SCHOOL OF LAW
CASE WESTERN RESERVE UNIVERSITY

Health Matrix: The Journal of Law-Medicine

Volume 9 | Issue 2

1999

# Stopping Science: The Case of Cryptography

David Banisar

# STOPPING SCIENCE: THE CASE OF CRYPTOGRAPHY

*David Banisar*[†]

**SINCE THE END OF WORLD WAR II**, the United States government has attempted to limit the development and availability of publicly available cryptography in order to preserve and enhance its ability to monitor communications anywhere in the world. This effort had been led by the super-secretive National Security Agency (NSA). In the last decade, it has been aided by the Department of Justice and the Federal Bureau of Investigation, which has taken the lead in arguing for new laws restricting domestic development and use. Together the agencies have been successful in setting government policy towards surveillance in the face of Congressional and public opposition. To limit cryptography, the agencies have lobbied for new laws, subverted standards processes, threatened academic and private cryptographers, used export control laws to influence domestic policy, and lobbied other governments and international organizations to create international restrictions. They have also eliminated or co-opted other agencies who are authorized to operate in this field. As computers and networks have become an essential part of modern life, this battle has become a major public policy issue.

By one measure, their actions have been successful – thus far, they have been able to delay the widespread adoption of encryption for over twenty years. However, the effectiveness of their powers are ending. Due to the Internet, demand for cryptography to protect privacy and ensure security has exploded while distribution using the Internet has made it possible to send or receive strong cryptography from nearly anywhere in the world in seconds.

[†] The Author is an attorney in the Washington, D.C. area, specializing in privacy and freedom of information law. He is a senior fellow at the Electronic Privacy Information Center (http://www.epic.org) in Washington, D.C. and Deputy Director of Privacy International (http://www.privacyinternational.org). He is co-author, with Bruce Schneier, of THE ELECTRONIC PRIVACY PAPERS: DOCUMENTS ON THE BATTLE FOR PRIVACY IN THE AGE OF SURVEILLANCE (John Wiley & Sons, 1997). He is a 1993 graduate of The Columbus School of Law, the Catholic University of America and is a member of the Maryland Bar. Some portions of this Article previously appeared in THE ELECTRONIC PRIVACY PAPERS.

In the past few years, many foreign companies have sprung up. American companies and independent researchers are developing and making available new programs each day. Other governments have rejected the U.S. approach and are relaxing controls. The international consensus is now against the United States.

## I. WHAT IS CRYPTOGRAPHY?

Cryptography provides a means of accomplishing two crucial functions – encryption and authentication. Encryption is the process of encoding or "scrambling" the contents of any data or voice communication with an algorithm (a mathematical formula) and a randomly selected variable associated with the algorithm, known as a "key." Only the intended recipient of the communication, who holds the key, can decrypt and access the information. The key is essentially a string of numbers; the longer the string, the stronger the security.[1]

The authentication capabilities of cryptographic systems involve the use of "digital signatures." A digital signature is a cryptographically based assurance that a particular document was created or transmitted by a given person. It thus provides a means of authenticating the integrity of electronically transmitted data and the identity of the sender, much as a handwritten signature verifies the authenticity of a paper record. Digital signatures also provide for the "non-repudiation" of electronic data – the inability to deny the authenticity of the transmitted information. As the world moves toward increased reliance on electronic communications, the importance of such capabilities is apparent.

Emerging computer and communications technologies are radically altering the ways in which we communicate and exchange information. Along with the speed, efficiency, and cost-saving benefits of the "digital revolution" come new challenges to the security and privacy of communications and information traversing the global communications infrastructure. As the National Research Council's Committee to Study Cryptography Policy (NRC Committee) noted, the threat to personal privacy is substantial:

[1] The Author would like to thank David L. Sobel of EPIC for providing this section. *See generally* BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY (2d ed. 1996) (explaining the function of the "key" in cryptography). *See, e.g.*, Philip R. Zimmermann, *Cryptography for the Internet*, SCI. AM., Oct. 1998, at 110 (describing the lack of privacy in electronically sent information and how well-designed cryptography systems can provide better protection).

> Increasing reliance on electronic commerce and the use of networked communication for all manner of activities suggest that more information about more people will be stored in network-accessible systems and will be communicated more broadly and more often, thus raising questions about the security of that information.[2]

Communication and information stored and transmitted by computers can be protected against interception through the use of cryptographic security techniques. Electronic communications are now widely used in the civilian sector and have become an integral component of the global economy. Computers store and exchange an ever-increasing amount of highly personal information, including medical and financial data. Communications applications such as electronic mail and electronic fund transfers require secure means of encryption and authentication – features that can only be provided if cryptographic technology is widely available and unencumbered by government regulation.

## II. STRATEGY 1: SUPPRESSION AND CONTROL

The NSA has long attempted to suppress discussion, development, and dissemination of encryption. It has used various tactics including intimidating academic researchers, misapplying laws, eliminating research funding and competing government agencies, and pressing for legislation that would ban its use.

The NSA has long opposed discussing cryptography. This is perhaps best exemplified in a 1992 letter opposing a proposal for hearings on cryptography: "[T]he National Security Agency has serious reservations about a public debate on cryptography."[3]

### A. Born Classified

Over the past half-century in the United States, there has been an ongoing debate about military efforts to control the dissemination of unclassified technical, scientific, and economic information, including cryptography. The military and intelligence com-

[2] National Research Council, Cryptography's Role in Securing the Information Society, at 41 (Kenneth W. Dam & Herbert S. Lin eds., 1996) [hereinafter NRC Report] (explaining individual and personal interests in privacy in the information age).

[3] Letter from J.M. McConnell, Vice Admiral, U.S. Navy, Director of National Security Agency, to Willis H. Ware, Chairman, National Computer System Security and Privacy Advisory Board (July 23, 1992) (on file with Author) (establishing the NSA's concern that public debate over cryptography will jeopardize national security interests).

munity has tried to control this information, arguing that its dissemination threatens the national security.[4] In opposition, the scientific community has argued that there must be a free flow of information to promote scientific inquiry and that the military should not have the power to determine what should be publicly available. As Congressman Jack Brooks noted in 1966:

> Since it is a natural tendency of DOD [the Department of Defense] to classify everything, it would be impossible for the department to strike an objective balance between the need to safeguard information and the need to maintain the free exchange of information.

As computers became more commonplace in the 1970s, academic and corporate interest in encryption strongly increased. Programs in encryption and computer security as a specialty of computer science sprang up at universities across the United States. These programs were spurred by the growing realization of the need to protect the massive amount of personal and proprietary information that was being computerized. This rapid increase in public interest did not go unnoticed by the NSA. Under the leadership of Director Bobby Ray Inman, the NSA began efforts to limit public development and dissemination of encryption.

One of its first targets was the funding of academic research. NSA employees began suggesting to their National Science Foundation (NSF) counterparts that the NSA had exclusive control over the funding of encryption research. In 1977, the NSA directly approached Fred Weingarten, Director of the Division of Computer Research of the NSF, and told him that federal law gave NSA complete control over cryptography. Weingarten, after consulting with NSF's lawyers, challenged the NSA's claim. The NSA backed off, offering to "review" NSF grant proposals. The NSF agreed, with the stipulation that the NSA would only review the technical merits of the proposals.

In 1978, the NSA tried a different strategy. It began aggressively using the 1951 Invention Secrecy Act[5] to attempt to classify cryptography products that were designed by non-government re-

[4] *See, e.g.*, Harold C. Relyea, *Silencing Science: National Security Controls and Scientific Communication* (1994) (discussing how the rapid development of science has caused an increase in the availability of various types of information and how various groups struggle for control over such information).

[5] 35 U.S.C. §§ 181-88 (1994) (establishing the government policy and procedures for denying access to inventories viewed as posing national security risks, as well as setting penalties for violating the stated policy).

searchers. Previously, the Act had only been applied to government researchers and those who had signed secrecy orders prior to conducting research. The Act allows the Patent Office to forward applications to government agencies which have an interest in the subject area. The agencies can then classify the proposal if they determine that it threatens national security. The person who receives the note is ordered not to discuss the patent again. Violators can be fined $10,000, and imprisoned for two years.

The first targets who went public were Professor George Davida of the University of Wisconsin and free-lance researcher Carl Nicolai. They had both filed for patents on encryption devices. Nicolai had created a simple analog voice encryption device that he planned to sell for $100. Davida had developed an encryption device for the high speed encryption of networks. After the classifications were made public, the NSA rescinded the orders, calling them "mistakes."

At the same time it was cracking down on outside research, the NSA also worked to limit any competition from inside the government. In 1977, President Carter signed Presidential Directive/NSC 24 (PD-24) to improve telecommunications protections for government-derived, unclassified information which may be of value to a foreign adversary after revelations that Soviet agents were eavesdropping on major U.S. telephone links, including Washington and New York.[6] The Directive appointed the Defense Department to protect "government-derived classified information and government-derived unclassified information which relates to national security" while the Commerce Department was assigned the task of protecting "government-derived unclassified information," and assisting the private sector with protecting its information. But when a division of the Department of Commerce began to investigate public cryptography, NSA Director Inman began to attack because he "perceived an unwillingness on the part of the [Commerce Department] to 'recognize the legitimate role of NSA.'"[7] He began to push for the elimination of Commerce's role and the merging of classified and unclassified measures under the control of the NSA. Eventually, after intense lobbying from Inman,

[6] *See* David Burnham, *New Unit Seeks to Prevent Russians from Spying on U.S. Phone System*, N.Y. TIMES, Mar. 26, 1979, at A16 (explaining that the Special Project Division was created to encourage businesses and federal agencies to protect information that could be useful to a potential enemy).

[7] George F. Jelen, *Information Security: An Elusive Goal*, 1985 PROGRAM ON INFO. RESOURCES POL'Y II-64 (discussing the unwillingness of the Commerce Department to admit that national security concerns existed).

funding was cut drastically in 1982, and the Commerce Department's Special Projects Division that was in charge of civilian computer security was eliminated.

In 1979, Inman began a public campaign to promote restrictions. At the Armed Forces Communications Electronics Association conference, Inman gave the first-ever public speech by an NSA Director. He called encryption dangerous and called for limitations on the public dissemination of encryption saying, "there is a very real and critical danger that unrestrained public discussion of cryptographic matters will seriously damage the ability of the government to conduct signals intelligence."[8] He demanded that an "accommodation" must be reached with the NSA over private sector research and development in cryptography. Finally, Inman called for limitations on other types of technical data.

Inman's efforts were quickly criticized by the scientific community. The American Association for the Advancement of Science (AAAS) passed a resolution condemning the restrictions:

> Whereas freedom and national security are best preserved by adherence to the principles of openness that are a fundamental tenet of both American society and the scientific process, be it resolved that the AAAS opposes governmental restrictions on the dissemination, exchange, or availability of unclassified knowledge.[9]

Inman followed this up by asking the American Council on Education, an association representing 1400 universities in the United States, to create a Public Cryptography Study Group in 1983 to examine the issue of limits on academic research of encryption.

Inman asked the panel to review the "acceptability of restrictions on domestic dissemination of non-governmental technical information relating to cryptography."[10] The panel rejected the suggestion. Instead, it voted to recommend that researchers voluntarily provide their research to the NSA. Today, almost no cryptographers except those with relationships with NSA submit their papers.

[8] For text of the Inman speech, see BRUCE SCHNEIER & DAVID BANISAR, THE ELECTRONIC PRIVACY PAPERS: DOCUMENTS ON THE BATTLE FOR PRIVACY IN THE AGE OF SURVEILLANCE 297 (1997) [hereinafter ELECTRONIC PRIVACY PAPERS].

[9] *Id.*

[10] *Id.*

## B. NSDD-145: The National Security Information State

With the election of Ronald Reagan in November 1980, the debate over controls on scientific information intensified. The new administration favored restricted access to information. As part of that effort, the NSA began to push again to take over computer security and encryption.

In April 1982, President Reagan signed Executive Order 12,356 on the classification of national security information. It eliminated the requirement that there be balancing of national security and public interests before information could be classified. In 1984, Reagan approved National Security Decision Directive NSDD-145, which expanded the security classification system to include "sensitive, but unclassified data."[11] The term was broadly defined as "information the disclosure, loss, misuse, alternation, or destruction that could adversely affect national security or other Federal Government interests."[12] The directive was based on the assumption that aggregating unclassified information could affect national security and, therefore, those systems should be controlled by the military.

NSDD-145 gave the NSA broad authority over computer security, including cryptography. A 1992 internal NSA memorandum bluntly stated: "In 1984, NSA engineered a National Security Decision Directive, NSDD-145, through the Reagan Administration that gave responsibility for the security of all U.S. information systems to the Director of NSA, removing NBS from this."[13] The NSA was appointed to "act as the government focal point for cryptography, telecommunications systems security, and automated information system security . . . to conduct, approve or endorse research" and to "review and approve all standards, techniques, systems and equipment."[14] It was given authority to "prescribe the minimum standards, methods and procedures for pro-

[11] NSDD-145 Sept. 1984, *National Policy on Telecommunications and Automated Information Systems Security* (replaced by NSD-42, *National Policy for the Security of National Security Telecommunications and Information Systems* (U) July 5, 1990).

[12] SCHNEIER & BANISAR, ELECTRONIC PRIVACY PAPERS, *supra* note 8, at 299.

[13] Memorandum from Clinton C. Brooks, Special Assistant to the Director of the National Security Agency (Apr. 28, 1992), *available at NSDD-145 and the Computer Security Act* (visited Mar. 14, 1999) <http://www.epic.org/crypto/csa/brooks.gif> (discussing a bill proposed by then-Chairman of the House Government Operations Committee, Rep. Jack Brooks, to reassert the responsibility of the National Bureau of Standards (NBS) in this area).

[14] SCHNEIER & BANISAR, ELECTRONIC PRIVACY PAPERS, *supra* note 8, at 299.

tecting cryptographic and other sensitive technical security material, techniques, and information."[15] Using these broad grants of authority, the NSA and other intelligence agencies attempted to expand their control over security and access to nonmilitary computer systems, both within the federal government and in the private sector.

In 1986, National Security Advisor Admiral John Poindexter issued an additional directive, NTISSP 2, extending the scope of NSDD-145 to include even more information.[16] The definition of information under its jurisdiction was extraordinarily broad:

> Sensitive, but unclassified information is information the disclosure, loss, misuse, alteration, or destruction of which could adversely affect national security or other Federal Government interests. National security interests are those unclassified matters that relate to the national defense or the foreign relations of the U.S. Government. Other government interests are those related, but not limited to the wide range of government or government-derived economic, human, financial, industrial, agricultural, technological, and law enforcement information, as well as the privacy or confidentiality of personal or commercial proprietary information provided to the U.S. Government by its citizens.[17]

The two directives together were used as authority for the NSA and the CIA to visit private companies and organizations that held "sensitive" information, including LEXIS/NEXIS, DIALOG, CompuServe, and banks. Mead, which owned LEXIS/NEXIS at the time, eventually purged from its system all the technical data obtained from the National Technical Information Service because of the visits. The directive was also reportedly used to justify an NSA investigation of the computer software used to count votes in the 1984 Presidential election.

By 1984, many members of Congress believed that legislative action would be necessary to resolve the conflict between the efforts of the military and the NSA to restrict information and the

[15] *Id.*

[16] National Policy on Protection of Sensitive, but Unclassified Information in Federal Government Telecommunications and Automated Information Systems (NTISSP 2) (Oct. 29, 1986), *reprinted in* SCHNEIER & BANISAR, ELECTRONIC PRIVACY PAPERS, *supra* note 8, at 367-70 (stating the manner in which sensitive information should be handled by federal departments and agencies).

[17] *Id* at 368.

civilian interest in the free flow of information. House Government Operations Chairman Jack Brooks expressed the sentiment of the Congress in his opening statement to hearings held in 1987: "these actions reflect an unprecedented expansion of the military's influence into our society, which is unhealthy politically and potentially very dangerous."[18]

After several unsuccessful attempts at passage, and against strong lobbying by the NSA, Congress enacted the Computer Security Act of 1987.[19] The Congress made clear its intent that there should be a separation of authority for classified and unclassified information security, including cryptography. The House Science, Space, and Technology Committee report noted that "the Committee felt it is important to pursue a legislative remedy to establish a civilian authority to develop standards relating to sensitive, but unclassified data."[20] The National Institute of Standards and Technology (NIST) (formerly the National Bureau of Standards (NBS)), a division of the Department of Commerce, was given "responsibility within the federal government for the developing of technical, management, physical, and administrative standards and guidelines for the cost-effective security and privacy of sensitive information in federal computer systems."[21] NBS was allowed to request technical assistance from NSA, at the discretion of the NBS.

With the enactment of the Computer Security Act, NSA again faced a challenge to its control over computer security and cryptography. Shortly after the law went into effect, NSA began efforts to undermine it with the support of NIST leadership. In March 1989, NIST Acting Director Raymond Kammer signed a Memorandum of Understanding with NSA which delegated to NSA

[18] *Computer Security Act of 1987, Hearings Before a Subcommittee of the Committee on Government Operations*, 100th Cong. 2 (1987) (statement of Jack Brooks, Chairman, House Government Operations) (suggesting that the balance between the need to protect national security and the need to pursue advanced technologies would be better determined via public hearings).

[19] Computer Security Act of 1987, Pub. L. No. 100-235, 101 Stat. 1724 (1988) (codified with some differences in language at 15 U.S.C. § 2789-3, 4 (1997) (establishing a computer standards program, government-wide computer security, and training for those in security matters) [hereinafter CSA].

[20] H.R. REP. NO. 100-153(I), at 22 (1987), *reprinted in* 1987 U.S.C.C.A.N. 3120, 3137 (reporting favorably on and recommending a bill providing for a computer standards program within the NBS, government-wide computer security, and training in security matters for those involved with federal computer systems).

[21] SCHNEIER & BANISAR, ELECTRONIC PRIVACY PAPERS, *supra* note 8, at 302.

many of the responsibilities that Congress had assigned to NIST once again placing NSA in the dominant role in setting standards.[22] The General Accounting Office testified in 1989 that:

> The document as a whole . . . allows such prerogatives to NSA as it seems to me go a long way towards nullifying any initiative that NIST might undertake to which NSA would at the same time object . . . . The memo to me does not project the full sense that it is NSA that will be responsive to NIST. Rather, it suggests that where there is any disagreement between NIST and NSA, that it will be NSA that keeps its hands on the levers of control.[23]

These concerns were later shown to be prophetic.[24]

### C. "Operation Root Canal": The FBI Joins the Fight

In 1991, the FBI joined the campaign to limit cryptography. The FBI convinced Senator Joseph Biden (D-DE) and Congressman Tom Lantos (D-CA) to introduce a "Sense of Congress" provision into several pending bills that encouraged telephone companies to provide law enforcement officials with the decrypted copies of encrypted communications of their subscribers.[25] In his remarks for the Congressional Record, Senator Biden described the purpose of the provision: "[I]t encourages electronic communications equipment providers to design such equipment to allow law en-

[22] Memorandum of Understanding Between the Director of the National Institute of Standards and Technology and the Director of the National Security Agency Concerning the Implementation of Public Law 100-235 (Mar. 1989), *available in Memorandum of Understanding* (Mar. 1989) (visited Apr. 9, 1999) <http://www.epic.org/crypto/csa/nist_nsa_mou.html>. *See also* SCHNEIER & BANISAR, ELECTRONIC PRIVACY PAPERS, *supra* note 8, at 302-03.

[23] *Military and Civilian Control of Civilian Computer Security Issues: Hearing Before the Subcommittee on Legislation and National Security of the House Committee on Government Operations*, 101st Cong. 37-38 (1989) (statement of Milton J. Scolar, Special Assistant to the Comptroller General, U.S. General Accounting Office) (discussing the issue of "the degree to which the responsibilities vested in the NIST under the act [were being subverted] by the role assigned to the NSA under the Memorandum").

[24] *See* Strategy 2: Subverting Standards, *infra* § III.

[25] The provision stated that "[i]t is the sense of Congress that providers of electronic communications services and manufacturers of electronic communications service equipment shall ensure that communications systems permit the government to obtain the plain text contents of voice, data, and other communications when appropriately authorized by law." Comprehensive Counterterrorism Improvement Act of 1991, S. 266, 102d Cong., § 2210 (1991). *See also* SCHNEIER & BANISAR, ELECTRONIC PRIVACY PAPERS, *supra* note 8, at 308.

forcement agencies, when duly authorized by law, to more easily conduct surveillance activities."[26]

Industry and civil liberties groups strongly and publicly opposed this proposal, arguing that it would have limited the development and dissemination of cryptography and force telephone companies to act as agents of the FBI. The provision was withdrawn in June 1991.[27]

At this point, the NSA began assisting the FBI with its efforts to enact legislation banning communications systems that did not have built-in surveillance capabilities. A September 1991 memo from the Justice Department described the objective as: "[t]o obtain approval of a strategy and legislation which will enable law enforcement real-time access to communications, whether encrypted or not."[28] This project was code-named "Operation Root Canal" by the FBI.

The early drafts of the digital wiretap legislation banned the use of any encryption not approved by NIST. A July 1991 memo described the new procedures as "[d]irect[ing] NIST to develop its standards under the Computer Security Act and other standards which for the first time would apply to the private sector . . . to be consistent with the objectives of this Act." [29] A later draft required that all encryption products be registered with the Federal Communications Commission and meet standards established by the National Institute of Standards and Technology "as a condition for use in connection with a communications system or service operated in the United States."[30]

In late 1991, the Department of Justice (DOJ), the NSA, and the CIA met to discuss legislative proposals, including encryption. They agreed that the encryption provisions were "controversial"

[26] 137 CONG. REC. S1190, S1191 (daily ed. Jan. 24, 1991) (statement of Sen. Biden) (introducing S. 266, the Comprehensive Counterterrorism Act of 1991, providing a detailed fact sheet containing section-by-section analysis of the bill).

[27] *See* SCHNEIER & BANISAR, ELECTRONIC PRIVACY PAPERS, *supra* note 8, at 139 (discussing a provision which encouraged telephone companies "to provide greater assistance to law encryption-related problems").

[28] Memorandum from Dan Levin, U.S. Department of Justice, Office of the Deputy Attorney General, to Kier Boyd et al. (Sept. 2, 1991), *available in* 1996 EPIC CRYPTOGRAPHY AND PRIVACY SOURCEBOOK, at C-5 (1996) (providing meeting notes discussing the objective of obtaining approval of a strategy which will enable law-enforcement real-time access to communications).

[29] Memorandum on Communications and Law Enforcement Legislation (July 8, 1991) (on file with Author) (providing draft legislation entitled "Communication and Law Enforcement Act").

[30] Memorandum on Digital Wiretap Legislation (Jan. 31, 1992) (on file with Author) (providing a draft of untitled legislation).

and would have to wait for another year.[31] In December 1991, National Security Advisor Brent Scowcroft submitted a memo to President George Bush recommending that he approve the digital wiretap proposal.[32] A month later, Bush approved the plan. In a memo sent to Secretary of Defense Dick Chaney, Attorney General Barr, and CIA Director Gates, Scowcroft noted that, "[s]uccess with digital telephony will lock in one major objective; we will have a beachhead we can exploit for the encryption fix; and the encryption access options can be developed more thoroughly in the meantime (TS)."[33]

In June 1992, an interagency group made up of the FBI, NSA and NIST was set up at the request of the FBI Director.[34] The FBI pushed to develop a "national cryptography policy."[35] By this time, the agencies recognized that banning encryption was politically volatile, "[a]ll parties deemed this alternative not to be a viable approach."[36] At a July meeting, the group agreed that more information was necessary to develop a policy.[37] A NIST representative who wrote up a summary of the meeting recognized that the FBI's desires for monitoring were problematic, writing, "[m]ore information [is necessary] on the FBI's 'real time' requirement. The closer 'real time' becomes to instantaneous, the more draconian and intrusive the solution becomes."[38]

The FBI, the DOJ, and the NSA pushed hard for a ban on other forms of encryption. In a briefing document sent to the National Security Council in February 1993, the FBI, the NSA, and the DOJ argued that:

> Technical solutions, such as they are, will only work if they are incorporated into all encryption products. To en-

[31] SCHNEIER & BANISAR, ELECTRONIC PRIVACY PAPERS, *supra* note 8, at 309.

[32] *Id.*

[33] Memorandum from Brent Scowcroft, National Security Advisor, to Dick Cheney, Secretary of Defense et al. (Jan. 17, 1991). *Id.* at 160.

[34] *See* Lynn McNulty, Memorandum for the Record (Aug. 18, 1992), *available in* 1996 EPIC CRYPTOGRPAPHY AND PRIVACY SOURCEBOOK, at C-14 (summarizing the July 1992 meetings of the interagency group created to develop a national encryption policy).

[35] *Id.* (developing a framework policy that would serve the public interest in general cryptographic security while protecting national security and law enforcement).

[36] *Id.* at C-17 (finding that the government must recognize the need for commercial encryption technology).

[37] *See id.* at C-18 (discussing the areas in which additional information is needed before conclusions can be drawn).

[38] *Id.* at C-19.

> sure that this occurs, legislation mandating the use of Government-approved encryption products or adherence to Government encryption criteria is required.[39]

Another FBI memo argued that, "[a] national policy embodied in legislation is needed which . . . [i]nsures cryptographic devices and systems . . . [which] are capable of real-time decryption by law enforcement . . . [and] [p]rohibits cryptography that cannot meet the Government standard."[40]

The panel presented its conclusions to the President, Vice-President, and the National Security Council in a report issued in late November 1993. At that point, the National Security Council rejected the banning of encryption as being politically unfeasible.[41]

Behind the scenes, however, the FBI continued to develop legislation to require that all encryption systems be readable by the government. Starting in March 1995, FBI Director Louis Freeh began meeting with members of Congress and testified before several Congressional committees to discuss how the "encryption problem" had to be solved. After the Oklahoma City bombing,[42] Freeh stepped up his efforts even more and began publicly calling for restrictions on the use of encryption, groundlessly claiming that the Oklahoma City bombing could have been stopped, even though none of the suspects was under surveillance prior to the incident and none used encryption.

Reporter Brock Meeks wrote in May 1995 that draft legislation

[39] SCHNEIER & BANISAR, ELECTRONIC PRIVACY PAPERS, *supra* note 8, at 311. *See also Encryption: The Threat, Applications and Potential Solutions* (visited Mar. 3, 1999) <http://www.epic.org/crypto/ban/fbi_dox/mandatory.gif> (showing scanned copy of the briefing document provided to the National Security Council).

[40] Federal Bureau of Investigation, *Impact of Emerging Telecommunications Technologies on Law Enforcement* (visited Apr. 9, 1999) <http://www.epic.org/ crypto/ban/fbi_dox/impact_text.gif> (encouraging legislation to control domestic encryption products by ensuring that law enforcement will have decryption capabilities, while affording protection to legitimate users).

[41] *See Nationalize an Industry* (visited Apr. 9, 1999) <http://www.us.net/softwar /nsa.html> (containing a brief, entitled *Impacts of Telecommunications and Encryption Technology on Law Enforcement and Intelligence Collection: Assessment, Options, and Recommendations*, which discusses the design of "a microelectronics chip that would provide high quality encryption while still enabling government decryption" and maintains that the encryption chip is "only a partial solution" to the privacy issue).

[42] On April 19, 1995, Timothy McVeigh and Terry Nichols, both subsequently tried and convicted, detonated a bomb outside the Murrah Federal Building in downtown Oklahoma City killing 169 men, women, and children.

was being proposed to require key escrow.[43] Meeks cited a draft proposal which was floated in March, describing a strategy to eliminate competition by mandating all systems be certified before use.[44] Meeks quoted one government official as admitting the difficulty in introducing the proposal to the public: "We all know what a bitch this is going to be trying to sell it to the selling public."[45] Following that lead, in June 1995, Senator Charles Grassley introduced a bill to restrict access to encryption software on the Internet and promoted weakened forms of encryption by making it unlawful to "distribute computer software that encodes or encrypts electronic or digital communications to computer networks that the person distributing the software knows or reasonably should know, is accessible to foreign nationals and foreign governments" unless the program "used a universal decoding device or program that was provided to the Department of Justice prior to the distribution."[46] Industry and public interest groups overwhelmingly criticized the bill. Even the Justice Department withdrew its support of the measure, claiming that it had nothing to do with its introduction.

In September 1997, the FBI tried again. Several Congressional committees approved a law that would have relaxed the export controls on encryption. At the behest of the law enforcement and intelligence agencies, two committees, the House Intelligence Committee and the House National Security Committee, approved amendments that would ban the use of encryption in the United States without government approval. The agencies also put heavy pressure on the House Commerce Committee to approve a similar amendment. There was a furious scramble as phone companies, computer companies, civil liberties groups, and the public lobbied the Committee to reject the amendment after it appeared that it would be approved. The Committee reversed its support and approved the bill without the amendment. The bill later died in the House Committee because of pressure by the FBI on House Rules Committee Chairman Gerald Solomon.

So far, attempts to take over the field of encryption or ban encryption that cannot be decrypted by government agencies have

[43] Brock N. Meeks, *Jacking in From the Narco-Terrorist Encryption Port* (visited Apr. 9, 1999) <http://www.epic.org/crypto/ban/cyberwire.html> (admonishing the government for legislation banning private encryption).

[44] *Id.*

[45] *Id.*

[46] The Anti-Electronic Racketeering Act of 1995, S. 974, 104th Cong. § 1030A (banning certain acts involving computers in the furtherance of crimes and providing an affirmative defense to prosecution).

been unsuccessful because of public opposition. Ironically, many of their attempts have had a reverse effect, with the controversy generating more interest in the issue and causing more development of encryption devices rather than less.

## III. STRATEGY 2: SUBVERTING STANDARDS

A second strategy to limit cryptography has been the efforts of the NSA and FBI to manipulate the development of technical standards to facilitate their demands for surveillance. They have successfully controlled normally independent and open government standards-setting bodies. Traditionally, standards developed by the National Institute of Standards and Technology are developed in an open and public process which allows for full public comment and input. Interested parties in government, industry, and academia submit proposals and comments. NIST acts as an independent arbitrator choosing the best system and making it a standard that can then be used by all. Open standards are considered very important in the telecommunications and computer field so that the standard will be acceptable to those who must adopt it. Secrecy may also undermine the security of the mechanism. Under traditional standards setting procedures for computer security, a standard is made public so that a large number of researchers are able to examine it for flaws using different approaches. In 1993, the General Accounting Office determined that, "[a]lthough the Computer Security Act of 1987 reaffirmed NIST's responsibility for developing federal information-processing standards for the security of sensitive, unclassified information, NIST follows NSA's lead in developing certain cryptographic standards."[47]

### A. The Data Encryption Standard

The NSA's efforts to interfere with the standards process began with the development of the first public government encryption standard, the Data Encryption Standard (DES). In 1972, the National Bureau of Standards, after several years of study, decided to create a new encryption standard for protecting unclassified government information which could also be used by the private

[47] Communications Privacy – Federal Policy and Actions, GAO/OSI-94-2, 3 (Nov. 1993), *also available at Communications Privacy – Federal Policy and Actions* (visited Apr. 9, 1999) <http://www.epic.org/crypto/reports/GAO_comm_privacy.html>, at 2 (discussing government roles in maintaining encryption programs developed to combat economic espionage).

sector.

IBM submitted its Lucifer algorithm, a symmetric key encryption system with a 128-bit key that was already being used by Lloyds Bank in its networks.[48] At the insistence of the NSA, IBM reduced the key size by over half to fifty-six bits and also revised some of the internal workings, known as the "S-Boxes." The NSA changes prompted a public debate about the role of the NSA in developing the standard. In response to public criticism, the NSA issued a terse written statement which said, "IBM designed the algorithm. NSA evaluated the algorithm for the NBS. Key length is adequate for the application."

In July 1977, NBS formally adopted the modified Lucifer algorithm as the official U.S. Data Encryption Standard (DES).[49] From the perspective of the NSA, the controversy must have been considered successful. The controversy discouraged many companies from adopting the standard. Many including CitiBank and Banker's Trust opted for propriety standards. The reduction of the key size also reduced the future use of the DES.

Not satisfied with weakening the DES, the NSA began to discourage publicly its use a few years later. In a 1986 letter to the NBS, the NSA stated that the widespread use of DES "could motivate a hostile intelligence organization to mount a large scale" attack and recommended that it only be used for financial services.[50] As a suggested replacement, the NSA announced two programs for manufacturers to develop NSA-certified cryptography in which the NSA would provide secret algorithms in tamper-proof chips to "approved companies" that implemented them into larger systems.

Industry organizations strongly opposed this effort because they feared handing over too much control of their banking and communications networks to the NSA. It was widely assumed that if the NSA built these systems, it would be able to read all communications that used them. In addition, because of the classified algorithms, there were severe limitations on the use of the devices. They could not be used outside the United States, which posed a

[48] A symmetric key encryption system is one that requires the same key to encrypt and decrypt.

[49] *See generally* Encryption Algorithm for Computer Data Protection, 40 Fed. Reg. 12,134 (1975) (describing accepted encryption algorithm and soliciting comments on behalf of the NBS).

[50] Letter from Gerald R. Young, Deputy Director for Plans and Policy, National Security Agency, to Director, Institute for Computer Sciences and Technology, National Bureau of Standards (June 1987) (on file with Author) (expressing concern that the Data Encryption Standard could be an attractive intelligence target).

major problem for the international banking industry. The banking industry also opposed the proposal because it had invested a large amount of money implementing DES and was concerned about compatibility.

The NBS ignored the NSA suggestion and reauthorized DES as an official government standard for another five years. Again, from an NSA perspective, the controversy must have been considered successful, as it discouraged many companies from adopting the standard. Cheryl Helsing of the American Bankers Association testified: "Our industry has lost valuable momentum in adopting improved security technology, and it still remains to be seen if we can overcome the damage that has been done to the perceived security of DES-based technologies."

Today, DES remains a federal standard, but few believe that it is secure because of the short key length. In a contest sponsored by RSA Data Security in January 1999, the Electronic Frontier Foundation, an advocacy group, cracked a DES encrypted message in twenty-one hours using a combination of a machine built for $300,000 and a network of computers attached to the Internet. Had the NSA not interfered with its creation, the standard would have lasted for at least another twenty years. Now many companies are using an unapproved version of DES that effectively doubles the key length until a new national standard is developed.

### B. The Digital Signature Standard

A second battle for standards erupted in the early 1990s with efforts by the National Institute of Standards and Technology to replace DES with a new algorithm that would provide for encryption and digital signatures. In 1989, as its first action under the Computer Security Act, NIST began working on a new public key encryption standard to protect unclassified, sensitive information held by government agencies and multinational corporations. This proposal began in secret under the auspices of a NIST/NSA Technical Working Group. NIST initially intended to use RSA, a system already in wide use by industry, but the NSA opposed the choice. NSA opposition caused conflicts at the Technical Working Group (TWG) meetings. At the January 31, 1990 meeting of the TWG, NIST representatives expressed frustration with the process: "It's increasingly evident that it is difficult, if not impossible, to reconcile the concerns and requirements of the NSA, NIST, and the general public though using this approach."[51] The FBI also began to pressure NIST. Soon after, FBI representatives joined the working group.

The NSA and the FBI put intense pressure on NIST to adopt an NSA-designed system that only provided for signatures. In an October 19, 1990 memo, the NSA showed its determination to force NIST to adopt its system: "[NSA Assistant Director] Clint [Brooks] has agreed to arrange a meeting with [Acting NIST Director] Ray Kammer to present our entire package . . . . If Kammer does not accept our proposal, we will have to consider escalating the problem."[52] In April 1991, Kammer committed NIST to adopting the NSA Digital Signature Standard (DSS) proposal. The FBI was blunt about their success in preventing a confidentiality standard from being released, describing the DSS as a "stalking horse for subsequent release of an encryption/interface standard."[53] A 1992 memo from FBI Director William Sessions to Attorney General William Barr trying to gather support for the proposal stated, "[NIST's] . . . efforts in support of a digital signature standard (the first phase of our strategy to address the encryption issue) must be re-energized."[54]

In August 1991, NIST publicly announced the DSS.[55] The role of the NSA was not uncovered until Computer Professionals for Social Responsibility initiated a Freedom of Information Act lawsuit against NIST to force disclosure of background documents.[56]

[51] Memorandum for the Record from the NIST/NSA Technical Working Group (Jan. 31, 1990) (on file with Author) (noting concerns expressed during the twelfth meeting of the TWG).

[52] Memorandum from the National Security Agency (Oct. 19, 1990) (discussing efforts to gain support for the NSA's proposed standards from the NIST). *See* SCHNEIER & BANISAR, ELECTRONIC PRIVACY PAPERS, *supra* note 8, at 305.

[53] Memorandum from the Federal Bureau of Investigation entitled *Digital Telephony: The Threat and the Issues* (Oct. 1, 1994) (discussing the congressional, digital, and industrial atmosphere surrounding the use of encryption technology and the effect of the technologies on the ability of the FBI to conduct voice, data, and image surveillance). *Id.* at 306.

[54] Memorandum from William Sessions, Director of the Federal Bureau of Investigation, to William Barr, United States Attorney General (May 26, 1992) (discussing key initiatives in compelling the telecommunication industry to cooperate with the FBI's proposed digital signal standard). *Id.* at 208-10.

[55] *See* A Proposed Federal Information Processing Standard for Digital Signature Standard (DSS), 56 Fed. Reg. 42,980 (1991) (proposing a specified "public-key based digital signature algorithm (DSA) appropriate for Federal digital signature applications").

[56] *See* David L. Sobel, *Government Restrictions on the Development and Dissemination of Cryptographic Technologies: The Controversy over the Digital Signature Standard,* 16 COMPUTER LAW REP. 265, 267-68 (1992) (arguing that the NSA's

Both the public and various industry groups reacted very negatively to the proposed standard. Over one hundred companies, trade associations, and individuals submitted comments. Although many people were encouraged that NIST was finally releasing something after ten years of inaction, nearly every public comment opposed the proposed standard. The comments noted a number of problems, including the lack of privacy protection, incompatibility with the industry standard RSA algorithm, the NSA role in designing the algorithm, and several technical problems. Even some government agencies were critical of the standard. The Department of the Treasury and the IRS threatened to adopt the stronger RSA system.[57] The Canadian government and the European Community both filed comments opposing the proposal because of the royalty agreements.

In May 1994, NIST announced the adoption of the DSS, even after the overwhelmingly negative comments from the public and the failure of the hashing algorithm.[58] NIST ignored the criticism, stating that "NIST considered all of the issues raised and believes that it has addressed them."[59]

### C. The Clipper Chip

The controversy over the Digital Signature Standard did not end with its adoption. Because the DSS lacked the ability to provide for confidentiality, an encryption system was still necessary. While the debate on the Digital Signature Standard went on publicly, the NSA and the FBI continued working behind the scenes on another proposal to introduce an encryption algorithm to replace DES that would protect private communications, but would allow government agencies to intercept and decrypt communications. The encryption ability was separated from the signature function at an early stage in the TWG meetings due to pressure from the NSA and the FBI.

involvement in the development of DSS is "contrary to Congress' intentions in enacting the Computer Security Act of 1987").

[57] *See* Letter from Steven Broadbent, Department of Treasury, to James Burrows, NIST (Feb. 4, 1992) (on file with Author).

[58] Approval of Federal Information Processing Standards Publication 186, Digital Signature Standard (DSS), 59 Fed. Reg. 26,208 (1994) (announcing that the Secretary of Commerce approved the Digital Signature Standard as one of the recognized Federal Information Processing Standards due to its "capability to generate digital signatures that cannot be forged").

[59] SCHNEIER & BANISAR, ELECTRONIC PRIVACY PAPERS, *supra* note 8, at 307.

By early 1991, the NSA had formalized its proposal. According to documents, the encryption algorithm, code-named "Skipjack," was developed by the NSA in 1985 for classified use. Under the NSA system, an NSA contractor would produce the chips, which would then be placed in commercial devices and sold to the public. The internal encryption key would be split up and handed over to two government agencies who would give it to intelligence and law enforcement agencies upon their request. The initiative was internally code-named "Clipper," a name that later became public at the insistence of the policymakers who adopted it over the opposition of the NSA "because they found it so convenient to use that it stuck."[60] A more sophisticated version to be used for computer communications, called the Capstone Chip, was also developed.

After the November 1992 election of William J. Clinton, discussions began immediately to get the new President's approval of the proposal. For political reasons, the decision to announce was held back for fear that the incoming administration would reject the proposal if it were publicly announced before the inauguration. The NSA and the FBI met with the new administration and other government agencies to convince them to support the proposal. The agencies focused their efforts on convincing Vice President Al Gore who had built a reputation in Congress on high-technology issues.

The Department of Justice and the NSA pushed manufacturers to adopt the standard. They expected to create a large enough market to make the Clipper a de facto standard.[61] AT&T agreed to support the Clipper Chip and drop its plans to sell its phone encryption device incorporating DES if the Justice Department agreed to buy 9,000 Clipper-enabled telephone scramblers from AT&T.

On April 15, 1993, President Clinton signed Presidential De-

[60] Letter from Clint Brooks, Special Assistant to the Director of the National Security Agency (Apr. 20, 1993) (entitled *Presidential Encryption Policy*, explaining where the internal encryption key got its name). *Id.* at 308.

[61] *See Technology and the Law: Privacy Issues in the Telecommunications Industry*, 1994: Hearing on the Administration's "Clipper Chip" Key-Escrow Encryption Program before the Senate Judiciary Subcommittee on Technology and the Law, 103rd Cong. (1994) (statement of Jo Ann Harris, Assistant Attorney General, Criminal Division, U.S. Department of Justice) (explaining that, due to the quality and strength of key-escrow encryption, the Attorney General's office expects the technology to be adopted by the private sector).

cision Directive 5 authorizing the Clipper initiative.[62] The directive ordered the Attorney General to "request manufacturers of communications hardware which incorporates encryption to install the U.S. Government Developed key-escrow microcircuits in their products."[63] Manufacturers could adopt other systems that were "equally effective in assuring both privacy and a secure key-escrow system."[64] The Attorney General was ordered to determine the key holders and set out procedures for their release. The Department of Commerce was ordered to begin the standards-setting process to procure and use the new encryption chip in "federal communications systems that process sensitive but unclassified information" within six months of the directive.[65] To make it more palatable to industry, the State Department announced it would relax export controls on products that contain Clipper Chips while maintaining controls on other encryption products. In addition, the NIST announced that it would not reapprove DES in 1998, leaving Skipjack as the only official government standard for protecting unclassified information.

The Clipper proposal immediately generated intense public opposition. A March 1994 *Time/CNN* poll of 1,000 people found that eighty percent of the public opposed the Clipper proposal when it was described to them.[66] An electronic petition organized by Computer Professionals for Social Responsibility (CPSR) asking President Clinton to withdraw the Clipper proposal gathered nearly 50,000 signatures, including many of the world's most prominent computer security and cryptography experts. Dozens of newspapers across the country wrote editorials against the Clipper proposal. Syndicated columnist William Safire, writing in the *New York Times* noted, "[w]ell-meaning law and intelligence officials, vainly seeking to maintain their vanishing ability to eavesdrop, have come up with a scheme that endangers the personal freedom

[62] Letter from William J. Clinton, President of the United States of America, on Public Encryption Management (Apr. 15, 1993) (explaining that the public encryption management directive, called the Clipper Initiative, would "assist law enforcement and other government agencies to collect and decrypt" legally collected, electronically transmitted information).

[63] SCHNEIER & BANISAR, ELECTRONIC PRIVACY PAPERS, *supra* note 8, at 312.

[64] *Id.*

[65] *Id.*

[66] *See* Philip Elmer Dewitt, *Who Should Keep the Keys?*, TIME, Mar. 14, 1993, at 90 (noting that two-thirds of people polled said "it was more important to protect the privacy of phone calls than to preserve the ability of police to conduct wire taps").

of every American."[67] *Business Week* asked, "[w]ill the Information Superhighway enable the federal government to become a high-tech snoop on a scale undreamt of in George Orwell's worst nightmares?"[68]

Surveys of industry and security experts found nearly unanimous opposition. In June 1993, the Computer Security System and Privacy Advisory Board held public hearings on the Clipper and heard testimony from dozens of corporations, industry associations, public interest groups, and interested individuals. Nearly all of the written and oral testimony presented to the Board was critical of the proposal. The Board recommended that the White House stop implementation of Clipper until a more extensive review of the proposal was conducted. Over 300 companies, industry and professional associations, public interest groups, and individuals responded to the NIST Federal Register notice asking for public comments while only two individuals supported the proposal.[69] Nearly all the commentators objected to the NSA role in the process and the implementation of a system in which the U.S. government held the keys. Privacy and security concerns were cited for the opposition. There was a widespread belief that at some point, a mandatory system would be imposed. Another major objection of the commentators was that the Clipper proposal reversed the usual presumption of open standards settings. For the first time, an NIST standard for computer security of public computer systems was totally classified. They also cited its incompatibility with industry standards such as RSA and the DES.

In February 1994, even after the overwhelming public opposition, the White House announced that it was formally adopting the Clipper as a "voluntary" government standard. The White House acknowledged that the plan was controversial. It brushed off the overwhelmingly negative comments, stating that since the standard was voluntary, "the Department of Commerce has found that notice and comment is unnecessary."[70] NIST Assistant Direc-

[67] William Safire, *Sink the Clipper Chip,* N.Y. TIMES, Feb. 14, 1994, at A17 (expressing fear that the federal government will be able to intrude upon the privacy of every American via the "Clipper Chip").

[68] *Don't Let Washington Play "I Spy" On You,* BUS. WEEK, Mar. 24, 1994, at 126 (asserting that the "Clipper Chip" will give the government enormous snooping power over American citizens).

[69] *See* Approval of Federal Information Processing Standards Publication 185, Escrowed Encryption Standard (EES) 59 Fed. Reg. 5,997 (1994) (giving information concerning the applicability, implementation, and maintenance of the standard, and a specifications section dealing with the technical requirements).

[70] SCHEIER & BANISAR, ELECTRONIC PRIVACY PAPERS, *supra* note 8, at 316.

tor Kammer stated in a Commerce Department press release that "[w]hile the vast majority of comments were negative, many reflected misunderstanding of skepticism about the administration's statements that the EES would be a voluntary standard."[71] The public comments reflecting concerns about privacy were also summarily rejected. "The Department of Justice has assured NIST that the Escrowed Encryption Standard is fully consistent with protection of individual privacy rights."[72] One Congressional staffer summed up the process as "a cynical sham given the outcome was predetermined by PDD-5" and suggested that the process was "apparently pointless except to occupy the public while they [the NSA] deployed the technology."[73]

Overall, the Clipper Chip was a spectacular failure. Only a handful were sold outside the Justice Department order. AT&T shut down its product line and laid off its workers because of the lack of sales and now only sells a non-escrow device based on a proprietary algorithm. Even many of the AT&T devices bought by the Justice Department reportedly sit unused in a warehouse. A similar fate befell the Capstone Chip, which was incorporated into smart cards, but was also widely rejected.

### D. Clipper With a Happy Face: Key Escrow and Key Recovery

With the failure of hardware-based key escrow systems, the NSA and NIST began wooing companies to develop a software encryption system that would provide the same access to keys as that by government agencies. The approach, called key escrow or key recovery, emphasized that the keys would be held by a "trusted third party" instead of a government agency and that the software would be designed by industry, rather than by the NSA. Industry was also encouraged to use the system because it would allow users to recover keys in case of accidents.

This approach was first introduced in an April 1994 letter from Vice President Al Gore to Congresswoman Maria Cantwell (D-WA) reaffirming the administration's position on key escrow encryption.[74] In July 1996, Vice President Gore officially announced the administration's software key escrow policy.[75] Under

[71] *Id.*

[72] *Id.*

[73] *Id.*

[74] *Id.* at 319.

[75] *Administration Statement on Commercial Encryption Policy*, July 12, 1996, (visited June 10, 1999) <http://www.epic.org/crypto/key_escrow/wh_cke_796.html>

the Gore announcement, a "framework based on a global key management infrastructure that supports digital signatures and confidentiality" would be implemented.[76] The proposal called for the encryption key to be "provided voluntarily by a computer user to a trusted party who holds it for safe keeping."[77] Export controls on software that used these parties would be relaxed. The administration stated that a growing consensus toward key escrow was emerging. The proposal was for a "voluntary" system but under various legal pressures, the end result would be to ban all individuals from the network who refused to give their keys to the certification/escrow authority.[78] Again, companies that made acceptable key escrow software would be allowed to export their software.[79]

Today, software key escrow is suffering the same fate as the Clipper Chip. Only a small market has emerged for the products. Virtually no individuals and few companies trust a third party to control their keys. International consensus is against escrow.[80]

Government efforts to subvert standards to prevent the proliferation of cryptography have been partially successful. The DES was weakened and is now no longer usable for protecting information of any level of sensitivity. The Digital Signature Standard is used by some companies, but it is incompatible with industry standards and its lack of a confidentiality function limits its use. The Clipper Chip is dead, but key escrow remains a main component of policy. The uncertainty caused by these battles has prevented the adoption of a single, strong system that can be used across many systems.

## IV. STRATEGY 3: EXPORT CONTROLS

A third tactic used by the U.S. government to limit cryptogra-

(explaining the importance of an encryption policy to the federal government and describing the value of the key recovery system of encryption).

[76] *Id.*

[77] *Id.*

[78] *Id.*

[79] Bruce W. McConnell & Edward J. Appel, *Executive Office of the President, Office of Management and Budget, Memorandum for Interested Parties* (visited Apr. 9, 1999) <http://www.epic.org/crypto/key_escrow/white_paper.html> (providing a draft paper entitled *Enabling Privacy, Commerce, Security and Public Safety in the Global Information Infrastructure*, which proposes export controls on key escrow software).

[80] *See Cryptography and Liberty 1998: An International Survey of Encryption Policy*, (Feb. 1998) (visited Aug. 27, 1999) <http://www.gilc.org/crypto/crypto-survey.html>.

phy both domestically and internationally has been imposing export controls on software and hardware that incorporate encryption. These are used to drive domestic policy by promoting products such as escrow, allowing their export and discouraging development of strong encryption by making it difficult to sell it overseas. The NSA has significant power over approvals on the export of cryptography. As noted by the General Accounting Office in 1993:

> NSA plays a major role in determining rules for exporting U.S. products with encryption capabilities. The scope of NSA's review is generally limited to those products and technologies whose export could affect the performance of NSA missions. The review affects such decisions as (1) whether individual products are placed on the more restrictive State-controlled "munitions list" or the less restrictive Commerce-controlled list and (2) whether particular products on the munitions list may be licensed for export.[81]

Since then, the rules have changed but the NSA is still in control.

Export controls reduce the availability of encryption in common programs such as operating systems, electronic mail, and word processors, especially from American companies. Companies are reluctant to develop two different product lines, one for domestic use that contains strong encryption and an international version with weaker encryption. The restrictions also make it difficult to develop international standards for encryption and interoperability of different programs. Countries must develop their own local programs which do not inter-operate well if at all with other programs developed independently in other countries. They may not be as secure because of a lack of peer-review. Companies and individuals are not as interested in developing programs because of smaller potential profits due to smaller markets.

U.S. export control rules are enforced by the U.S. Department of Commerce. The Export Administration Regulations (EAR) set forth comprehensive controls on exports of non-military commodities and information from the United States.[82] To export

[81] Communications Privacy – Federal Policy and Actions, *supra* note 47, at 3-4.

[82] The Regulations were originally promulgated by authority of the Export Administration Act (EAA), 50 U.S.C. App. §§ 2401-2420 (1991). The EAA has lapsed and has not been reenacted by Congress. The provisions of both the EAA and the Export Administration Regulations (EAR) have been kept in force since 1994 by

strong encryption software and technology anywhere except Canada, the exporter must first apply for and receive an individual license from the Commerce Department. Prior to 1986, encryption software and technology was controlled by the U.S. Department of State under the International Traffic in Arms Regulations (ITAR) where they were considered as munitions, and treated in the same way as machine guns or tanks.

"Export" is defined expansively under the Export Administration Regulations to include not only "actual shipment or transmission . . . out of the United States" or "release of technology or software in a foreign country" but also transfers or disclosures that take place entirely within the United States.[83] For encryption software, "export" includes making the software available on Internet sites or any other "communications facilities" that are merely accessible to persons outside the United States, unless certain onerous precautions are taken.[84] The discretion of the government to grant or deny the license is essentially unbounded. The Regulations provide only that "applications will be reviewed on a case-by-case basis" by the Commerce Department, in conjunction with several other agencies, to determine whether the export or reexport "is consistent with U.S. national security and foreign policy interests."[85] No definite time for a final decision is established, and judicial review is apparently unavailable.[86]

The controls on encryption have generated considerable controversy. American industry has strongly opposed the restrictions, citing the loss of hundreds of millions of dollars in sales to foreign competitors who offer similar products without restrictions. The National Research Council found in 1991 that, "[i]f the United States does not allow vendors of commercial systems to export security products and products with relatively effective security features, large multi-national firms as well as foreign consumers will simply purchase equivalent systems from foreign manufactur-

executive orders exercising the President's emergency powers under the International Emergency Economic Powers Act (IEEPA), 50 U.S.C. §§ 1701-06. *See* 63 Fed. Reg. 44,121 (1998) (continuing the state of national emergency declared by President Clinton due to the expiration of the Export Administration Act of 1979, and the failure by Congress to renew it). Exec. Order No. 12924, 59 Fed. Reg. 43,437 (1994) (continuing the export control regulations against unrestricted foreign parties in light of the expiration of the Export Administration Act of 1979, as amended).

[83] Export Administration Regulations, 15 C.F.R. § 734.2 (b)(1).

[84] *Id.* § 734.2(b)(9)(ii).

[85] *Id.* § 742.15(b).

[86] *See id.*

ers."[87] Indeed, many computer companies such as Network Associates, the producer of Pretty Good Privacy (PGP), and RSA Data Security, have set up foreign subsidiaries to sell encryption products worldwide.

In the past several years, the controls have led to several controversial cases over the abusive application of export controls to harass and to restrict free speech. In 1991, activist Phil Zimmermann released a free program called "Pretty Good Privacy" (PGP), which used the RSA algorithm for key exchange and a Swiss-designed algorithm, the International Data Encryption Algorithm, for encryption. Zimmermann wrote the program in response to the introduction of Senate Bill 266.[88] One of the users placed PGP on the Internet, making it available worldwide. Shortly after its release, a federal prosecutor in San Jose, California began investigating Zimmermann for violating the International Traffic in Arms Regulations (ITAR). Subpoenas were filed with companies that sold PGP and several members of the Internet activist community were questioned by the grand jury or by the prosecutors. Often they made the questions public, infuriating the prosecutor. The investigation dragged on for three years, prompting many to suggest that it was politically motivated to harass Zimmermann and prevent him from releasing new versions of his software. The investigation was finally dropped without comment in January 1996. The NSA has also used such controls to threaten manufacturers into modifying their products. According to the employees at the National Center for Supercomputing Applications, the NSA approached them in June 1995 and told them to remove the links for PGP and other encryption programs from the publicly available versions of Mosaic, a popular Internet browsing program. In 1996, NSA officials visited Sun Microsystems demanding they limit the security features of the new Java language.[89]

There are three constitutional challenges to the export control rules. Thus far, one federal court has ruled that export controls violate the First Amendment. All three cases are pending and it

[87] SYSTEM SECURITY STUDY COMM'N., NATIONAL RESEARCH COUNCIL, COMPUTERS AT RISK IN THE INFORMATION AGE 37 (1991) (clarifying export control criteria).

[88] Comprehensive Counterterrorism Improvement Act of 1991, *supra* note 23, at § 2201.

[89] *See* Ellen Messmer, *Sun to Feds: Keep Your Paws Off Java*, NETWORK WORLD, June 3, 1996, at 1, 15 (explaining why the NSA objects to the exportation of Sun's JavaSoft division technology, and why Sun believes the technology requires additional security features).

seems likely that the U.S. Supreme Court will make the final decision.

In February 1994, Phil Karn, an engineer from San Diego, applied for permission to export a treatise on cryptography entitled *Applied Cryptography*.[90] The request was granted by the State Department. When Karn applied to export the disk-based, electronic version a month later, the State Department denied the request, basing their decision on the rationale that ease of implementing the disk version made it different from the book. The author of the treatise, Bruce Schneier, believes that the basis for their decision can probably be attributed to the fact that "foreigners can't type."[91] Karn filed suit in September 1995. In March 1996, the U.S. District Court in Washington, D.C. dismissed the case, ruling that it was a "political question" which should be decided by the executive branch and Congress.[92] The court denied Karn's constitutional challenge, ruling that the regulations were "content neutral" and therefore did not infringe on free speech rights.[93] The D.C. Court of Appeals sent the decision back to the District Court following the 1996 changes to the export laws and it is in discovery phase now.[94] On February 18, 1999, Judge Louis Oberdorfer granted Plaintiff's request for an evidentiary hearing.[95]

A second case filed against the regulations came out with a different decision. In 1995, a University of California Ph.D. math student, Dan Bernstein, filed suit against the State Department and the NSA, challenging the constitutionality of the ITAR. Bernstein had applied for permission to export a cryptosystem he had invented called *Snuffle* which modified the Digital Signature Stan-

[90] *See* SCHNEIER, *supra* note 1.

[91] *The Applied Cryptography Case: Only Americans Can Type* (visited June 16, 1999) <http://people.qualcomm.com/karn/export/index.html>.

[92] *Memorandum Opinion of Charles R. Richey, United States District Court Judge*, (visited June 16, 1999), <http://people.qualcomm.com/karn/export/richey_dec-ision.html>.

[93] Karn v. United States Dep't of State, 925 F. Supp. 1, 9-11 (D. D.C. 1996) (holding that the government did not regulate the export of Karn's diskette because of its content, but rather was acting to prevent foreign intelligence sources from encoding the information). Because the rationale for the regulation was held to be content-neutral, the court did not presume it to be invalid. *Id.* Instead, the court determined that the regulation was justifiable as vital to national security interests.

[94] Karn v. United States Dep't of State, No. 96-5121, 1997 U.S. App. LEXIS 3123, at 2-3 (D.C. Cir. Jan. 21, 1997) (remanding the case "[i]n light of the recent Executive Order transferring regulatory authority of non-military cryptographic computer source code to the Commerce Department, and the Commerce Department's promulgation of a new regulation").

[95] *See The Applied Cryptography Case, supra* note 91.

dard to provide privacy protection. He also wanted to export accompanying documentation. Bernstein submitted a request with the State Department for a determination about whether the program and the documentation were controlled under ITAR, thus limiting him from publishing information about the program. After several months, the State Department ruled that nothing, including several non-technical papers, could be exported. Bernstein filed suit in 1995 challenging the constitutionality of the decision.

The State Department argued their rules regulated conduct, like the burning of draft cards, not speech, and therefore did not involve the First Amendment. In a substantially different analysis from the *Karn* decision, Judge Marilyn Patel initially ruled that the source code was protected by the First Amendment. Judge Patel ruled that, "[t]his court can find no meaningful difference between computer language, particularly high-level languages as defined above, and German or French . . . . Like music and mathematical equations, computer language is just that, language, and it communicates information either to a computer or to those who can read it."[96] The Judge ruled that the case could continue and upheld the preliminary decision in August 1997. The government appealed, and the case is now pending before the U.S. Court of Appeals for the Ninth Circuit.

In a third case, Peter Junger, a law professor at Case Western Reserve University Law School, proposed to include on his class information Web site the source code for "Fiddle," a software program he wrote, and also some other programs. Because the source code for each program included mathematical algorithms useful for encrypting information, in June 1997 Junger asked the Commerce Department for permission to make them available. The Commerce Department ruled that placing the programs on his Web site was considered to be an export and required their permission, which they then denied. Junger filed suit in September 1997 in the District Court for the Northern District of Ohio, arguing that the restrictions on publication of encryption software violated the First Amendment. The district court granted judgment to the government ruling that "[e]xport Regulations are constitutional because encryption source code is inherently functional, because the Export Regulations are not directed at source code's expressive elements,

[96] Bernstein v. United States Dep't of State, 922 F. Supp. 1426, 1435 (N.D. Cal. 1996) (finding that cryptographic computer code is a form of protected free speech and that government regulations restricting the use of this code could be challenged on a constitutional basis).

and because the Export Regulations do not reach academic discussions of software, or software in print form."[97] Junger has appealed the case and the U.S. Court of Appeals for the Sixth Circuit will hear oral arguments in a few months.

Moved by the reports of industry losses and lax security on the Internet, Congress has tried several times to relax the export controls. Each time they have faced considerable opposition from the White House and the NSA. However, each year that the proposals are introduced, they gain progressively more support.[98]

The Internet has significantly changed the effectiveness of export controls. Strong, unbreakable encryption programs can now be delivered in seconds to anywhere in the world from anywhere in the world with a network connection. It has been increasingly difficult for countries to limit dissemination, and once a program is released, it is nearly impossible to stop its redissemination, especially if it is in one of the many countries around the world with no export controls.

## V. STRATEGY 4: POLICY LAUNDERING: INTERNATIONAL EFFORTS TO RESTRICT ENCRYPTION

Over the past several years, the role of international organizations has become crucial in the development of encryption policies. These include the Organization for Economic Cooperation and Development (OECD), the European Union, NATO, the G-7/G-8, the Council of Europe, and the Wassenaar Arrangement. In all of these, the United States, with the support of the government of the United Kingdom, and occasionally the French and Australian governments, has led efforts to gain international support for restrictions. Opposition to their efforts has been led by Germany and the Scandinavian countries.

The United States has demanded that other countries adopt restrictions on cryptography, even though these restrictions are not supported in the United States. Using these proposed restrictions, the U.S. government has lobbied Congress for new domestic re-

[97] Junger v. Daley, 8 F. Supp. 2d 708, 712 (N.D. Ohio 1998) (holding that computer encryption software export regulations were constitutional because the export of encryption software source code was not sufficiently expressive to merit First Amendment protection).

[98] *See generally* Internet Privacy Coalition, *Latest News* (last modified Feb. 1, 1999) <http://www.crypto.org/> (providing current events page designed to "promote privacy and security on the Internet through widespread public availability of strong encryption and the relaxation of export controls on cryptography").

strictions, arguing that the rest of the world is adopting restrictions, so the United States must do so, too, to ensure that its laws are compatible. For the most part the United States has been unsuccessful in this effort. This has obviously been a clever effort at policy laundering.

## A. Organization for Economic Cooperation and Development

In 1995, the Organization for Economic Cooperation and Development (OECD), a Paris-based international body of twenty-nine countries, began work on developing cryptography guidelines. The OECD had previously developed well-respected guidelines on the privacy of personal information and computer security. The United States began pressuring the OECD to adopt key escrow and domestic restrictions as an international standard. Shortly after the OECD began the process, the key staff member who was the only person in the organization familiar with cryptography was mysteriously forced out and replaced with a junior attorney who had no experience in the subject. A U.S. Department of Justice attorney was also placed in the OECD to help develop the guidelines. The OECD also changed their previous traditional two-year process of consensus to a one-year accelerated process that included a "core group," led by the U.S. government, who were there to write the guidelines. At the meetings, the U.S. delegation, which was led by the Justice Department, the FBI, and the NSA, began to lobby the committee to adopt key escrow.

The OECD was severely divided by the proposals. The U.S. position was supported by France and the United Kingdom. The Japanese government, represented by their Ministry of Trade, was strongly opposed. The Scandinavian countries also announced that they were unhappy with the proposals, stating that the system would undermine trust. Denmark's representative announced that key escrow would not be included in a nation-wide card system. Industry representatives wanted to ensure that they would have the right to adopt any system of their choosing. The Canadian and Australian delegations demanded that a privacy principle be included.

In March 1997, the OECD issued its Guidelines on Cryptography Policy. The OECD Recommendation is a non-binding agreement that identifies the basic issues that countries should consider in drawing up cryptography policies at the national and international level. The OECD recommended that while governments may restrict encryption, they must take the basic principles of privacy and human rights into account before imposing restrictions. Since their adoption, many countries such as Ireland, Finland, and Canada have issued new cryptography policies without restrictions.[99] France reversed its previous restrictive policy in January 1999.[100]

## B. G7/G8

The Group of 8 (G-8) is made up of the heads of state of the top eight industrialized countries in the world.[101] The leaders have been meeting annually since 1975 to discuss issues of importance, including the information highway, crime, and terrorism.

In 1996, the United States began pressuring the G-7/G-8 to address cryptography. At their meeting in Lyon, France in 1996, the G-8 agreed to "[a]ccelerate consultations, in appropriate bilateral or multilateral fora, on the use of encryption that allows, when necessary, lawful government access to data and communications in order to, *inter alia*, prevent or investigate acts of terrorism, while protecting the privacy of legitimate communications."[102]

At the Denver Summit in June 1997, they decided "[t]o counter, *inter alia*, the use of strong encryption by terrorists, we have endorsed acceleration of consultations and adoption of the OECD guidelines for cryptography policy and invited all states to develop national policies on encryption, including key, management, which may allow, consistent with these guidelines, lawful government access to prevent and investigate acts of terrorism and to find a mechanism to cooperate internationally in implementing such policies."

At the Birmingham, England meeting in May 1998, the G-8 Ministers adopted a recommendation on ten principles and a ten-point action plan on high-tech crime that did not explicitly mention

[99] *See generally* Global Internet Liberty Campaign, *Cryptography and Liberty: An International Survey of Encryption Policy* (visited Apr. 9, 1999) <http://www.gilc.org/crypto/crypto-results.html> (providing results of a survey of countries' policies regarding controls and cryptogrtaphy).

[100] *See Interministerial Committee on the Information Society (CISI) – January 19, 1999: Decisions Taken* (visited Mar. 25, 1999) <http://www.premier-ministre.gouv.fr/GB/INFO/FICHE1GB.HTM> (outlining a number of new dispositions on encryption and protection of personal data presented to Parliament by the French government).

[101] The Group of Eight (G-8) is made up of the following countries: Canada, France, Germany, Great Britain, Italy, Japan, Russia, the United States, and the European Commission.

[102] Electronic Privacy Information Center, *G7-G8, Ministerial Conference on Terrorism*, Paris, July 30, 1996 (visited Aug. 31, 1999) <http://www.epic.org/privacy/terrorism/g7_resolutions.html>, at 11.

encryption. The ministers announced:

> We call for close cooperation with industry to reach agreement on a legal framework for obtaining, presenting, and preserving electronic data as evidence, while maintaining appropriate privacy protection, and agreements on sharing evidence of those crimes with international partners. This will help us combat a wide range of crime, including abuse of the internet and other new technologies.[103]

## C. The Wassenaar Arrangement

The United States has been somewhat successful in promoting restrictions though the extension of export controls. The main international agreement on export controls is the Wassenaar Arrangement. The Wassenaar Arrangement (WA) is an agreement by a group of thirty-three industrialized countries[104] to restrict the export of conventional weapons and "dual use" technology to certain other countries considered pariah states or, in some cases, those who are at war. Certain cryptographic products, along with other technology such as supercomputers and high-level computer security access software, are considered to be "dual use" in that they can be used for both commercial and military purposes.

The WA representatives largely represent the law enforcement, signals intelligence, and weapons control sectors of participant governments and have little appreciation for commercial or privacy concerns. The WA countries maintain export controls for the items on the agreed Control Lists, which are reviewed periodically to take into account technological developments. Decisions to amend the Control Lists, as with all WA decisions, are made by consensus, i.e., they must be unanimous. Participating states com-

[103] *G-8 Communique*, (visited Mar. 25, 1999) <http://www.gilc.org/crypto/g7/g8-birmingham-598.html> (summarizing the May 18, 1998 G-8 Meeting in Birmingham, England, which focused on economic growth and combating crime through the use of technological tools).

[104] Argentina, Australia, Austria, Belgium, Bulgaria, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Luxembourg, the Netherlands, New Zealand, Norway, Poland, Portugal, the Republic of Korea, Romania, the Russian Federation, the Slovak Republic, Spain, Sweden, Switzerland, Turkey, Ukraine, the United Kingdom, and the United States. *See* Wassenaar Export Control Regime (visited Mar. 25, 1999) <http://www.fas.org/spp/starwars/offdocs/s960712.htm> (reporting on the establishment of a new system to monitor and control exports of conventional arms and dual-use technologies).

mit to adjust their national export control policies to adhere to the WA Control Lists, but this commitment is discretionary in nature and is not mandatory. Participating States may adjust their cryptographic export policies through new regulations or legislation.

On December 3, 1998, the Wassenaar Secretariat announced that new cryptography guidelines had been added to the Arrangement. The Wassenaar Dual-Use Control List was extended to cover mass market software that contained encryption such as Web browsers, e-mail applications, electronic commerce servers, and telephone scrambling devices with strengths over 64-bits. These controls must be renewed and approved unanimously in two years, otherwise they will be canceled. The Wassenaar countries also agreed to control other software, for example, the kind that is used in specific sectors such as banking, insurance, and health – at the 56-bit level.

However, the United States did not get everything it wanted. According to a press release from the German Ministry of Economy, "[c]ertain states that had initially demanded special treatment for 'key recovery' products have not been successful. Thus, the export of encryption technology will remain possible without depositing keys with government agencies." Most importantly, and in what constitutes an important "loophole," the new WA controls do not apply to the "intangible" distribution of cryptography, including downloads from the Internet.

It remains to be seen what the effects will actually be on the flow of encryption products. Several countries such as Canada and Germany have indicated that they do not plan to impose new strict restrictions on exports of mass-market software. The Swiss government wrote:

> The upcoming minor revisions to Switzerland's export controls on cryptographic goods as a result of the December '98 changes to the Wassenaar Arrangement Lists of controlled goods and technology will not alter the liberal Swiss Cryptography Policy . . . . Switzerland will keep its efficient export permit process for cryptographic goods in order to encourage Swiss exporters to increase their sales and share worldwide while being mindful of national security interests.[105]

[105] Letter from Bernard Jaggy, First Secretary (Economic Affairs), Embassy of Switzerland, to Wayne Madsen, EPIC (Jan. 27, 1999) (on file with author) (providing

## VI. CONCLUSION

The efforts by the U.S. government over the last twenty years to stunt the widespread deployment of encryption both inside and outside of the United States have been successful. However, their effectiveness is now running out. Many factors are pushing in the opposite direction: the increased publicity because of the Clipper Chip and Digital Signature Standards prevents the adoption of more secret standards and any new proposal receives intense scrutiny; the increasing pressure by industry for adequate security for electronic commerce, and the globalization of trade make domestic controls increasingly tenuous. A ubiquitous international key escrow scheme has been rejected by other countries and the Internet effectively ends the use of export controls. The battle will continue for the foreseeable future because the stakes are too high for everyone, but the end of the era of crypto restrictions is near.

information on Switzerland's revised import/export controls on cryptographic goods in response to a request to update the 1998 report *Cryptography and Liberty*).