INVITED TALK 2

J. H. P. Eloff et al. (eds.), *Information Security — the Next Decade*

6

Encryption Policy for the Global Information Infrastructure

Lance J. Hoffman

Institute for Computer and Telecommunications Systems Policy and
Department of Electrical Engineering and Computer Science
The George Washington University
Washington, D.C. 20052 USA
hoffman@seas.gwu.edu

Abstract

Cryptology policy deals not only with various technological encryption methods but also with thorny political and administrative problems. It is a challenge to address these in a timely and open manner. The problems arise in law enforcement, civil liberties, and export control policy. They must be confronted if a rational cryptographic policy is to provide a framework in which technological solutions can operate.

1.0 Introduction

The announcement of the Clipper chip by the U.S. Government in April 1993 set off a frenzy of discussions about cryptography policy in the computer community. The shock waves from it ultimately produced front page treatment in *The New York Times*, repeated questions to the Vice President of the United States, and a new newsgroup on the Internet. They also produced a great deal of public discussion about striking the balance between national security, law enforcement, and civil liberties.

As the Global Information Infrastructure develops, more governments are becoming concerned with communications privacy and security. This is not a new phenomenon; even before the French revolution governments were worried about accountability of authors and publication of seditious materials[Hesse 1990]. In 1993, the scepter of effectively unbreakable cryptography available to any individual pushed the United States government into launching three interrelated initiatives: the digital telephony improvement initiative, the Clipper chip key escrow encryption initiative, and export control reform. The first effectively makes the public switched telephone network "wiretap-friendly"; the second promotes encryption that can be broken, under certain conditions, by the government; the third is supposed to expedite licensing of encryption product exports.

We attempt here to present a survey of the policy issues in a non-ethnocentric manner.

However, since the United States has been in the forefront of framing the debate, and since the author has been close to that debate, this account necessarily will reflect his knowledge. It would be welcome if similar accounts from other countries were made available.

This paper does not examine the technology of cryptography; readers interested in those issues are referred to [Beth 1992, Brassard 1989, Rivest 1990, Kahn 1967, Diffie 1976]. Here, we present a Cook's Tour of encryption policy, sketching out the general landscape and providing pointers on where to go to get more detailed information.

1.1 The Digital Telephony Initiative

The digital telephony initiative was a successful effort by the U. S. Government to maintain some capability to wiretap in cases where advances in telecommunications technology could (or had already) outrun law enforcement's ability to intercept communications in order to enforce laws and protect national security. Recent legislation [HR4922] passed by the U. S. Congress requires telecommunications carriers to ensure that they possess the capability and capacity to enable the government to isolate and intercept, pursuant to authorization by a court, call identifying information and the contents of a communication. The requirements apply only to carriers who engage in "the transmission of switching of wire or electronic communications as a common carrier for hire." They do not apply to information service providers (the Internet, America Online, Prodigy, etc.), to private networks, or to PBX's. The requirements for obtaining a warrant prior to the interception have not been changed. Law enforcement cannot require a carrier to install a port which can be remotely activated by a law enforcement officer. All taps must be conducted with the intervention of the carrier (as is the case under current law). The new law authorizes US$500 million to be paid by the government for this retrofitting of the telephone system.

1.2 The Clipper Chip Key Escrow Encryption Initiative

The key escrow encryption initiative (popularly known as the "Clipper plan", or just "Clipper") is a U. S. Government attempt to protect communications against industrial espionage and other compromises while at the same time maintaining the existing capability of law enforcement and national security agencies to eavesdrop, with a court order, on suspect communications. When law enforcement or national security agencies are interested in a person's communication, they obtain a warrant from the appropriate issuing authority. They then fax a notification that they have this to two independent government agencies (currently the National Institute of Standards and Technology and the Automated Systems Division of the Department of the Treasury), who then each give up half of the digital key necessary to decrypt the conversation. When the two half-keys are joined to form the entire key, law enforcement officials can then obtain the unit key for the given chip used in the communicating telephone and use it to decrypt

the conversation (assuming that telephone has used the Clipper chip in the first place). A detailed description of the system appears in [Denning 1994a].

This so-called "escrowed encryption standard" [NIST 1994a] is encouraged but voluntary in the federal government. The Administration, after looking into potential violations of the U. S. Constitution, decided not to make it mandatory for private persons. Nevertheless, it clearly hopes that almost everybody will use this system. Some civil libertarians and outside observers are concerned that it will become mandatory in the future. Indeed, FBI Director Louis Freeh has been quoted as stating that he will have to seriously consider proposing this if public acceptance of Clipper does not increase.

No one has seriously suggested that the algorithm is insecure (although a method of using it which negates any value to law enforcement because of a minor design flaw (now corrected) received wide publicity [Markoff 1994]). But many do not completely trust the key escrow agents. Many suggestions have been made such as adding a third escrow agent from the private sector, or one from the judicial branch of government, or letting users pick whichever escrow agents they want, or having software manufacturers serve as the escrow agents, etc. Only recently has the government started seriously looking at some of these alternatives, possibly due to the cold reception generally accorded Clipper.

Clipper's encryption algorithm, "Skipjack", fits into Capstone, the U.S. government's long-term project to develop a set of standards for publicly available cryptography for use in voice and data communications. In one scenario, the government itself and all private companies doing electronic business with the government would be required to use Capstone, which could all be contained on a single computer chip. This would provide economies of scale but would also force users who wanted "government-proof" communications to superencrypt using other commercially available algorithms.

1.3. Export Control Reform

There is a large and growing collection of encryption software and hardware available around the world (see Figure 1). The October 1994 Software Publishers Association Foreign Availability Study turned up 870 products in 24 countries, 394 of which are manufactured outside the United States [SPA 1994]; roughly half of these use DES. Since with export controls, sales may be (and have been [Walker 1994]) lost to non-U.S. competitors with stronger encryption packages, one U. S. vendor has actually set up a completely independent cryptographic development lab overseas from which crypto products can be exported almost anywhere, including the United States.

Only recently have export controls been loosened a bit so traveling business executives can at least take their laptops overseas and encrypt information using the Data Encryption Standard [NBS 1977] without violating the export laws (*in theory* -- for a first-hand account of what actually happens when one tries to comply with this U. S. law, see [Blaze 1995]). There is some Congressional interest in abandoning many export controls on encryption, arguing that the economic needs outweigh the national security needs. The U. S. Commerce Department is currently studying this issue. They appear to be convinced of the foreign availability of strong (DES or "better") encryption, but are looking into how badly its nonexportability harms U. S. firms.

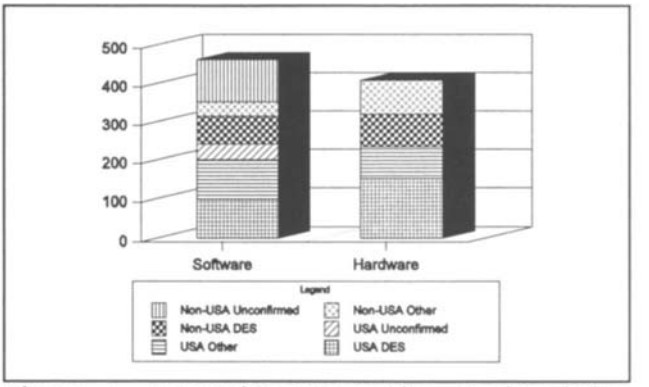

Figure 1. Worldwide Encryption Availability (Software Publishers Association, Oct. 1994)

2.0. Key Escrow Cryptosystems

Key escrow systems are those where part or all of the cryptographic keys are kept "in escrow" by third parties. The keys are released only upon proper authority to allow some person other than the original sender or receiver to read the message. The U. S. government is strongly supporting key escrow as a way to balance the needs for secrecy between communicating persons against the needs of law enforcement and national security agencies to sometimes read these encrypted communications (with proper legal authority).

2.1. U. S. Government Key Escrow

As of this writing, the U. S. Government's initial and only key escrowing suggestion is the Escrowed Encryption Standard [NIST 1994a] which defines a family of processors popularly known as Clipper chips. It uses the Skipjack algorithm which is classified but has been examined by a non-Government review team; this team had only a limited time to consider brute force attacks by exhaustive search, susceptibility to shortcut attacks, and the National Security Agency's design and evaluation process. Their interim report, the closest thing to a technical evaluation publicly available, concluded that [Brickell 1993]:

1. 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 the Data Encryption Standard today. Thus, there is no significant risk that SKIPJACK will be broken by exhaustive search in the next 30-40 years.

2. There is no significant risk that SKIPJACK can be broken through a shortcut method of attack.

3. While the internal structure of SKIPJACK must be classified in order to protect law enforcement and national security objectives, the strength of SKIPJACK against a cryptanalytic attack does not depend on the secrecy of the algorithm.

After this report was issued, Blaze described potential problems with Clipper that this review team failed to mention [Blaze 1994], including two methods to avoid message interception by the government. While there are more effective ways of "beating the system" (like superencryption) which are well-known, this paper made front page news in the *New York Times* [Markoff 1994], sending shock waves across some policymakers' radar screens.

The U. S. Government hopes that the Capstone chip, which incorporates several government standards including Skipjack, will be widely used in both public and private sectors. It is being installed in "Fortezza" PCMCIA electronic boards and used for the Pre-message Security Protocol (PMSP) program for the security of the Defense Messaging System. It implements the Skipjack algorithm (for bulk data encryption), the digital signature algorithm as specified in the digital signature standard [NIST 1994b], a key exchange algorithm based on a public key exchange, and the secure hashing algorithm (NIST 1994c).

On July 20, 1994, Vice President Gore acknowledged some of the problems with Clipper and stated that "the Clipper chip is an approved federal standard for telephone communication and not for computer networks and video networks"; that he would like a "more versatile, less expensive system" with key escrow implementable in software, firmware or hardware, or any combination thereof" which "would not rely on a classified algorithm"; and that "there are many severe challenges to developing such a system" which "must permit the use of private-sector key escrow agents as one option". He promised [Gore 1994] to reassess the current relatively strict export control licensing regime based on the results of two government studies to be carried out in 1994 and 1995.

2.2. Alternatives

There are alternatives to Government Key Escrow. Micali has patented a process [Micali 1993] for building a "fair" cryptosystem that balances the needs of the Government and those of

the public and private sectors (U. S. patent no. 5,276,737 issued 4 January 1994). It appears to cover the Escrowed Encryption Standard (Clipper) and the U.S. government has negotiated with him a limited use license for state and federal law enforcement. Banker's Trust International has proposed a common key escrow system for government and commerce using unclassified algorithms, with users having public-private keys [Singh 1994]. Trusted Information Systems [Balenson 1994] has proposed two software-only designs for key escrow systems, one paralleling Clipper and one an improvement which is likely to be much more palatable to private organizations [Walker 1995]. The latter (see Figure 2) is really more properly called a (near) real-time emergency access system, since there is nothing in escrow and no escrow agent. The U. S. Government itself is actively examining alternatives [NIST 1993]. These generally avoid some of the practical problems associated with the official U.S. Government key escrow system [Denning 1994b].

Characteristic	*Clipper*	*Micali*	*TIS "Commercial Key Escrow"*
No. of escrow agents	2	N	none
Defined agents	Government (Administration)	Don't care	Corporate, government, or private data recovery center
Secure hardware	yes	no	no
Direct cost to end-user	US$25 (eventually)	$0	metered (possibly anonymous) phone call
Majority logic (K of N can allow access)	no	yes	yes
Can use public key systems	no	yes	yes
Allows law enforcement real-time access	yes	It depends	It depends
Secrets kept at	central site	central site	user machine
Other properties	???	yes	yes

Figure 2. (Near) Real-Time Emergency Systems

3.0. Law Enforcement and Civil Liberties Issues

Some assert [Denning 1994c] that the Clipper Chip initiative strikes the proper balance between individual and organizational needs for secret communications with our common need for public safety and monitoring of criminal and terrorist activities. Civilized life is a compromise

and everything has honest costs [Gelernter 1994]. But people disagree on these "honest costs". While most expert testimony submitted to the government opposed both Clipper and current export controls and while the public comments by organizations and individuals were 318-2 against the initiative [Levy 1994], the government decided that the arguments on the other side were more compelling; it never issued the report on Clipper it promised when announcing the initiative in April 1993.

This ongoing communications gap and lack of trust between the federal government (especially the national security agencies with their closed culture) and much of the computer community and the media poisoned the Clipper discussions for a long time. Indeed, one local trade publication questioned why the National Security Agency (NSA), supposedly not involved in domestic issues, has taken such an active role in advocating Clipper as a national encryption standard; it effectively stated that "the agency is breaking the law" [Brendler 1994]. But if, as many (especially in the national security community) argue, key escrow systems represent "the last chance to protect personal safety and national security against a developing information anarchy that fosters criminals, terrorists and foreign foes" [Levy 1994], shouldn't these and other systems be examined more closely, and by a broader range of people?

In fact, this is what is happening. The debate has now shifted from relatively arcane technological details to the policy matters. A broad policy review is now being carried out by the National Research Council. One important outcome of this should be "the development of more open processes to determine how cryptography will be deployed throughout society in support of electronic delivery of government services, copyright management, and digital commerce" [OTA 1994]. This report will not be ready until 1996. Walker suggests that is too long a time and that if the problem is not resolved by using "commercial key escrow" as opposed to "government key escrow", and soon, the opportunity will be lost to limit the expansion of incompatible product-by-product solutions. He thinks that if governments continue to "study the problem", a plethora of cryptographic mechanisms will be put into computing software, and that this will seriously damage law enforcement and national security interests [Walker 1995].

Should anyone be able to develop and disseminate encryption technology or should it be "born classified"? Diffie is concerned about the effect of a *secret* cryptographic standard on individual rights and technology development [Diffie 1993] and on innovation in the computer and communications industries. He states that the public (not government) cryptographic community has been the principal source of innovation in cryptography; he does not want to hobble this innovation. He has urged that all aspects of Clipper be made public, not only to expose them to public scrutiny but also to guarantee that once made available as standards they will not be prematurely withdrawn by an all-powerful agency. He observes that "law, technology, and economics ... must all be kept in harmony if freedom is to be secure" and wants rights (such as that to have a private conversation) recognized by law to be supported rather than undermined by technology.

The American Civil Liberties Union (ACLU), reacting to the announcement of the Clipper

Chip proposal, expressed a concern that the rights protected under the First, Fourth, and Fifth Amendments of the U. S. Constitution (freedom of speech; no unreasonable search and seizure, warrants with particulars; no self-incrimination or private property taking) may be violated. They also assert that the present system of export controls on cryptography is unconstitutional, a point apparently agreed with by an assistant attorney general in a 1978 government memo [Harmon 1978].

Froomkin sees the issue as less clear, however. As he points out, "the rights of private non-commercial users appear to be a distressingly close question given the current state of civil rights doctrine and the great importance that the courts give to law enforcement and national security." [Froomkin 1994]

To show that the public welfare may indeed be threatened by too much and too good cryptography available to the general public, we point out an example of the criminal sophistication that is possible with today's technology: the undetectable electronic crime [Von Solms 1992]. Is the scepter of enough of these so likely and so threatening that diminution of some other civil liberties is warranted?

Because of these concerns, a bill (H. R. 5199) was introduced in the 1994 U. S. Congress to regulate "voluntary encryption standards" for privacy, security, and authenticity of domestic and international electronic communications. Its key features include:

- The Secretary of Commerce will establish an Encryption Standards and Procedures Program conducted by the director of the National Institute of Standards and Technology. The Secretary will be authorized to conduct research, make grants, and enter into agreements.

- Any encryption standard put forward by the Secretary shall meet the following requirements: ensure confidentiality, integrity, or authenticity of electronic communications; advance the development of the National Information Infrastructure (NII); contribute to public safety and national security; preserve existing privacy rights; preserve the functional ability of government to interpret electronic information lawfully obtained; be implementable in software, firmware, or hardware.

- Standards shall be developed in consultation with the Attorney General, the Federal Bureau of Investigation, the National Security Agency, and other federal agencies. The Computer System Security and Privacy Advisory Board shall review any standard before issuance.

- Nothing in [this act] shall be construed to require the use of such standards.

- Key escrow agents may be established by the President. Each escrow agent will be a federal agency that is competent to the administer the program and is not a federal agency authorized by law to conduct electronic surveillance.

- The key escrow agent may only disclose the keys to an authorized government entity and that entity may only use the keys for the purpose expressly provided for in the court order. Foreign entities may have access to the keys if the President determines that it would be in the national security interests of the United States.

- The Secretary of Commerce shall conduct a public hearing every three years on the program and then submit a report to Congress.

The Electronic Privacy Information Center of Washington welcomed this first attempt to "bring encryption standards setting under the rule of law", but proposed several changes [EPIC 1994] including improving citizen privacy by either creating a privacy agency or by taking away the special status for pre-issuance review of proposed encryption standards that the FBI, NSA, and the Attorney General have under this draft; providing a proper and public risk assessment of the government's key escrow policy (see also [Hanson 1994]); and transferring key escrow responsibility from the executive branch to the judicial branch of government so that the regulators report to different persons than the regulated.

4.0 Export Policy: Prudent Controls in a Risky World?

The United States Government continues to impose rigid controls on the export of encryption software and hardware products, despite evidence that the policies governing the issuing of export licenses inhibit U.S. businesses' ability to compete in the foreign marketplace -- a marketplace that already offers encryption software and hardware that incorporates the very standards that U.S. businesses cannot export because of export controls.

Exports of cryptographic software and hardware are controlled by the U.S. Department of State and the U.S. Department of Commerce. The State Department uses the International Traffic in Arms Regulations (ITAR) which include the "Munitions List"; this list enumerates munitions material for which export licensing is required; encryption materials are included in Category XIII. Commerce Department requirements are set forth in the Export Administration Regulations and the Commerce Control List. The National Security Agency (NSA) has a very strong voice in these decisions [Hoffman 1994].

Walker [Walker 1994] describes importing several DES products and notes the "frustrating and somewhat humorous" incident in which NIST posted source code for DES to the Internet without an export restriction notice and it was immediately copied by computers in Denmark, the United Kingdom, and Taiwan. As he points out, FIPS 181 (which contains the DES source code)

now "is available from hosts throughout the world along with the notice that export from the U. S. is in violation of U. S. export controls."

Complying with export regulations is daunting, and a manufacturer who is exporting software or having foreign nationals develop it could unwittingly run afoul of U. S. law [Christensen 1993] That's what may have happened to Phil Zimmermann, the author of Pretty Good Privacy (PGP), who has come under pressure from the U. S. government for the unregulated distribution of strong encryption. A federal grand jury in San Jose, California is examining whether he broke laws against exporting encryption codes. He says a friend, who he refuses to identify, put PGP on the Internet. Zimmermann's lawyer says his client could face charges carrying a prison sentence of up to 51 months. [Bulkeley 1994] Miller, in a fundraising appeal for the Phil Zimmermann Defense Fund posted to a number of newsgroups, claims that the government also hopes to establish the proposition that posting a cryptographic program on a bulletin board system or on the Internet is the same as exporting a "munition" [Miller 1994].

There are two conflicting U. S. government rulings on the legality of exporting cryptographic information. In the first, the Department of State [Harris 1994] ruled that export of a diskette with source code for high quality cryptography is prohibited, even though export of the same source code printed in a book is allowed (even in this day of inexpensive scanners!). The second [Harmon 1978] is a Justice Department memorandum to the Science Advisor to the President, stating that "the present ITAR licensing scheme does not meet constitutional standards". This memorandum concluded that "a prepublication review requirement for cryptographic information might meet First Amendment standards if it provided necessary procedural safeguards and precisely drawn guidelines." Apparently, an informal system of prepublication review instituted in 1981 [PCSG 1981] has worked well for the publication of cryptographic papers. A broad-based committee of the Association for Computing Machinery has written that "As far as the research community has been concerned, it is fair to say that there have been no long-term chilling effects." [Landau 1994].

Charles A. Hawkins, Jr., Acting Assistant Secretary of Defense (C3I) summarized the encryption policy issue very well in a memo for the U.S. Deputy Secretary of Defense on May 3, 1993. He correctly observed that encryption policy is not a technological issue:

> Trapdoor encryption technology is not essential to the debate since a system that required the escrow of keys by users of cryptographic technologies could be established even if the trapdoor chips did not exist. Proposed use of trapdoor technology does raise a further complication: neither the academic community nor private industry is comfortable with encryption algorithms that are kept secret, as will be the case with the trapdoor chip. It has been suggested that an independent panel of cryptography experts will be invited to evaluate the algorithm. This will not reassure the community at large that there are no unrecognized vulnerabilities, since the panel will be perceived as captive and tainted.

5.0. Summary

We are just starting to deal with the thorny technological, political, and administrative issues raised by modern cryptography. This survey has discussed these issues and provided pointers to the original source material. It will be a challenge to address the issues in a timely manner and an open fashion, but this must be done if we are to develop a rational cryptography policy..

REFERENCES

[Balenson 1994] Balenson, D. M., Ellison, C. M., Lipner, S. B., and Walker, S. T., "A New Approach to Software Key Escrow Encryption" in [Hoffman 1995].

[Beth 1992] Beth, T., Frisch, M., and Simmons, G. (Eds.), 1992, Public Key Cryptography: State of the Art and Future Directions, *Lecture Notes in Computer Science 578*, Springer-Verlag, 1992.

[Blaze 1994] Blaze, M., "Protocol failure in the escrowed encryption standard", *Proceedings of the 2nd ACM Conference on Computer and Communications Security*, Fairfax, VA, November 1994 (reprinted in [Hoffman 1995]).

[Blaze 1995] Blaze, M., "My life as an international arms courier", comp.risks, January 6, 1995.

[Brassard 1989] Brassard, G., Modern Cryptology. *Lecture Notes in Computer Science 325*, Springer-Verlag, New York, 1989.

[Brendler 1994] Brendler, B., 'Secret' Agency Steps Over the Line, *Washington Technology*, February 10, 1994 (reprinted in [Hoffman 1995]).

[Brickell 1993] Brickell, E. F., Denning, D. E., Kent, S. T., Maher, D. P., and Tuchman, W., "SKIPJACK Review: Interim Report", posted to sci.crypt, August 1, 1993 by Dorothy Denning (reprinted in [Hoffman 1995]).

[Bulkeley 1994] Bulkeley, W. M., "Genie is Out of the Bottle", *Wall Street Journal*, April 28, 1994, p. 1 (reprinted in [Hoffman 1995]).

[Christensen 1993] Christensen, L. E., "Technology and Software Controls" in *Law and Policy of Export Controls: Recent Essays on Key Export Issues*, August 1993, pp. 3-33 (reprinted in [Hoffman 1995]).

[Denning 1994a] Denning, D., "The U. S. Key Escrow Encryption Technology", *Computer Communications 17*, 7 (July 1994), Butterworth-Heinemann Ltd., Linacre House, Jordan Hill, Oxford, OX2 8DP, United Kingdom (reprinted in [Hoffman 1995]).

[Denning 1994b] Denning, D. and M. Smid, "Key Escrowing Today", *IEEE Communications*, September 1994.

[Denning 1994c] Denning, D., Testimony before the U. S. House of Representatives Subcommittee on Technology, Environment, and Aviation of the Committee on Science, Space, and Technology, May 3, 1994 (reprinted in [Hoffman 1995]) .

[Diffie 1976] Diffie, W. and Hellman, M. E., "New Directions in Cryptography", *IEEE Transactions on Information Theory IT-22*, pp. 644-654, 1976.

[Diffie 1993] Diffie, W., "The Impact of a Secret Cryptographic Standard on Encryption, Privacy, Law Enforcement and Technology", Hearings before the Subcommittee on Telecommunications and Finance of the Committee on Energy and Commerce, U. S. House of Representatives, 103rd Congress, 1st Session, April 19 and June 9, 1993. Serial No. 103-53, pp. 111-116 (reprinted in [Hoffman 1995]).

[EPIC 1994] Electronic Privacy Information Center, Statement on Wiretap Bill, October 8, 1994 (reprinted in [Hoffman 1995]).

[Froomkin 1994] Froomkin, A. M., "The Constitutionality of Mandatory Key Escrow -- A First Look", in [Hoffman 1995].

[Gelernter 1994] Gelernter, D., "Wiretaps for a Wireless Age", *The New York Times,* Section 4 Op-Ed, May 8, 1994, (reprinted in [Hoffman 1995]).

[Gore 1994] Gore, A., Letter to Hon. Maria Cantwell, July 20, 1994 (reprinted in [Hoffman 1995]).

[Hanson 1994] Hanson, R., "Can Wiretaps Remain Cost-Effective?", *Communications of the ACM 37*, 12 (December 1994), pp. 13-15.

[Harmon 1978] Harmon, J. M., "Constitutionality Under the First Amendment of ITAR Restrictions on Public Cryptography", Memorandum to Dr. Frank Press, Science Advisor to the U. S. President, May 11, 1978 (reprinted in [Hoffman 1995]).

[Harris 1994] Harris, M., letter to Philip R. Karn, Jr., October 7, 1994 reaffirming determination on cryptographic export media (reprinted in [Hoffman 1995]).

[Hesse 1990] Hesse, C., "Enlightenment Epistemology and the Laws of Authorship in Revolutionary France, 1777-1783", *Representations 30*, Spring 1990, University of California, Berkeley.

[Kahn 1967] Kahn, D., *The Codebreakers*, MacMillan Co., New York, NY, 1967.

[Hoffman 1993] Hoffman, L. J., "Clipping Clipper", *Communications of the ACM 36,* 9 (September 1993), pp. 15-17.

[Hoffman 1994] Hoffman, L. J., Ali, F. A., Heckler, S. L., and Huybrechts, A., "Cryptography Policy", *Communications of the ACM 37,* 9 (September 1994), p. 109ff.

[Hoffman 1995] Hoffman, L. J. (ed.), *Building in Big Brother*, Springer-Verlag, New

York, NY, 1995.

[HR4922] H. R. 4922, "Digital Telephony and Communications Privacy Improvement Act of 1994", (reprinted in [Hoffman 1995]).

[Landau 1994] Landau, S., Kent, S., Brooks, C., Charney, S., Denning, D., Diffie, W., Lauck, A., Miller, D., Neumann, P., Sobel, D., Codes, Keys, and Conflicts: Issues in U. S. Crypto Policy, June 1994. Available from Association for Computing Machinery, New York. Chapter on "Cryptography in Public: A Brief History" reprinted in [Hoffman 1995].

[Levy 1994] Levy, S., "The Cypherpunks vs. Uncle Sam", *The New York Times Magazine,* June 12, 1994 (reprinted in [Hoffman 1995]).

[Markoff 1994] Markoff, J., "Flaw Discovered in Federal Plan for Wiretapping", *The New York Times*, June 2, 1994, page 1.

[Micali 1993] Micali, S., Fair Cryptosystems, Laboratory for Computer Science, Massachusetts Institute of Technology, Cambridge, Mass., MIT/LCS/TR-579.b, November 1993 (reprinted in [Hoffman 1995]).

[Miller 1994] Miller, H., REVISED: Zimmermann Defense Fund Appeal, Article 8319 of talk.politics.crypto, December 22, 1994.

[NBS 1977] National Bureau of Standards, "Data Encryption Standard", FIPS PUB 46, Washington, D. C., January 1977.

[NIST 1993] National Institute of Standards and Technology, Opportunity to Join a Cooperative Research and Development Consortium to Develop Secure Software Encryption with Integrated Cryptographic Key Escrowing Techniques, *Federal Register, Notices, vol. 58,* no. 162, August 24, 1993.

[NIST 1994a] National Institute of Standards and Technology, Escrowed Encryption Standard, Federal Information Processing Standards Publication 185, U. S. Department of Commerce, 1994.

[NIST 1994b] National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication XX, May 19, 1994, Gaithersburg, Md. (reprinted in [Hoffman 1995]).

[NIST 1994c] National Institute of Standards and Technology, Secure Hash Standard (SHS), Federal Information Processing Standards Publication 180, May 11, 1994, Gaithersburg, Md. (reprinted in [Hoffman 1995]).

[OTA 1994] Office of Technology Assessment, U. S. Congress, *Information Security and Privacy in Network Environments,* 1994.

[PCSG 1981] Public Cryptography Study Group, 1981, Report of the Public Cryptography Study Group, American Council on Education, February 1981.

[Rivest 1990] Rivest, R. L., "Cryptography" in J. van Leeuwen (ed.), *Handbook of Theoretical Computer Science*, MIT Press/Elsevier, Amsterdam, 1990.

[Singh 1994] Singh, M., "Key Escrowing: How It Really Works Today and Tomorrow", *Data Security Letter 54*, November 1994, Trusted Information Systems, Inc., Glenwood, Md.

[SPA 1994] Software Publishers Association, Encryption Products Database Statistics, October 1994. Available from Trusted Information Systems, Inc., Glenwood, Md. and from http://www.seas.gwu.edu/seas/instctsp/crypto-survey.html

[von Solms 1992] von Solms, S. and Naccache, D., "On Blind Signatures and Perfect Crimes", *Computers and Security 11*, 6 (1992), Elsevier Science Publishers Ltd., (reprinted in [Hoffman 1995]).

[Walker 1994] Walker, S. T., "Testimony Before the United States Senate Committee on the Judiciary Subcommittee on Technology and the Law", May 3, 1994, reprinted in [Hoffman 1995].

[Walker 1995] Walker, S. T., Lipner, S. B., Ellison, C. M., Branstad, D. K., Balenson, D. M., "Commercial Key Escrow: Something for Everyone Now and for the Future", Trusted Information Systems, Inc., Glenwood, Md., January 3, 1995.