms the U.S. Government's assertions that SKIPJACK appears to be the strongest algorithm currently available on the international encryption market.[225]

2. Enhanced U.S. Law Enforcement Capabilities

The key escrow technology incorporated into EES chips enables U.S. Government agencies to intercept personal data communications encrypted with EES technology for law enforcement purposes.[226] Interception of crime-related communications provides law enforcement agencies with the information necessary to prevent crimes and prosecutors with incriminating evidence to prosecute criminal offenders.[227] The law enforce-

---

take approximately 4 million years to break SKIPJACK by a brute force attack. *Id.* SKIPJACK evaluators concluded:

> Under an assumption that the cost of processing power is halved every eighteen months, it will be 36 years before the cost of breaking SKIPJACK by exhaustive search will be equal to the cost of breaking [DES] today. Thus, there is no significant risk that SKIPJACK will be broken by exhaustive search in the next 30-40 years.

Id. at 118.

224. *Id.* at 113; *see* Slovick, *supra* note 150, at 117 (reporting that Dr. Matthew Blaze, computer scientist at Bell Laboratories, created computer program that prevents anyone, including U.S. Government, from intercepting communication encrypted with EES technology).

225. Denning, *The U.S. Key Escrow Encryption Technology*, *in* BUILDING IN BIG BROTHER, *supra* note 168, at 113.

226. OTA, *supra* note 15, at 116; *see* Slovick, *supra* note 150, at 116 (stating that law enforcement agencies need ability to intercept and monitor content of calls made electronically by mobsters, terrorists, and drug dealers). U.S. DEPT. OF JUSTICE, *Benefits and Costs of Legislation to Ensure the Government's Continued Capability to Investigate Crime with the Implementation of New Telecommunications Technologies*, Document C.A. 92-2117 (368) (testimony of David C. Williams, Office of Special Investigations, General Accounting Office). "Electronic surveillance is another tool that has been of great value to the law enforcement community to combat the La Cosa Nostra ("LCN") [organized crime families]. Evidence gathered through electronic surveillance . . . has had a devastating impact on organized crime." *Id.* Statistics from 1985-91 regarding the success of electronic surveillance include: 7,324 individuals convicted; US$295,851,162 in fines levied, US$756,363,288 in court-ordered recoveries, restitutions and forfeitures, and US$1,862,414,937 in prevented potential economic loss. *Id.* Electronic surveillance has also prevented terrorist incidents. *Id.* "[A] terrorist rocket attack against a United States ally by a foreign-based terrorist group was thwarted, and the electronic surveillance- based investigation led to the arrest of the principals and to the prevention of the loss of life of scores of persons." *Id.*

227. *See* U.S. DEPT. OF JUSTICE, *Authorization Procedures for Release of Encryption Key Components in conjunction with Intercepts Pursuant to State Statutes* (1994) (discussing procedure for release of keys to prosecutors).

ment access field[228] ("LEAF") included on each EES chip facilitates data interception.[229] Each LEAF contains the identity of the individual chip employed to encrypt data and the computer user's chip-unique key.[230] The LEAF electronically reveals the identity of the individual chip, allowing the law enforcement agency to retrieve the components of the escrowed chip-unique key from the designated escrow agents.[231]

U.S. Government agencies may only obtain an escrowed key for law enforcement purposes.[232] The agencies must first receive legal authorization to obtain the escrowed key.[233] The agencies must then present the authorization to the governmental bodies that hold the components of the key in escrow.[234] U.S. Government agencies that retrieve the components of the chip-unique key from the designated escrow agents combine the two parts of the key and decrypt the encrypted information.[235] When the law enforcement agents complete the interception, the key's ability to decrypt data encrypted with a particular chip terminates.[236]

---

228. OTA, *supra* note 15, at 117. Each EES chip contains a law enforcement access field ("LEAF") that allows data communications to be easily decrypted when the equivalent of a legal wiretap has been authorized. *Id.*

229. Kleiner, *supra* note 141, at 14.

230. *Id.*

231. *Id.*

232. *See* Schuyler, *supra* note 181, at 46 (citing Kent Walker, assistant U.S. Attorney in San Francisco) (explaining that Department of Justice monitors purposes for which keys are obtained). *But see* Garner, *supra* note 90, at 54 (conceding that although escrow agents are only authorized to relinquish keys for law enforcement purposes, possibility exists that keys will be revealed illegally, and used to perpetrate acts of fraud and bribery). To illustrate the possible illegal uses of keys:

> Both John Walker and Aldridge Ames committed treason for money, not ideology. In Walker's case, that information was the actual cryptographic keys used by the US Navy, allowing the Soviets to decipher submarine communications. Now imagine how much a hostile power might pay for every escrowed key used within the United States.

Id.

233. *See Questions and Answers about the Clinton Administration's Encryption Policy*, *supra* note 188 (noting that authorization to obtain escrowed keys is usually court ordered).

234. *Questions and Answers About the Clinton Administration's Encryption Policy*, *supra* note 188. *See supra* notes 177-78 and accompanying text (examining functions of Commerce and Treasury Departments).

235. OTA, *supra* note 15, at 117.

236. *Key Escrow Announcements*, *supra* note 179; *see* Schuyler, *supra* note 181, at 46 (citing Kent Walker) (explaining that each escrowed key was designed to work for only one specific serial number chip).

C. Potential Disadvantages of EES

The establishment of EES as the *de facto* encryption standard in the United States will engender disadvantages that do not justify the implementation of this system.[237] U.S. businesses that are engaged in international, computerized transactions will suffer economically because EES technology is incompatible with the state of the art security standard outlined in Article 17.[238] Additionally, the U.S. Government's manipulation of encryption export controls to establish widespread implementation of EES handicaps U.S. encryption software manufacturers' ability to compete in the international encryption market.[239] Furthermore, worldwide availability of DES and RSA inhibits the U.S. Government from realizing the law enforcement benefits attributed to EES' key escrow technology.[240]

1. Incompatibility with Article 17

While Article 17 provides individual EU Member States with discretion regarding which specific security measures data controllers may implement when processing personal data, Article 17 ensures that all EU Member States require data controllers to secure personal data with state of the art technology.[241] EU Member States, unwilling to provide the U.S. Government with the ability to eavesdrop on communications conveyed over EU computer networks,[242] have indicated that EES's key escrow feature prevents this encryption system from satisfying the state of

---

237. *See supra* note 185 and accompanying text (emphasizing negative consequences of EES).

238. *See supra* notes 79-84, 171-80 and accompanying text (describing state of art standard in Article 17 and key escrow technology featured in EES).

239. Bob Violino, *Encryption Triggers Competition*, INFO. WK., Feb. 7, 1994, at 15.

240. *New SPA Study: Export Regulations Preclude U.S. Companies From Cashing in on Multi-Million Dollar Encryption Software Market*, U.S. NEWSWIRE, Sept. 1, 1993, *available in* LEXIS, News Library, USNWR File [hereinafter *New SPA Study*]. A study released by the Software Publishers Association ("SPA") identifies 215 encryption products manufactured in twenty foreign counties, including: Russia, Japan, South Africa, Germany, India, the United Kingdom, and Canada. *Id.* The study also reported that eighty-four out of these 215 encryption products employ DES technology. *Id.*

241. 1995 Directive No. 1/95, *supra* note 1, art. 17(1), O/J. L 93/01, at 12 (1995).

242. *See* Schuyler, *supra* note 181, at 48 (discussing EU states' reluctance to allow U.S. Government surveillance). "[W]hy would an overseas customer who needs to be sure of data security buy a product which they know the U.S. government has access to." Kleiner, *supra* note 141, at 15.

the art standard outlined in Article 17.[243] The incompatibility of EES and Article 17 will severely inhibit the ability of U.S. businesses to conduct international data communications because EU Member States will prohibit these communications from entering their jurisdictions.[244]

2. Impediments to U.S. Encryption Manufacturers

U.S. encryption software manufacturers claim that stringent U.S. export controls on encryption software, such as DES and RSA, restrict their ability to participate in the growing international encryption market.[245] Computer users in the European Union are unable to purchase these encryption devices from U.S. manufactures because stringent encryption export controls prevent devices manufactured in the United States from entering the international encryption market.[246] Additionally, export controls on DES and RSA compel U.S. businesses operating outside the United States to purchase these encryption systems from non-U.S. manufacturers.[247] Further, although the U.S. Government permits the exportation of EES, computer users operating outside the United States do not purchase EES technology.[248] These computer users do not want the U.S. Government to eavesdrop on their data communications.[249] U.S. encryption software manufacturers' inability to export DES and RSA, combined with the international disinterest in EES technology, de-

---

243. *See supra* notes 79-84, 141-80 and accompanying text (describing state of art standard in Article 17 and key escrow technology featured in EES).

244. Schuyler, *supra* note 181, at 48.

245. *New SPA Study*, *supra* note 240. "Because [strong encryption] products cannot be exported, their manufacturers cannot compete with the rapidly growing number of foreign firms in the encryption market." *Id.*; *see* Violino, *supra* note 239, at 15 (stating that letter was sent to Vice President Al Gore from Chief Executive Officers of eight U.S. software manufacture companies, asking Clinton Administration to eliminate export controls on strong encryption technology).

246. *See Cryptography Policy*, *supra* note 3, at 111 (noting that although U.S. software manufacturers control approximately seventy-five percent of market, encryption export controls do not allow U.S. market share in cryptographic products sold internationally to rise above fifty percent).

247. *Id.* "[A] recent survey of *Fortune 500* companies conducted for the Business Software Alliance ("BSA"), a Washington-based vendor group that represents companies that wrote to Gore, shows that more than one-third would consider buying encrypted software from foreign suppliers for their overseas offices." *Id.*

248. Mr. Rohrabacher, *supra* note 185.

249. *Id.* "[N]o one overseas will buy our . . . computer equipment. Why should they? Why should they pay us money so we can eavesdrop on them?" *Id.*

prives the U.S. encryption software industry of billions of dollars of potential annual revenue.[250]

3. Resistance to the Implementation of EES

The U.S. Government can only reap the law enforcement benefits attributed to EES' key escrow technology if every computer user in the United States, including every criminal, encrypts data with EES technology.[251] Successfully establishing EES as the *de facto* encryption standard, however, will not produce this result.[252] The establishment of EES as the *de facto* encryption standard will compel many computer users who are not conducting crime-related communications over computer networks to encrypt data with EES technology.[253] Computer users conducting crime-related data communications, however, will not encrypt data with EES.[254] Criminals, unwilling to facilitate the ability of the U.S. Government to eavesdrop on crime-related communications, will obtain competing encryption devices, such as DES and RSA, from non-U.S. manufacturers.[255] DES and RSA, although invented in the United States, are manufactured worldwide.[256] Criminals' ability to avoid encrypting crime-re-

---

250. *See* Violino, *supra* note 239, at 15 (explaining that BSA estimates that U.S. manufacturers stand to lose US$9 billion dollars in revenue in 1995 and tens of thousands of jobs as result of stringent encryption export controls).

251. Garner, *supra* note 90, at 51.

252. *See id.* (concluding that criminals will not encrypt data with EES technology).

253. Fallows, *supra* note 21, at 50. "By establishing [EES] as a standard, the government hopes to keep encryption . . . from becoming so cheap that anyone can walk into a Radio Shack and buy a perfectly secure phone." *Id.*

254. *Id.* "The stated reason for a scrambling chip that permits wiretapping is that otherwise terrorists, drug dealers, and other criminals might use untappable scrambling schemes. With [EES technology] they still can." *Id.*

255. *See* Daly, *supra* note 91, at 79 (stating that study conducted by Software Publishers Association in Washington, D.C. reports that DES and RSA are flourishing abroad); *supra* note 240 and accompanying text (listing non-U.S. nations that manufacture DES and RSA).

256. Fallows, *supra* note 21, at 50.

> By establishing [EES] as a standard, the government hopes to keep encryption, especially public-key systems, from becoming so cheap and convenient that anyone can walk into a Radio Shack and buy a perfectly secure phone . . . it is guaranteed to be least effective against the most serious criminal opponents, such as state-sponsored terrorist rings that will not be limited to what they can find at Radio Shack.

Id.; Kleiner, *supra* note 141, at 14 (citing Chris Castor, a computer consultant and member of Computer System Security and Privacy Advisory Board). "If you tell crooks that if they use [EES] the law enforcement people are going to be able to intercept your calls,

lated communications with EES technology will prevent law enforcement agencies from intercepting these communications, and will thereby impede the enhancement of law enforcement capabilities.[257]

D. Recent Developments

On August 17, 1995, the Clinton Administration yielded to pressure from U.S. encryption software manufacturers[258] and pledged to develop a proposal to modify the U.S. Government's current positions on data security and encryption export controls.[259] This proposal will introduce an alternative encryption system to EES.[260] This new encryption system will, like EES, involve escrowed keys.[261] The Clinton Administration, however, will consider allowing non-governmental entities to act as the escrow agents of the keys.[262] Under the proposal, the U.S. Government will be required to acquire a search warrant to obtain the key from the non-governmental escrow agent.[263]

The proposal will also suggest modifications of the U.S. Government's policy on encryption export controls.[264] Currently, export controls permit U.S. encryption software manufacturers to export encryption devices with keys containing no more than forty bits.[265] The Clinton Administration will consider allowing

---

they're not going to use it. Deducing this does not need rocket science." *Id.* *But see* Baker, *Don't Worry Be Happy*, *in* BUILDING IN BIG BROTHER, *supra* note 90, at 298 (recognizing that for criminals to scramble information with encryption devices, criminals must first purchase and distribute expensive gear to all participating criminals, but few criminals possess sufficient resources to accomplish this).

257. Fallows, *supra* note 21, at 50 (quoting statement of Jim Kallstrom, FBI Special Agent in charge of New York). "Will some criminals catch on to the system, and buy their encryption from, let's say, Israel? Yes. Will that be a problem? Yes." *Id.*

258. *See U.S. to Urge A New Policy on Software*, *supra* note 186, at D1 (explaining that officials from encryption software industry recently wrote to Vice President Al Gore and requested that negotiations about U.S. encryption policy resume).

259. *Id.*

260. *Id.*

261. *Id.*; Daniel Pearl, *Encryption-Software Plan Presented Using 'Keys' Held by Escrow Agents*, WALL ST. J., Aug. 18, 1995, at A3. "[T]he government would have to get a search warrant to obtain the key from a company holding it on behalf of the person sending or receiving encrypted messages." *Id.*

262. *See* Pearl, *supra* note 261, at A3 (noting that certification process of escrow agents to exclude criminals remains unresolved issue).

263. *Id.*

264. *U.S. to Urge A New Policy on Software*, *supra* note 186, at D1.

265. *Id.* at D6.

The vulnerability of 40-bit systems was underscored [on August 16, 1995, when

the export of encryption devices containing keys with sixty-four bits, the length of the key incorporated into the DES system.[266]

III. *THE U.S. GOVERNMENT SHOULD ABANDON EES AND PROMOTE AN ALTERNATIVE STANDARD THAT ENSURES CONTINUED U.S. PARTICIPATION IN THE INTERNATIONAL MARKETPLACE*

The prospect of incompatible EU and U.S. data security requirements,[267] U.S. encryption software manufactures' exclusion from the international encryption market, and U.S. law enforcement agencies' inability to realize the potential law enforcement benefits associated with EES outweigh the advantage of advanced security afforded by EES technology.[268] Accordingly, the U.S. Government should abandon its quest to establish EES as the *de facto* U.S. encryption standard and should instead promote an international data security standard.[269] To facilitate the implementation of this international data security standard, an international entity should be established to hold keys in escrow. An international standard would eliminate all incompatibilities between national data security laws and would facilitate data processing across national borders.[270] Despite the advantages as-

---

> a] French student decoded a message that had been encoded using the 40-bit security feature . . . [t]he student . . . used 120 computers in a campus network to simultaneously test every key possible in a short period. It took him eight days, but he was able to decode a single encoded . . . message.

Id.

266. *See id.* (noting that U.S. Government will only consider allowing export of encryption devices with 64-bits if decoding keys are held in escrow for access by law enforcement agencies). "A 64-bit program would, theoretically, be 65,000 times harder to crack than a 40-bit program." *Id.*

267. *See supra* notes 241-44 and accompanying text (discussing incompatibility of EU and U.S. data security requirements). The following hypothetical illustrates the standards' incompatibility: Person A, who works at Bank X in Paris, asks Person B, who works at a financial institution Y in New York, to transmit personal data regarding Person C. Person A, as the data controller, must ensure that the data transmitted by Person B is protected with state of the art security measures. If the U.S. Government successfully establishes EES as the *de facto* encryption standard, Person B will likely implement EES to encrypt data. However, if the French Government does not consider EES state of the art, under French law, Person A will not be permitted to receive the data.

268. *See supra* notes 215-57 and accompanying text (discussing advantages and disadvantages associated with EES technology).

269. *See Cryptography Policy*, *supra* note 3, at 116-17 (discussing various U.S. Government options regarding data security, and potential consequences of these options).

270. *See supra* notes 241-44 and accompanying text (discussing incompatibilities that prevent data processing across national borders).

sociated with an international standard, however, the U.S. Government has not indicated whether it will consider the development of international data security standard.[271]

On August 17, 1995, the Clinton Administration responded to critics of EES[272] by pledging to develop a proposal for a new data security standard that would replace EES.[273] Although the proposal will advocate the replacement of Government key escrow agents with non-governmental key escrow agents, the U.S. Government will not relinquish its ability to acquire keys for law enforcement purposes.[274] This proposed alternative does not eliminate the concerns of computer users in the European Union and the United States who are plagued by incompatible personal data security laws.[275] The U.S. Government's continued ability to eavesdrop on data communication encrypted with the proposed standard will render this encryption system incompatible with Article 17's state of the art standard.[276] EU Member States, therefore, will continue to prohibit data communications encrypted with key escrow technology from entering their jurisdictions.[277] Furthermore, even if the European Union declares that the proposed encryption system satisfies Article 17's state of the art standard, creating an alternative encryption device requires significant research and development.[278] If the U.S. Government continues to manipulate the U.S. encryption market and to impose restrictive encryption export controls, EES will become the *de facto* standard in the United States before an alternative device is developed.[279]

---

271. *See supra* notes 258-66 and accompanying text (discussing U.S. Government proposal for data security, which is to be implemented solely in United States).

272. *See supra* note 186 and accompanying text (discussing criticisms of EES).

273. *Statement of the Press Secretary*, *supra* note 7. "The Administration is announcing its intent to work with industry to develop other key escrow products that might better meet the needs of individuals and industry." *Id.*

274. *Id.*

275. *See supra* notes 241-44, 267 (describing potential consequences of incompatible data security standards in European Union and United States).

276. *See supra* note 242 and accompanying text (describing EU states' reluctance to allow U.S. Government to eavesdrop on data communications).

277. *See supra* note 244 and accompanying text (noting that incompatibility of two standards compels U.S. states to prohibit data encrypted with EES from entering jurisdictions).

278. *See supra* note 90 (recognizing that development of encryption technology is time-consuming and expensive because of need to test strength of algorithm).

279. *See supra* notes 188-214 and accompanying text (discussing U.S. Government's manipulation of encryption market and export controls).

The U.S. Government's most viable alternative is to concurrently terminate all attempts to transform EES into the *de facto* encryption standard in the United States and to facilitate the accessibility of all currently available encryption devices, including DES and RSA.[280] This alternative eliminates the disadvantages associated with EES in an inexpensive[281] and non-disruptive manner.[282] Although the U.S. Government considers this solution unsatisfactory because it prevents the enhancement of U.S. law enforcement capabilities,[283] no peace-time precedent suggests that the U.S. Government possesses the ability to mandate EES, or any other key escrow system.[284] The U.S. Government continues to rely on voluntary compliance of EES.[285] Accordingly, computer users processing personal data between the United States and the European Union can avoid the disadvantages associated with EES by refraining from employing this system or by implementing alternative encryption devices.[286]

CONCLUSION

The advanced data security afforded by EES does not justify the economic disadvantages attributed to widespread implementation of this system. To avoid these disadvantages, the U.S. Government should terminate all attempts to establish EES as the *de facto* U.S. encryption standard. Facilitating the availability of all encryption devices, such as DES and RSA, allows: (a) computer users in the United States to protect data with strong encryption devices; (b) businesses to conduct international data communications; and (c) U.S. encryption software manufacturers to participate in the international encryption market. The U.S. Gov-

280. *See supra* notes 132-62 and accompanying text (presenting DES and RSA encryption systems).

281. *See supra* note 19 and accompanying text (specifying costs expended for creation and upkeep of the EES key escrow system).

282. *See supra* notes 237-57 and accompanying text (discussing disadvantages associated with EES technology).

283. *See supra* notes 258-66 and accompanying text (discussing U.S. Government's most recent proposal, which involves key escrow technology); *but see supra* notes 251-57 and accompanying text (describing inability of EES to substantially enhance U.S. Government law enforcement capabilities).

284. Fallows, *supra* note 21, at 49-50.

285. *Id.*

286. Barlow, *Jackboots on the Infobahn*, *in* BUILDING IN BIG BROTHER, *supra* note 199, at 313. "Don't buy any product with Big Brother inside. [The U.S. Government] cannot, as yet, require you to do so. Just say no." *Id.*

ernment's refusal to facilitate the availability of all encryption devices will ultimately exclude the United States from participating in the international marketplace.