Private Locks, Public Keys and State Secrets New Problems in Guarding Information with Cryptography

Tom Ferguson

Program on Information Resources Policy

Harvard University
Center for Information Policy Research

Cambridge, Massachusetts

A publication of the Program on Information Resources Policy

PRIVATE LOCKS, PUBLIC KEYS AND STATE SECRETS New Problems in Guarding Information with Cryptography
Tom Ferguson
April 1982, P-82-5

Project Director: Anthony G. Oettinger

Tom Ferguson is a graduate student at the J. F. Kennedy School of Government.

The Program on Information Resources Policy is jointly sponsored by Harvard University and the Center for Informatiion Policy Research.

Printing 5 4 3 2

ACKNOWLEDGEMENTS

Special thanks are due to the following persons who reviewed and commented critically on drafts of this report. These persons and the Program's affiliates are not, however, responsible for or necessarily in agreement with the views expressed herein, nor should they be blamed for any errors of fact or interpretation.

Wilbur Alderson
John Cherniavsky
Howard Crumb
George Davida
Donald Davies
Harry B. DeMaio
Michael L. Dertouzos
W. Todd Furniss
Martin E. Hellman
Timothy Ingram
B. R. Inman
David Kahn
Wayne Kay
Mel Klein
Donald E. Kraft
Lee Merkhover
Donn B. Parker
Howard Rosenblum
Daniel Schwartz
Victor Walling
Charles K. Wilk
Eugene F. Yeates

Table of Contents

EXECUTIVE SUMMARY

Tom Ferguson, "Private Locks, Public Keys and State Secrets:
New Problems in Guarding Information with Cryptography"

A growing number of new cryptographic systems may have significance for both national security and commercial enterprise.

To date, government influence in both the development and application of public cryptography has not followed a clear path.

Work on these new coding schemes has raised new and difficult questions: Is the right of unrestricted inquiry into cryptography worth the potential national secuirty losses? Or, could national security be threatened if new developments in cryptography are kept from the private sector?

Among the factors behind the increased demand for private sector cryptography are: (1) the spread of computer networks and remote-access data processing; (2) the increasing value of information stored and tramsmitted by computer; and (3) the threat to privacy posed by computerized processing of personal data.

Within current research, two major events have dramatically increased public knowledge, discussion, and controversy about encryption technology: (1) the promotion of the Federal Data Encryption Standard (DES), and (2) research on a new range of enciphering techniques known as public-key cryptography.

The existing and future market for cryptographic products involves some unanswered questions: To what extent can the general technological improvement and growth in communications and computers be linked to growth in the use of encryption? What effect will govern policies and statutes have on the potential market and vice versa?

Key organizations and individuals, in and out of government, are in the process of shaping the policy discussions and establishing the procedures for modern cryptography. A series of informal meetings and talks between National Security Agency officials and academic cryptologists constitute the Public Cryptography Study Group. The Science Advisor of the White House has requested the Departments of Commerce and Defense to derive jointly the necessary elements of a national policy on cryptography.

Three possible future directions for cryptography are: (1) a more centralized development and application of civil sector cryptography under the umbrella of a single organization; (2) the creation of competing expertise by establishing a substantial communications security branch of government outside the military and intelligence community; and (3) a continuation of the irregular pattern visible today where federal regulation becomes less of a driving force than market conditions and privately developed standards.

Introduction

The range of secret codes and ciphers currently used to protect confidential information is noticeably broad. Any information can be regarded as confidential if its leakage to unintended parties is perceived as harmful by the confiders. With this definition, confidential information includes everything from the scrambled airwaves of subscription television to the communications transmitted over the Washington-Moscow "hot line."

But the secrecy systems used in these two examples differ as widely as their relative bearing on the national security. The hot line uses an unbreakable cipher, a one-time key for every message, that is so superior to any scheme used for pay television that the two are hardly comparable. But in between the Electronic Teleprinter Cryptographic Regenerative Repeater Mixer II once used by the White House[1] and the simple decoding boxes used on home televisions is an increasing number of new coding systems which could affect both national security and commercial enterprise.

Work on these new schemes, by academic and industrial scientists outside government, poses some new and difficult questions. Is the right of unrestricted inquiry into cryptography worth the potential national security losses? Published results might encourage foreign countries and competitors to create new and impenetrable codes, thereby hampering American foreign code-cracking activities and cutting off valuable intelligence information. On the other side of the coin, could national security be threatened if new developments in cryptography are kept from the private sector? Economic intelligence is becoming as valuable as military and diplomatic information; foreign powers could cause considerable damage by intercepting corporate mail, tampering with electronic fund transfer systems, or gaining access to confidential information in the grain and oil businesses.

To begin to address such questions, we examine the reasons behind the new demand for private sector cryptography. Then, the current research in the area is detailed, and the existing and future market for cryptographic products outlined. The analysis focuses on two major events which have dramatically increased public knowledge about encryption technology: the promotion of the Federal Data Encryption Standard and research on a new range of enciphering techniques known as public-key cryptography. An effort is made to identify the relevant organizations and individuals, in and out of government, whose interests and capabilities are shaping the policy discussions and establishing the procedures for coming to grips with the problems of modern cryptography.

The study will look at the new problems of cryptography arising in the private sector and their implications for government-related activities. It does not concentrate on the highly classified activities in cryptology that exist independent of commercial activity--such as the coding of communications channels for controlling nuclear weapons systems or the encryption of telephone conversations of high state officials. But, throughout the study, the analysis bumps into the unavoidable obstacles inherent in an open, public discussion of a matter that touches on some of the nation's most closely held secrets.

1. The New Need for Secrets

Computers and terminals are beginning to say more and more sensitive things to each other than ever before. And their conversations are no longer limited to military or diplomatic topics. Data communications now involve most major industries and consumer services--transmission lines carry information on everything from oil drilling sites and corporate pricing strategies to personal checking accounts. It follows that many of the data transmitted must be confidential; they should not be revealed to unauthorized personnel or altered or damaged during their passage through the communication network. Hence the need for security measures from locks on file cabinets to cryptography, the varied techniques used to put messages in secret form by code or cipher.

The general flow of computer technology from large-scale military and industrial uses to commercial and consumer applications is often reported.[2] The same engineering that went into missile guidance systems is now used for pocket calculators and electronic toys. And the flow of technology is not strictly one-way; there is evidence that some innovations in the consumer computer market are exceeding current military standards. For example, car makers now demand microchips whose quality and reliability must far exceed the performance of chips in missiles and satellites.[3]

This same flow of technology from military to commercial activity is evident in cryptology. Cryptographic skills travel across sectors as people shift from the classified community to pursue civil and commercial work. However, the exchange has not been so open; military codes and cryptographic information are closely guarded, leaving much of commercial cryptography to be developed independently. Also the flow back from commercial applications to national security uses is shrouded in secrecy.

Just how much commercial development and public discussion of cryptography will cause governments to revise their own schemes is unclear. It is doubtful that most commercial coding schemes would approach the sophistication of the ciphers used by the intelligence community, whose expertise is far more extensive and long-standing. There have, however, been minor instances where public discussion of cryptography has dealt directly with possible national security applications.

One such example involved the proposed SALT II treaty and the academic discussion of public-key cryptosystems. In all coding systems, encryption and decryption are inverse mathematical procedures. In traditional systems, it is simple to calculate how to decrypt once it is known how to encrypt and vice versa. However, in public-key systems one can make either the encrypting or decrypting schemes "public"; only the inverse procedure still remains confidential. Public-key schemes were primarily regarded as applicable to electronic fund transfer systems and the like, but they were also considered for use in the monitoring devices used to check U.S. and Soviet missile tests.[4] It was proposed that, under the terms of the SALT II treaty, such devices might be placed in the Soviet Union to broadcast back any information of nuclear tests conducted in violation of the agreement. Since it was vital that the devices not be tampered with or the transmitted information altered, this implied that encoding of the transmissions would be necessary. However, this would not prove acceptable to the Soviet Union since the encoded transmissions might contain other intelligence information not included under the treaty and over which they had no control. It was proposed that a public-key system might solve this dilemma. The Soviets could be given the key needed to decode the transmission, but this knowledge would not enable them to encode false information, thereby preserving the integrity of the transmissions and fulfilling the treaty.[5]

This particular application may or may not prove possible, and the SALT talks appear dead as of November 1980.[6] But what is certain is that the military and intelligence community no longer enjoys a monopoly on cryptology; new factors are bringing cryptography into the public domain.

One factor is the spread of computer networks and remote-access data processing. Geographically dispersed corporations have become more and more common; their management depends on electronic means of information transmission. It is taken for granted today that a bank account with one branch should be good throughout the state or country or even the world. Time-sensitive data such as current account balances must be distributed electronically from separate branches to a central processing unit and then back again. The commercial usefulness of remote-access data processing systems--systems in which data are transmitted by communication links to and from a central computer performing data processing functions--has greatly increased. This is because of the lower costs associated with large computers, because of a desire to share costly system resources in a convenient way, and because of the desire to centralize the storage of related information.[7]

Thus, many large corporations find themselves reliant on far-reaching data networks. While most corporate networks were designed to carry voice messages, new communications links are being designed specifically for data transmission. The bulk of these corporate telecommunications, whether voice or data messages, are transmitted by insecure common carrier lines. The fact that most long-haul terrestrial transmission in the U.S. is by microwave radio means that interception can be accomplished without a "physical tap" on the telephone line--it can be done several miles to either side of the transmission beam. The vulnerability of satellite microwaves is even greater in that signals may be intercepted within a satellite footprint thousands of square miles in area. To get some idea of the potential problem, consider that 65-70 percent of all toll messages are carried by microwave radio facilities at some point along their route.[8] In 1980, terrestrial microwave radio transmissions exceeded 190,000 route miles and were expanding at a tenfold rate every twelve years.[9]

Not all 190,000 miles of transmissions need be encrypted. However, encryption may be the only practical method by which some private communications can be made secure. Most vulnerable of all messages transmitted by common carrier are those directed over leased private lines. A caller using the public network will have his call switched and transmitted over a wide number of routes and facilities depending on traffic loads, system engineering, and circuit availability. However, a caller using private lines usually has his call directed over the same circuit; if transmitted by microwave, the call occupies the same segment of the radio spectrum. Once an interceptor "locates" the frequency or determines the route, he can readily monitor every message over that route.[10] Thus, in spite of the belief that private line services ensure "private" communications,[11] many dedicated line users are significantly more vulnerable to eavesdropping.

Private lines become less vulnerable in networks consisting of hundreds of private lines where calls are switched over any unused private line in the network. Switched private lines, along with public networks, present a larger burden to the interceptor. In the case of voice communications, at least for now, technology is not well enough developed to monitor large volumes of calls; without some kind of signal identifying the telephone number involved, a costly human evaluation of each message is needed.[12] However, advances in automatic speech recognition and work-spotting techniques may substantially reduce the cost of electronic interception in the future.[13, 14]

Some examples of interception that have already occurred include the case of a major U.S. financial institution and its foreign-based subsidiary. Government officials in the host country confronted management with the firm's confidential plan to shift resources to another country; as evidence of the shift, the officials used verbatim transcripts of the firm's international conversations.[15] In another case, the board of directors of an international auto manufacturer, after having trouble completing a conference call with a foreign branch, were told by an unexplained voice to "turn the right knob clockwise."[16] One final case occurring within the United States involves an oil company engaged in highly competitive bidding in Alaska. It had a computer terminal in the area connected to a central computer in another state to simulate bidding and develop bidding strategies. The company started losing bids by small amounts and later discovered the reason--an identical terminal three miles down the line was tapped in.[17]

The last case demonstrates another factor stimulating demand for commercial cryptography. Information stored and transmitted by computer is becoming more and more valuable. Typically, office computers in the past were used to store and transmit raw data and to analyze those data. Now modern corporate systems go two steps further--the conclusions from the data and the plans for action are also computerized. Previously, tapping an oil company's data lines might have yielded unwieldy statistics and geological findings; now the eavesdroppers may have immediate, usable information on prime drilling sites and actual bidding strategies. Electronic messages of managerial decisions often replace the paper memo. Whereas information from the paper memo is only available through direct physical access, the electronic messages can be "read" without ever entering an office or searching a single desk. It is often true that there are easier ways to get information than to bother with wiretapping; a clerk can be bribed or a file stolen. But as security increases around office terminals and computers, the data communication lines become the weakest links. And the more valuable the information, the greater the incentives for "wiretapping."

The greatest incentives of all exist in the electronic fund transfer systems where the assets themselves are in the computer. Today thousands of people no longer receive paychecks. Their employer sends the bank reels of magnetic tape containing the name, account number, and pay amount for each employee.

> At the bank, a pattern of small magnetized areas on the tape is converted to electric pulses which then cause a change of state in electronic circuits. Another set of electrical pulses diverted by the electronic circuits, in an equivalent pattern to the one on the tape, is sent to a device that forms a magnetic pattern on the surface of a rotating disk.[18]

By this time the employer has paid his workers; the bank now has the money and is often authorized to pay bills or cover checks through another change of pulses and electronic signals.

> The pulses can be converted to the form of checks by a computer printer or to monetary currency by computer-printed reports that authorize cashiers to transfer cash from boxes to people or to other boxes.[19]

And, with the trend toward automated teller machines, human hands need never interfere with the exchange of funds at all. The physical exchange of reels of tape is replaced by the direct transmission of data assets by telecommunication from computer to computer.

This kind of funds transfer may require extensive encryption techniques. A customer wishing to use an automated teller system is typically issued a card with a magnetic strip. The strip contains some identification of the customer, such as an account number, which is read by the terminal upon insertion of the card. The customer then keys in some other personal number, he is allowed on the system, and then he can withdraw or deposit as necessary. Now, if these numbers are not disguised by some form of code, an eavesdropper could learn the magnetic strip number and the corresponding personal identification. He could then steal cards for which he knows the personal identification number, or more profitably manufacture his own. Also tampering with the line could be just as profitable. If the deposits and withdrawals were not at least partially encoded, it would be easy to impersonate a terminal and divert funds illegally.[20]

One final factor encouraging data encryption, along with the growth of computer networks and the increased value of transmissions, is the need for personal privacy. There is now a widespread concern with the threat to privacy posed by computerized processing of personal data. Through the networking of data bases, it is possible to collect and maintain up-to-date dossiers on individuals' life styles, activities, views, and interaction with others.

> Whether he knows it or not, whenever an American travels on a commercial airline, reserves a room at one of the national hotel chains, rents a car, he is likely

> to leave distinctive electronic tracks in the memory of a computer than can tell a great deal about his activities--his movements, his habits, his associations.[21]

Without encryption and other computer security measures, these "electronic tracks" are often easy to trace. Compared with paper files, computer-based records are much more readily stored, searched, and exchanged. This increased vulnerability of computer-based records has already led to omnibus data protection laws in Western Europe. France and Germany have already passed laws requiring that stored or transmitted personal data be encrypted where necessary.[22] If and when the suggestions in the U.K. Data Protection Committee Report (Cmnd 7341) become law, it may become mandatory for security measures to be used for certain classes of data storage or transmission. In some cases, encryption may be the most suitable method available.[23]

In the United States, the perceived link between personal privacy and the need for encryption is not as strong. Privacy legislation has focused on the over 800 computerized data banks of the federal government which contain over a billion records on individual citizens. The Privacy Act of 1974 (P.L. 93-579) was aimed at safeguarding "individual privacy from the use of federal records."[24] This Act stimulated a flurry of government activity primarily because it required each record-keeping agency to establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records. These records were to be protected from any anticipated threats to their integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual.[25]

Following the Privacy Act, the Office of Management and Budget circulated guidelines for federal agencies to safeguard any data processing systems and telecommunications networks which contained personal, proprietary, or other sensitive data.[26] As a result, agencies began reviewing their security requirements and reporting to OMB on their plans for any increased protection. A November 1980 report from the General Accounting Office (GAO), which reviewed the various privacy protection requirements, included the comment that "the federal agency responses to the safeguarding provisions have ranged from no response at all to what may only be termed technological overkill."[27]

The GAO study found that protection of data transmissions could be strengthened by revising laws pertaining to wiretapping; current definitions of "intercept" in the 1968 Crime Control Act only provide against aural interception--wiretaps where the sense of hearing is used.[28] The report also called for more "specific executive level guidance for determining when the use of encryption is needed."[29] This guidance is needed, according to the report, because it is difficult to determine when encryption provides the most cost-effective protection of personal data. Several reasons why encryption might not be appropriate were listed: (i) not one documented case was found where wiretapping was used to intercept and exploit personal data transmissions; (ii) data that could be intercepted are generally unpredictable and hence less valuable; (iii) personal data are much more vulnerable to government officials operating the systems than to wiretappers; and (iv) encryption may give a false sense of security.[30]

However, a GAO report also included other recommendations which may require additional encryption techniques and applications. It was found that the rapid and uncoordinated growth of telecommunications in the federal government had resulted in duplication and costly dedicated networks; a common-user network was recommended to reduce overlap.[31] This common-user capacity could permit government workers to make more effective, and possibly more intrusive, use of information already in government files. Comments appended to the report called for controls to "diminish abuses caused by indiscriminate interagency sharing, machine searching, matching and correlation" of personal data.[32]

Before concluding the discussion of factors encouraging commercial cryptography, one more question needs to be addressed. Advanced electronic and computer technology now has many business and consumer applications. Does this new technology aid the cryptographer or the cryptanalyst, the code-maker or the code-breaker?

As always technology plays a dual role.

Rapid advances in electronics have increased the likelihood of unauthorized access to and alteration of electronically transformed data. Pamphlets from corporations marketing computer security document how, for around $500, an "eavesdropping kit" can be assembled with readily available components from electronics supply stores.[33] Also powerful minicomputers can be leased and programmed to simulate authentic terminals. Or they can be used to selectively monitor or dial up communications lines. There are no hard figures on how many wiretaps of commercial data lines occur; often such incidents are kept quiet to prevent imitation or embarrassment to the company involved. What is becoming clear is that many incidents are inside jobs. Current employees sometimes consider themselves justified in fiddling with their employer's computer. It is an intellectual challenge of man against machine. This same attitude is prevalent among a new breed of college computer experts--young people who have grown up with computers and electronic gadgets--who sharpen their skills with playful attacks on the university computer system.

Aside from individual efforts, the steep rise in computational power offers opportunities to organizations and government agencies to amass greater code-breaking capabilities. To grasp these capabilities, consider an exhaustive attack on the 56-bit key of the Federal Data Encryption Standard; an attempt to estimate the cost of such an attack was conducted at Stanford University. (The key is a particular pattern that the coding scheme uses to control the jumbling and shuffling of the bits of data into unreadable form; an exhaustive attack involves trying every possible key until the correct one is found.) Assuming that the attacker had access to both encrypted data and its readable form, researchers estimated that a specially constructed computer, costing $20 million and using about $5000 worth of computer time, could find the right key. These figures were based on computer costs in the year 1976. By 1986, the same attack could cost $50 and the required machine only $200,000.[34] The exact figures published by the researchers have been debated,[35] but the general decrease in the future cost of code-breaking computers is widely accepted.

But the same technology that makes code-cracking easier also aids the maker of codes. Faster and cheaper logic allows the cryptographer to use more complex ciphers; the same computers that break codes can also be used to generate them. Large-scale integration of circuits has made more secure and inexpensive cipher systems available than ever before. Also it is generally acknowledged that the cost of breaking a particular code increases far more rapidly than the cost of creating or strengthening the code. For instance, if the same exhaustive attack mentioned previously was carried out on a 112-bit key rather than a 56-bit one, the cost estimates would rise from \$5000 to $\$4x10^{20}$ for computing time and from \$20 million to $\$10^{24}$ for the actual machine cost.[36]

It would seem, then, that advancing technology is on the side of the code-maker rather than the code-breaker. This conclusion probably holds if the field of cryptology is considered as a whole; however advances in relevant technology typically occur in spurts and jumps. The individual corporation or industry that is behind the times electronically, or ignorant of the latest commercial techniques, could suffer from the newly available eavesdropping kits and microcomputers programmed for code-cracking. If this last observation is correct, it would imply that information on cryptology needs better circulation among potential users. But telling others how to keep secrets to themselves is always a tricky, almost paradoxical business. In 1977, when the Office of Telecommunications Policy commissioned a study on wiretapping, it got what was in effect an easy-to-read manual giving step-by-step instructions on eavesdropping. (The handbook included an eleven-step procedure for monitoring suburban phone calls, beginning with the instruction to "climb pole."[37]) The manual was more explicit than intended and had to be withheld from widespread public distribution; AT&T spokesmen protested that the manual would encourage interception of residential telephones and business data communications.[38]

Since March 1978, government attempts to encourage secure communications have been conducted by the Special Project Office of the National Telecommunications and Information Administration (NTIA). This branch of the Department of Commerce is chartered by Executive Order 12046 and is given a broad national role in telecommunication and information issues.[39] The Special Project Office was created in response to a National

Telecommunications Protection Policy Directive issued from the White House on February 15, 1979. The directive, issued in part because of reported Soviet interception of U.S. telecommunications, called for an increased government role in alerting non-military federal agencies, private telecommunications carriers, and private government contractors to the vulnerability of their communications.[40] As part of its work, the Special Project Office published, in December 1980, a user's guide to communications security. The December 1980 guide discusses the methods of interception and the various techniques available to combat these methods and also includes a listing of vendors offering encryption equipment.[41] It was distributed to a select list of federal agencies and private contractors but is also available to the public through the National Technical Information Service.

In addition to publishing the user's guide, the NTIA Special Project Office also commissioned a report by SRI International entitled "Impacts of Federal Policy Options for Nonmilitary Cryptography." The report examined various policy options available for both the control and promotion of private cryptographic research. Because of the rapidly expanding need for civil sector encryption, the SRI study found that the U.S. government policy on cryptography should be characterized by:

> - Explicit procedures to balance the nonmilitary social, economic, and technological cost and benefit impacts with the expected national security costs and benefits, both narrowly and broadly defined.
>
> - Awareness of foreign scientific progress and product development in the field of cryptography.[42]

The second point -- the importance of open cryptographic developments in other countries -- is one which may prove most relevant in the future. Academic and industrial work in cryptography is currently more advanced in the U.S. than elsewhere. However, there is no reason to assume that significant new developments will not occur in Japan, West Germany, or other countries pursuing open work in cryptography. These developments would weaken the case for U.S. controls on private developments at home. Thus the possibility of increased foreign cryptography becomes yet another factor to be weighed in the delicate balance involved in both promoting a new technology of secrets and limiting its harmful effects.

2. From Lucifer to Public Keys - The Evolution of Current Research in Cryptology

In his history of secret writing, The Codebreakers, David Kahn begins with "a town called Menet Khufu bordering the thin ribbon of the Nile" where "a master scribe sketched out the hieroglyphs that told the story of his lord's life -- and in so doing he opened the recorded history of cryptology."[1]

This analysis may begin in 1965. The Brooks Act (Automatic Data Processing & Equipment Act, P.L. 89-306) had just become law. It authorized the Department of Commerce to begin work on "uniform federal automatic data processing standards."[2] The National Bureau of Standards (NBS) was assigned the task of developing the various standards to cover all aspects of computer systems. In 1971 the Bureau began a program in computer security and, two years later, began a major effort on data encryption.

> The primary constituency under the Brooks Act for NBS data encryption standards were federal agencies; the secondary constituency deriving from NBS responsibilities as a member of the Department of Commerce was the buyer not operating under national security provisions and directives.[3]

Responsibilities for cryptographic research involving national security were, at the time, assigned to the National Security Agency (NSA) under a Presidential Directive of 1952.[4] Later, in 1976, an executive order reaffirmed the NSA's responsibility for the "conduct of research and development to meet the needs of the United States for signals intelligence and communications security."[5] The Bureau of Standards moved to take advantage of the NSA's cryptographic expertise in developing their encryption standards.

In May 1973 and again in August 1974, the Bureau solicited in the Federal Register information and suggestions for an efficient, economical method of encryption compatible with a variety of computer systems. Most responses were largely impractical or inefficient with the exception of IBM's Lucifer scheme.[6] The Bureau of Standards, in consultation with the NSA, judged the IBM scheme to be the best candidate for the Federal Data Encryption Standard (DES). The algorithm finally selected was similar to IBM's original design with the most evident difference involving a reduction in key size from 128 to 56 bits. The algorithm was published for public comment in March 1975, and two workshops in August 1975 and September 1977 were conducted on the DES and its cryptographic implications. During the time, IBM was granted limited patent rights to market the DES; the company also volunteered to issue non-exclusive, royalty-free licenses under this right. The DES was adopted as a Federal Standard on November 23, 1976, with an effective date of July 15, 1977.[7]

But the actual events did not proceed as smoothly as they read. To understand the various quarrels which began over the DES, it is helpful first to outline the basic workings of the algorithm, which operates on data expressed in "bits," coded impulses representing either "1" or a "0" (pulse or no pulse). The stream of bits is then modified according to a complex general formula specified by the DES; the particular modification used is controlled by a unique 56-bit pattern. The general modification formula will produce various outcomes, each dependent on a specific pattern or key.

To modify the original bit stream, the DES uses two principal techniques: transposition and substitution. To transpose the data means to change the order of the bits according to a fixed permutation.[8] For instance, consider a 4-bit transposition according to the permutation 4,1,3,2. Then, if the input stream in bits was 1100, the output stream would be 0101. The DES uses several similar transpositions and other rearrangements which maintain the size of the input block or increase or decrease its size by duplicating or discarding bits.[9] The other technique used is substitution--the systematic replacement of one symbol by another. In the case of binary operations, a look-up table is required. The bits of the message are divided into small groups and reassigned meanings according to the table. For instance, the input 111000 could be looked up in an agreed-upon table; the same table would then dictate a substitution, say 010001.[10] The DES uses eight different look-up tables, or "S-boxes," which govern the substitutions.

The algorithm thus uses various substitutions and transpositions on bits of input in a series of complex, key-dependent computations. Controversy immediately broke out over the 56-bit key size and the particular S-boxes chosen to perform the substitutions. What fueled the controversy was the fact that NSA had worked with IBM and NBS in developing the standard. Some felt that the "system was carefully designed to be just secure enough so that corporate spies outside the government could not break a user's code and just vulnerable enough so that the NSA could break it."[11] Many felt the key size was too small in comparison with current military key sizes, which were routinely 20 times larger; they felt NSA had deliberately limited the key size to maintain its code-breaking ability at the expense of the user's security. Spokesmen from IBM defended the key size on the basis of economy; larger key sizes would require more computer time, and the 56-bit key was conveniently implemented on a chip.[12]

Critics of the DES also worried that crucial aspects of the design of the algorithm were being kept secret. The idea behind open publication of the algorithm was to subject it to complete scrutiny as to any embedded flaws in the design--the strength of the code would rely on the secrecy of the individual key rather than on the secrecy of the design. But the NSA asked IBM to classify the way the S-boxes were constructed. This led some cryptographic specialists to believe there might be some internal structure, or "trapdoor," which, when known, could be "sprung," making the code much easier to break. Spokesmen from IBM and NSA insisted that the S-boxes were chosen to make the DES secure and that the Agency had not tampered with their structure. The principles of S-box construction were not disclosed. David Kahn, a writer on the history of cryptology, wrote that a debate had broken out between two sides in the NSA:

> The code-breaking side wanted to make sure that any cipher was weak enough for the NSA to solve it when used by foreign nations and companies. The code-making side wanted any cipher it was certifying for use by Americans to be truly good. The upshot was a bureaucratic compromise. Part of the cipher--the S-boxes that performed the substitution--was strengthened. Another part--the key . . . was weakened.[13]

All the allegations and speculations regarding NSA involvement in the DES were officially investigated by the Senate Select Committee on Intelligence. Their findings, released in an unclassified summary on April 13, 1978, state:

> In the development of the DES, NSA convinced IBM that a reduced key size was sufficient; indirectly assisted in the development of the S-box structures; and certified that the final DES algorithm was, to the best of their knowledge, free of any statistical or mathematical weaknesses. NSA did not tamper with the design of the

algorithm in any way.[14]

Today the debate over the specific design features of the DES has subsided. It is now a recognized national standard and is the most prevalent encryption algorithm in use today. It is generally agreed that the protection of a larger key can be achieved by encrypting the data two or three times with different 56-bit keys. No trapdoor has been found; Stanford Professor Martin Hellman, who led the academic criticism of the DES, now believes no trapdoor exists. He finds the current standard economical and better than no standard at all. However, more than three years after the standard's July 1977 adoption, Hellman would still prefer to design the algorithm differently if given the chance to start over.[15]

Key sizes and S-boxes are no longer hot issues, but two other sensitive points, brought to light by the DES activity, remain: (1) academic and other non-governmental research in cryptology has become respectable and innovative, thereby influencing government-related work; and (2) the general questions that arise from NSA involvement in this research are far from answered.

To illustrate the first, consider the work of Professor Hellman and Mr. Diffie who led the cryptanalytic attack on the DES.[16] Their work was largely responsible for the two workshops held by NBS to discuss the encryption standard. The Stanford study illustrated that unclassified cryptology was no longer an obscure area of research pursued only by hobbyists and amateurs. Cryptographic research was now a respectable field at the nation's most prestigious universities; the modern computer resources now available to academic scientists had greatly increased their cryptographic sophistication.

Before illustrating the second point, it is necessary to touch upon the technical breakthroughs that have created the field of public-key cryptography. During the time of the DES activity, Hellman and Diffie introduced the concepts of one-way functions and their role in public-key systems.[17]

> A function f(x) is said to be a one-way function of x if f(x) can be computed, but given a value y that is known to satisfy y = f(x) for some unknown x, in all but a small number of cases, x cannot be found by any practical method.[18]

Hellman proposed that such functions could provide a basis for encoding schemes where particular information about the encoding key could be revealed but (because of the properties of the one-way functions involved) the decoding key could now be discovered. When first proposed, these ideas seemed theoretically elegant but without practical significance. However, Hellman and Diffie's work was immediately picked up and refined by three scientists at MIT, Rivest, Shamir, and Adleman, into a usable algorithm know as the RSA method.[19]

The RSA algorithm creates a workable scheme where knowing how to encrypt does not allow one to decrypt. This solves some, but not all, of the problems of distributing keys between the two parties wishing to communicate in secret. In traditional systems, the key must be distributed in secret between the two parties. Also, during every communication, each party must be able to authenticate the other's identity. Each user wants to be certain he is sending his coded messages to the intended receiver and not to some impostor at the other end of the line.

With public-key systems, the encrypting keys of various parties can be recorded in a public directory; communicating with one of the listed parties would require looking up the correct key and encrypting the message in that key. The intended receiver could then use his own private (and secret) decrypting key to read the message. However, the above instance only solves one part of the key distribution problem--the need for secrecy. The directory need not be kept secret but it must be guarded against illicit alterations. Otherwise, a perpetrator could change a party's listed encrypting key to one of his own (for which he had his own, private decrypting key). Then all messages intended solely for the affected party would be instead encoded in the perpetrator's key and subject to his reading.

Thus, public-key systems solve some, but not all, of the key distribution problems posed by traditional systems. The new systems also offer a new twist that is not practical with traditional coding schemes, namely digital signatures. If A wishes to send you a "signed" message, A first encrypts it with his secret decrypting key, and then encodes it again with your public key, listed in some directory. Upon receipt of the transmission, you first undo the last encryption by applying your secret decryption key. Then, using A's publicly listed encryption key, you may read the original message confident that it could only have come from A (since only A has the secret decryption key which is the inverse of his public encryption key).[20] This idea of digital signatures, while not yet in practice, illustrates the innovative and productive work now carried out in the non-governmental sector.

Tension between unclassified work in the private sector and the work of the NSA has caused continual strife over secrecy orders and research funding. In April 1978, the Commissioner of Patents and Trademarks followed the advice of the NSA and issued two secrecy orders to private individuals seeking patents for coding devices. The first ordered that George Davida's non-linear stream cipher device be kept secret.[21] Davida, a professor at the University of Wisconsin, had developed the device under a National Science Foundation (NSF) grant. University Chancellor Werner Baum publicly protested the order, which was rescinded a few weeks later. NSA Director Bobby R. Inman was quoted as saying the decision to seek a patent implied a profit motive rather than concerns of academic freedom: "If the individual had elected to publish in academic journals there would have been no question of a secrecy order."[22] Chancellor Baum called for some "minimal due process guarantees for individuals threatened with a secrecy order," and argued the "burden of proof should be on the government to show why a citizen's constitutional rights should be abridged in the interests of 'national security.'"[23]

The second secrecy order denied patent rights to the "Phaserphone" voice scrambler invented by George Nicolai and others working in Seattle. The order was not rescinded until October 1978, and no clear explanation was given upon removal. An article in <u>Reason</u> magazine quoted Daniel Silver, then NSA general counsel:

> As the reasons for concluding that disclosure would be detrimental to the national security are themselves classified information, unfortunately we cannot provide additional information on the basis of our conclusions.[24]

The magazine article then went on to speculate that, although similar devices to the Phaserphone were currently on the market, the new low-cost technology of the device prompted NSA's concern.[25]

Largely because of the publicity surrounding the two secrecy orders, a great deal of attention has been focused on the underlying statute, the Invention Secrecy Act of 1951. The law was approved February 1, 1952, and codified as 35 USC 181-188. Section 181 establishes two groups of inventions. If the government has a property interest in the invention, the Commissioner of Patents issues a secrecy order on being notified that, "in the opinion of the interested government agency," publication or disclosure by the grant of the patent might be detrimental to the national security. If the government does not have a property interest in the invention, the Commissioner makes the application available to the Defense agencies when disclosure "might in the opinion of the Commissioner be detrimental to the national security." If notified that, in the opinion of such an agency head, disclosure would be detrimental to the national security, "the Commissioner shall withhold the grant of a patent for such a period as the national interest requires, and notify the applicant thereof." (Defense agencies defined by the Act and subsequent directives are the AEC/DOE, the Secretary of Defense, NASA, and Department of Justice.)[26]

An invention "shall not be ordered kept secret and the grant of a patent withheld for a period of more than one year." However, the secrecy order is renewable for additional periods when the Commissioner is notified by the agency head who originally caused the order to be issued that "an affirmative determination has been made that the national interest continues so to require."[27] Furthermore, the Invention Secrecy Act granted secrecy orders a lifetime of six months beyond the duration of a declared national emergency. (This provision allowed secrecy orders to remain in effect without review or renewal from the time of President Truman's December 1950 proclamation of national emergency to its termination in 1978 following the passage of the National Emergencies Act of 1976.)[28] Further features of the act include a $10,000 fine and/or two-year prison term for secrecy violation, a method of appeal through the Secretary of Commerce, and the right of the applicant under secrecy order to seek just compensation from the agency that caused the order to be issued.[29]

In March 1980, the House Subcommittee on Government Information and Individual Rights held the first hearings on the act since its passage. In its report it recommended that Congress write a rationale for invoking the Secrecy Act in peacetime and then amend the act extensively to improve compensation, define national security, provide review classification procedures involving applications, and more.[30] Focusing on the NSA, the committee report detailed five private laws passed by Congress involving settlement of rights or claims involving secret cryptologic inventions--inventions where no patent application was filed at all, leaving sheer secrecy as the sole protection of the government's proprietary interests.[31] The subcommittee report also detailed the NSA's seven secrecy orders in force in 1980 and included some of the hearing testimony of those involved in the Davida and Nicolai orders. Contained in its recommendations to the NSA, the subcommittee included a request that the NSA director, not a subordinate acting on his behalf, determine that a secrecy order be requested.[32]

The NSA had already established a new review of the secrecy orders and patent applications. Officials of the Agency admitted that the previous procedure leading to the two 1978 secrecy orders was inadequate. The procedure in use in March 1981 involved a five-man board with representatives from the different branches of the Agency who reported directly to the Director. Members of the board included high-level officials from the Research & Development arm of the Agency, from the unit concerned with Signals Intelligence, from the Communications Security Division, as well as the General Counsel and the Deputy Director for Policy. The board has reduced the number of secrecy orders from seven to six and is currently evaluating removal of another existing order. In addition to the review board, the NSA engineers are currently encouraged to keep track of all their ideas in annually reviewed notebooks; there is the hope that these notebooks will clarify and protect the in-house investors' rights should secret designs later appear on the outside market.[33]

No new secrecy orders have been known to be issued to private inventors on behalf of the NSA since 1978. Agency officials stress that they expect only a very tiny fraction of all patent applications will ever be considered for such orders; members of the review board must act affirmatively to maintain existing orders or issue new ones--the burden is on the reviewers to prove why the secrecy orders should not be rescinded. In addition, the Agency asserts that, in the rare cases where an order might be issued, the inventor will be fairly compensated.[34]

In spite of the Agency's new procedures for evaluation of secrecy orders, skepticism over the entire patent review process throughout the Defense Department has received more coverage. The House Government Operations Committee report found that the right of compensation "appears more illusory than real" and that "invention secrecy is heavily weighted against private inventors who work outside the classified and defense community."[35] An article in the January 1981 issue of Reason stressed that, while only a small number of secrecy orders are actually issued, a far greater number of patent applications are scrutinized; this additional scrutiny, coupled with the fact that inventors are not told that their application was reviewed unless an order is imposed, formed the basis for the article's scenario of "a massive, day-to-day siphoning of state-of-the-art knowledge."[36] The extent to which this siphoning has actually occurred is far from clear.

Also, in the specific area of cryptographic devices, several unique points must be weighed. The NSA is generally credited with being several steps ahead of the non-governmental cryptologists; Admiral Inman and others at the Agency have testified that practically everything discovered in the open community has already been considered within the organization. This would indicate that private inventions would not advance the NSA's state-of-the-art substantially. How this will change as outside researchers gain greater sophistication in cryptology--and focus their expertise on those consumer and commercial interests outside the Agency's traditional mission--will become of greater concern as research progresses.

In addition to the patent secrecy questions, open research in cryptology has also raised issues in the area of research funding. The House Government Operations Committee report on the subject identified section 1-205 of Executive Order 12065 on National Security Information as "one of the unknowns in the public cryptography equation."[37] The "Exceptional Cases" provision of the Order reads:

> When an employee or contractor of an agency that does not have original classification authority originates information believed to require classification, the information shall be protected in the manner prescribed by this Order and implementing directives. The information shall be transmitted promptly under appropriate safeguards to the agency which has appropriate subject matter interest and classification authority.[38]

This provision applies to the NSF, which has no classification authority, and requires it to submit any cryptologic information requiring classification to the NSA, the agency with "appropriate subject matter interest." However, the House report also details some contrast between the provision's application to "an employee or contractor" and NSF's own security regulations, written after the Order, which apply only narrowly to "a Foundation employee [who] develops information that appears to warrant classification . . ." The report also mentions sections 1-602 of the Executive Order, "Basic scientific research information not clearly related to the national security may not be classified." When taken together, the Committee reports these provisions and security regulations "appear to mean there is virtually no expectation that an NSF contractor doing basic scientific research could--from NSF's point of view--generate information so clearly related to the national security that NSF would . . . forward the information to another agency for a second opinion."[39]

These findings of the House Committee are indicative of the speculation that has surfaced over NSF-NSA dealings in cryptology. Another incident involving the two agencies occurred in August 1980. Professor Adleman of MIT and the University of Southern California (and the A of the RSA algorithm) was told by an NSF official that the Foundation would not fund part of his proposal. Adleman's entire grant was in the hundred thousand dollar range, but the amount withheld was only a matter of a few thousand dollars. While the amount was small, press coverage implied that the ramifications for future cryptographic research were great. A Science article, subtitled "National Security Agency seeks to influence science agency policy," reported that "according to Inman, the reason NSF chose not to fund parts of Adleman's proposal is that NSA wants to fund the research itself."[40] For over two years, NSF had routinely submitted its cryptography proposals to NSA for review. The proposal by Adleman, and another by Professor Rivest (the R of RSA), appeared to Inman as good opportunities for NSA to begin sponsoring cryptographic research. The

Science article also expressed some of the fears of the academic community, including Adleman, that the NSA was not sensitive to the funding concerns of the academic community, that the Agency was attempting to blur the line between basic computer science and cryptography and that NSA might be too ready to classify Adleman's work.[41]

Officials at NSA explain that the entire incident was caused largely by a misunderstanding in the communications by NSF to the researchers; they also assert that their national security concerns over funded projects should not appear unusual to researchers accustomed to dealing with other Defense Department contracts.[42] In a letter to Science, Inman explained that NSA's funding efforts were "meant in no way to supersede or freeze out any other funding mechanisms for research in cryptography" and that "NSA does not now have and does not intend to seek the authority to prohibit NSF from funding in this area."[43] Inman's letter was followed by another from NSF Acting Director Donald Langenburg stating that "the NSF does not expect that the results of the basic research which it supports will be classified, except in very rare instances" and that "it makes no essential difference, in terms of the likelihood of classification, whether the research is supported by NSF or NSA."[44]

Largely as the result of the publicity surrounding the funding case, the directors of both NSF and NSA met with White House science advisor Frank Press on October 9, 1980.

> It was decided at the meeting that both NSF and NSA will fund cryptography research. For the time being, all cryptography proposals will be sent to the NSF, who will send them to NSA for technical review. If the NSA wants to fund a proposal, it will inform the NSF, which will offer the researcher the choice of accepting NSA or NSF funds.[45]

As of March 1981, the NSF treats proposals in the following manner. After the proposal is received in the Mathematical and Computer Sciences Division of the Foundation, it is sent out to leading cryptology researchers in the non-governmental sector. The Foundation uses this outside peer review in cryptology and other fields because expertise is limited within NSF. The reviewers rank proposals based on the past performance of the principal investigator, the importance and difficulty of the problems considered, and the general scientific merit of the approach. The program director at NSF then puts together the various views of the peer reviewers and tempers them with his own judgment--if, for instance, the researcher is not established in his field, the program director attaches less weight to the past performance criterion. Proposals are then funded according to available resources. There is considerable variation year after year, but typically $500,000 a year in total funds are granted, supporting approximately six to eight proposals.[46]

In addition to getting information from the non-governmental reviewers, the NSF also forwards proposals to the NSA attaching a letter to the Agency stating that the proposal is being sent for information purposes; the letter may also request technical comments and/or joint consideration for funding. If a peer review is requested, a separate letter is sent to an individual with identifiable expertise concerning the subject matter of the proposal.[47] Workers at the NSA and the NSF are preparing for joint funding of proposals and independent NSA grants. As explained in Inman's letter to Science, the NSA is "increasingly interested in investing in primary research in cryptography as well as related fields such as mathematics. Up to now this effort has been by means of entering into contracts with companies and institutions, although we are hoping to expand our efforts to include grants for significant primary research."[48] The NSA had originally hoped to provide Professor Martin Hellman its first grant; however the Agency ran into bureaucratic problems in gaining the new authority to issue grants and settled for a contract with the Stanford researcher. As of March 1981, NSA has the authority to issue grants and is preparing to release a set of guidelines to researchers outlining the type of support it is offering.[49]

Meanwhile academic and industrial research in cryptography continues. Citibank, among the more sophisticated users in the banking community, spent around a quarter of a million dollars funding cryptography research in universities during 1979. Scientists at MITRE and Digital Communications are experimenting with a "hybrid" cryptosystem which uses the DES for encryption of messages but relies on public-key systems to distribute the DES keys--thereby solving some of the traditional key distribution problems. MITRE is currently using such a scheme for in-house electronic mail, but researchers there believe widespread use of the scheme is years away.[50] Sandia Laboratories is also involved in a public-key test program at the Oak Ridge National Laboratory. Monitors measuring uranium enrichment will encode their findings with the new codes; the decoding keys will be made public, allowing open monitoring of the fuel but preventing any forged measurements.[51]

In the academic world, Rivest is refining the elctronic chip which performs the RSA algorithm. Others, including Professor Hellman of Stanford, are continuing their work on public keys and are engaging in private consulting in cryptography.[52] Also, there is a greater awareness throughout the scientific community of the cryptologic implications of basic work in mathematics and computer science. John Cherniavsky, of the

Mathematical and Computer Sciences Division of the NSF, predicts that increased efforts will be directed towards determining the security of particular cryptosystems. He also notes the advances in set theory, such as the mathematical notion of a random polynomial time computable set, which have evolved as a result of cryptologic research.[53] Others believe that cryptologic work might result in breakthroughs in an area such as scheduling theory.[54] In addition, basic mathematical questions involving computational complexity, testing for prime numbers, and generating random numbers are all receiving increased attention.[55]

The increased academic interest in cryptology has in turn increased NSA's interest in the academics. Then Vice Admiral Inman, Director of the NSA from July 1977 to March 1981, has taken unprecedented steps to increase communications between the Agency and the universities. In the first public address of any Agency director, Inman declared that "the Agency's mission can remain no longer in the shadows," and called for a "dialogue" between the Agency and the industrial and academic communities. In sponsoring secrecy orders, he declared "the Agency's sole consideration is the detrimental effect on the Agency's mission, and thus on the security of the United States, that would result from the proliferation abroad of sophisticated cryptologic technology."[56]

He then detailed the potential dangers to national security:

> Application of the genius of the American scholarly community to cryptographic and cryptanalytic problems and widespread dissemination of resulting discoveries, carries the clear risk that some of NSA's cryptanalytic successes will be duplicated, with a consequent improvement of cryptography by foreign targets. No less significant is the risk that the cryptographic principles embodied in communications security devices

> developed by the NSA will be rendered ineffective by paralleled non-governmental cryptologic activity and publications.[57]

Inman concluded his speech with criteria for restricting only a "central core of critical cryptologic information." He stated that restrictions should be as clear as possible, provide compensation for losses caused, and place the burden of proving their necessity on the government. He also suggested a "specially constituted court that could act under suitable security precautions" to review any restrictions taken.[58]

Director Inman also began a series of informal discussions, lunches, and meetings between Agency officials and scientists such Rivest, Hellman, and Adleman. As an outgrowth of these meetings, the NSF funded an eight-member Public Cryptography Study Group. Convened by the American Council on Education, the Group included Daniel Schwartz, NSA legal counsel, Ira Heyman, chancellor of the University of California at Berkeley, and six other representatives from industrial and educational societies.[59] The Group began meeting in March 1980, and it is yet to be seen how its February 1981 recommendation for a system of voluntary prepublication review will affect the delicate issues involving cryptography, national security, and individual rights. Before examining these important--but often intangible--issues, it is necessary to consider some more common concerns--the buying and selling of cryptography on the market.

3. Selling Cryptographic Products on the Market

Will data encryption quickly become common in the private sector? Or is it a technology, like satellite space stations or electric cars, that will teeter "on the brink" of widespread development for years to come? Estimates on the current and future use of commercial cryptography vary widely depending on who is consulted. The actual salesmen of cryptographic equipment often see a tremendous demand for their product while many data-processing managers are less enthusiastic. But everyone agrees that the market for cryptography will grow in the next ten years--what is not clear is how much and how fast.

Before examining the products on the market and who's buying, it's helpful to look at who isn't and why. In Fortune, a survey of 1000 data processing and communications managers found that about 25 percent used encryption, another 30 percent were studying it, and the remaining 45 percent had no real interest in it at all.[1]

Probably the first reason why data managers don't consider encryption is its cost. They don't see or cannot imagine how the information they deal with could be valuable enough to justify the expense of encryption. Single encryption chips, which perform the DES algorithm, are in the $200-$300 range but also require some software development and auxiliary hardware before becoming operational. Customers may also buy the chips in physically secure, stand-alone units; these units have built-in microprocessors and range in price from $1200 to $2000. Using this hardware, the cost of securing 500 terminals in a distributed network can run as high as $2 million.[2] This is often too high to justify. Also salesmen point out that selling cryptographic protection is akin to selling insurance--the buyer gets no tangible benefit for his money. (An exception to this occurs when the customer places a high value on error detection. A 1-bit error in the original message is magnified to 20 bits during the shuffling and jumbling of the algorithm, and is thus easier to detect.)

Another reason that data managers forego encryption is their theory of "least resistance." Many managers believe that perpetrators will seek the cheapest and easiest methods of access to confidential data. At present it may be far easier to pass $50 to a terminal operator than to tap a data line. Also most computer-related crimes have tended to be inside jobs; the whole system may be more vulnerable to those who feed and care for it--the data-entry clerks and in-house programmers--than to outside wiretappers.[3]

Also encryption is not used because it is a difficult, complicated business. Most managers are not familiar with the exact technology; the encryption device is a black box to them. They are never sure just how good the security being offered actually is. There are no proofs of the absolute security of any cryptographic device--it can only be shown to resist most known methods of attack. Data managers may also be reluctant to use encryption because it never completely solves their data security problems but merely localizes them: encrypting communications reduces the problems of securing vulnerable transmission lines to the problem of securing the particular keys to the code. The keys must be distributed to users but kept from outsiders; they must be authenticated; and they must be kept from physical destruction or loss. These are the problems of "key management" which often require new protocols and auxiliary equipment. Rather than redesign an existing network to accommodate encryption, many managers forego the coding or postpone it until other major changes are implemented.

A final factor discouraging encryption is the set of legal restrictions imposed on cryptographic products. Exporting any computer encryption device requires a license from the Office of Munitions Control at the State Department. Some companies, such as IBM, have received permission to export computer equipment incorporating the DES; however, others are unable to do so.[4] Also the restrictions upon certain countries vary. Eastern bloc countries are out, along with Iran, Iraq, and Libya; with other countries, such as Syria and Bolivia, exporting is an on-again-off-again proposition.[5] Other regulations, beside export controls, discourage international would-be users of encryption. Foreign regulations may require that the secrecy of the communications be compromised. The most obvious example involves the British Post Office which "must be able to monitor all data transmissions that cross U.K. borders. If a transmission is encoded or encrypted, the Post Office has rights of access to the codes or keys."[6]

In spite of the high costs, the difficulties of installation, and the existence of export restrictions, more and more companies are purchasing encryption equipment. Most sales representatives agree the market is growing and confide that they are currently sitting on a $4 million deal here and another $1 million sale there. The exact annual figures on encryption sales are hard to come by, partly because the non-military market has only really existed for five to eight years, and partly because some definitions of what constitutes cryptographic equipment are broader than others. A study in 1979 by International Resource Development placed the commercial market at $70 million with additional military demands boosting the total to nearly $170 million.[7] These estimates may be on the conservative side--one official, from one of the over twenty firms manufacturing encryption hardware, estimated that his company alone sells

$40-$60 million worth of equipment annually.

The kind of people who are buying were detailed by a 1979 report from Quantum Science Corporation:

> Banking and retail POS (point-of-sale) applications presently comprise about 60 percent of encryption orders; government applications account for 25 percent and the remaining 15 percent is for corporate applications across all major industry sectors. Virtually all of the encryption applications in banking and retail involve special purpose terminals, such as automated teller machines and point-of-sale, whereas the corporate and government applications are mainly associated with general-purpose terminals.[8]

Sales representatives note that it is only since 1979 that orders have increased from such non-banking areas as the oil and shipping industries. Also while most of their orders are for large networks, there has been an increase in small requests to secure one to ten-terminal systems. In addition many of the orders are for devices which are used not to protect communications network but to guard stored data. Encryption devices are often used to encode sensitive data kept on portable media such as tapes or disks. Over half of the crypto-boxes sold thus far by IBM are used for this purpose.[9]

Once the buyer chooses to encrypt his communications or his stored data, he is faced with a whole range of products: the Datacryptor, Infoguard, Cryptomatic, Cryptoline, Datalock, Gretacoder, the Silencer, etc. A chief criterion for determining the appropriate chip or device is its data handling rate. Roughly two classes of products have evolved.[10] One set, with a rate near 1 million bits per second (bps), is able to encrypt input and output data in close to real time, with a minimum of storage and buffering.[11] The other group, with a rate closer to

5,000-10,000 bps, is more appropriate for telex services, bank-card verification, and other computer networks.[12] Once the data rate is considered, the next criterion is often the number of different keys that the device will accommodate. And, eventually, the type of algorithm used must also be considered. Most of the devices employ the DES and have been certified by the Bureau of Standards as complying with the requirements of the algorithm.

This certification by the bureau has changed somewhat the "buyer beware" nature of the encryption market. The buyer is still buying devices he knows very little about, but, since 1977, he has an accepted federal standard to guide him. And commercial standards are now being developed by the American National Standards Institute, a clearinghouse for nationally coordinated voluntary standards. In August 1978, the Institute began work on the standards needed for encryption products.[13]

The Institute committees which review the standards proposed by various study groups are made up of representatives from the equipment manufacturers and affected service organizations. For instance, the Bank Standards Committee includes Burroughs and Digital Communications, Chase Manhattan and Bank of America, and VISA. The committees attempt to arrive at consensus standards through an iterative process. A small subcommittee begins work on the standard, pushes the ideas along until they require additional comment, and then submits the draft to the larger committee. The negative comments are then considered as the standard goes through several stages of planning and comment. It is then subject to public review as a draft of the standard is circulated and eventually published. In March 1980, standards for magnetically stripped bank cards and fund transfer message authentication were published for review. Other work by various committees include a software version of the DES, standards for encrypting physically interchangeable magnetic tape files, and possible satellite applications.[14]

Worldwide encryption standards are the responsibility of the International Standards Organization based in Geneva. Donald Davies, a scientist at Britain's National Physical Laboratory, is the appointed convener of the study group for encryption.[15] His work currently includes the Teletex system which "may become the principal means of correspondence for business purposes."[16] He has begun describing the enhancements needed to the Teletex document and session protocols in order to incorporate end-to-end encipherment and/or digital signatures.[17] The methods proposed are based on the DES, which is now proposed as an international standard, and also allow for applications of the RSA public-key scheme.

Davies believes encryption methods, such as those mentioned, will be widely used in the next five to ten years.[18] It is generally agreed that commercial standards have not yet evolved to allow large volume production of commercial cryptosystems. These systems must be low cost with low error rates and require minimal human intervention. What is keeping public-key schemes from meeting these criteria is primarily the data handling rate of the available hardware. Professor Rivest is currently testing a chip at MIT which performs the RSA algorithm, and he estimates that it may be marketable by 1983. However, it handles data at a rate close to 1200 bps and is immediately applicable only to distribute DES keys rather than to encrypt actual data. Other non-technological factors limit the use of public-key cryptosystems. Details on the patents for the two principal schemes have yet to be worked out between the Office of Patents and MIT and Stanford University. Also potential users are waiting for some kind of certification or assurance that public-key systems are indeed as secure as they seem. Cryptanalytic studies and other attempts to assess the strength of the algorithms have all been conducted informally without the formal support of NBS or the American National Standards Institute.

Nevertheless, extensive applications of public-key systems in particular, and consumer-oriented cryptography in general, are seen for the future. Victor Walling of SRI International foresees the role that cryptography can play in managing property rights of buyers and sellers.[19] Information products may be delivered and distributed in coded form; the buyer can then purchase a key which allows him to use the product. The most obvious example of this idea is subscription television where the subscriber's decoding box allows him to unscramble the programming. Mr. Walling also asserts that the signature and authentication aspects of commercial cryptography could prove more important in non-military applications than the secrecy uses. Codes might be used to "sign" electronic checks from home terminals, allowing the bank to authenticate the check while ensuring the original amount to be cashed is not changed. The technology for this type of operation is within reach, but the legal definition and status of electronic signatures have not yet been established.

For other outlooks on commercial cryptography that are more closely tied to the dollars spent and the hardware bought, consider the report from International Resource Development which saw a doubling in the dollar volume of the commercial crypto market--from $72 million in 1979 to $137 million in 1981 and then a leveling off to $148 million in the next eight years.[20]

> While the use of encryption will increase more than tenfold, however, the actual value of shipments of

> encryption gear will rise only modestly, because of the greatly reduced cost of integrated LSI modules.[21]

The Quantum Science report focused attention on the encryption capabilities of terminals in 1982:

> Of the 511,000 general-purpose terminals shipped, 50,000 will have encryption capabilities. Of the 307,000 special-purpose terminals shipped, 93,000 will have encryption capability. These include:
>
> 2,000 of 22,000 factory data collection terminals;
> 27,000 of 137,000 point-of-sale terminals;
> 29,000 of 73,000 credit authorization terminals.[22]

A later study by a group of students at the Department of Engineering and Public Policy, Carnegie-Mellon University, disputed some of the more expansive figures of the International Resource Development report. In general, they found that

> Despite the initial number of optimistic market forecasts, the magnitude of the civil sector data encryption market has remained small. Private organizations and individuals appear not to feel the compulsion to encrypt information that they handle by other, perhaps less secure, means.[23]

The study also stressed the point that there must be a level of demand sufficient to bring low-cost devices to the marketplace--this level of demand is needed in addition to the general decrease in costs brought about through cheaper integrated circuits and microprocessors. The study found that common carriers and specialized common carriers surveyed currently receive few requests for data encryption from their customers; only three of the fourteen surveyed offered any form of data encryption as a regular service, and only two others were planning to add it.[24] Students participating in the study also found that many of the manufacturers of crypto devices expressed disappointment in a small and only slowly growing market.

> Their initial assumption was that the market would grow at the same rate as the broader telecommunications market. Their confidence in this assumption is indicated in their failure to conduct their own market studies before undertaking the development and production of their product. As a result of the poor market, many products are now sitting unsold on shelves.[25]

After interviewing suppliers of encryption devices, the students then interviewed potential customers. One interview at a major local bank revealed that the bank preferred other system "controls" over encryption in its EFT system. Principal among their methods of protection were: (i) authorization--involving passwords distributed to the user; (ii) transaction sequences--giving numbers to each valid transaction executed by the system; and (iii) restriction--limiting the daily amount withdrawn by a user.[26] The bank representatives said encryption costs must decrease substantially--particularly the cost of retrofitting the existing system--before data encryption becomes widespread. It was also noted that, as prices fall, the first communications to be encrypted will be communications between local banks and the Federal Reserve System; banks may well wait until the reserve banks set a security standard or operational precedent before securing their own lines. A somewhat similar view of the use of encryption in the banking industry is held by Howard Crumb of the New York Federal Reserve Bank. He agrees that the industry is waiting for the handful of larger, leading banking institutions to pick up encryption methods and then foresees a kind of "domino" effect as the remaining banks follow suit.[27]

The Carnegie-Mellon study concludes with a section weighing civil sector data encryption and national security interests. Two cases are proposed. The first assumes a rapid development of civil telecommunications and digital communications; with this increased development comes a corresponding growth in the potential for security breaches and abuse of confidential data.[28] Scenarios that fit these assumptions include the loss of an American firm's confidential strategies used in negotiations in foreign countries, the premature disclosure of changes in the prime interest rate, or the unwanted dissemination of information and developments in advanced technologies.

Proceeding from this basis, further assumptions are made in the study's first case. Most advanced nations, including the Soviet bloc countries, are assumed to possess sophisticated encryption technology which prevents their networks from providing significant amounts of signals intelligence. However, developing countries are assumed to have far less secure communications which yield more foreign intelligence information. Development and marketing of inexpensive cryptographic equipment for the U.S. market will also seal off some intelligence sources in these countries. However, in the first case, the costs of insecure communications in the civil sector outweigh the signals intelligence benefits foregone abroad. In addition, the significant expansion of civil telecommunications makes encryption beneficial to national security as well as civil security by reducing strategic domestic information "leakiness." Under these circumstances, the study finds that "net social benefit" is greatest if both national security and civil security actors pursue policies encouraging civil sector encryption.[29]

The second case conjectures a slower civil telecommunications development where most users do not find encryption a valuable or necessary security measure; there are few known cases of data abuse or computer crime. If encouraged development of encryption technology comes before the civil sector can substantially benefit from it, then this development presents sizeable costs to national security in terms of diminished signals intelligence and reduced government communications security. In this case, net social benefits are highest if the relevant policy actors pursue policies that "would forestall, or at least not accelerate, encryption development and use."[30]

The second case hypothesized falls upon sympathetic ears at the National Security Agency--the primary user of cryptography and cryptographic research in the government. There is a feeling among some at the Agency that the need for civil sector encryption is less immediate than has often been projected--that the actual threat is less than publicized and that the costs are presently too high to sway corporate decision makers to encrypt. It should also be noted, however, that there is some divergence of opinion between those who are concerned with communication security and those whose primary work deals with data gathering and signals intelligence. On the communications security side, there is a greater emphasis placed on the potential benefits and new innovations that may emerge from civil cryptography. Those involved in signals intelligence, on the other hand, are already witnessing the damage to very fragile intelligence sources caused by the increased publicity surrounding cryptography; they do not necessarily wish to limit the spread of encryption technology to those U.S. companies requiring it, but they are extremely reluctant to have widespread publication and discussion of cryptologic methods.

Many have argued that the NSA has a decided self-interest in keeping the lid on non-governmental cryptology. David Kahn, in an article in Foreign Affairs, wrote that integrated circuits and other electronic advances are putting excellent encryption technology within the price range of more and more countries than ever before; this means fewer and fewer code-breaking possibilities for NSA.[31] Similarly, an article in Reason discussed the possibility that "eclipsed by work done 'outside,' the NSA is increasingly falling behind and getting desperate." The article included the argument that the major powers of the world have had secure systems for years, that the NSA can decode only about four percent of the transmissions it picks up, and that "attempts by the NSA to prevent Third World communications security is a losing rear-guard battle."[32] However, the argument that the signals intelligence mission of the NSA is declining and may eventually end should be weighed alongside historical trends which have shown the amount of both code-making and code-breaking to grow as rapidly as communication itself. Indeed, George Davida, one of the most avid spokesmen against NSA involvement in private cryptographic research, testified before Congress that he expects "NSA to improve its intelligence gathering" and that codes reported as "unbreakable" are in fact nowhere near so.[33]

Another scientist who expresses concern with the future market for encryption is Professor Michael Dertouzos, director of the Laboratory for Computer Science at MIT. He finds that the Carnegie-Mellon study and the estimates of the market for encryption coming from inside the NSA are far too limited in their vision.[34] He is concerned that too much emphasis on the national security/signals intelligence side of cryptology will cause lopsided development in the crucial areas of computer and communications security. What current studies have failed to grasp, he asserts, are the staggering security problems caused by computer-to-computer interconnections. Within the next ten years he predicts that networks consisting of tens of thousands of computers will connect businesses, corporations, and banks.[35]

Dertouzos sees these interconnections occurring in three phases. First, there are the intra-organizational connections--which are already occurring--where computers within large organizations are hooked together to share data and capabilities. Then, in the next five to fifteen years, come the inter-organizational connections where, for instance, a manufacturing company will connect its computer with the firm which is its steel supplier in order to automate raw material requests, product delivery, and billing. The final phase of the computer-to-computer connections takes place with the advent of home computers connected with others to perform office work, financial transactions, and other personal needs. Without some sort of security regulation such as encryption, abuses may become staggering. Dertouzos draws the analogy of "a network of filing cabinets, connected by subterranean tunnels" where "agents can crawl through these tunnels, copy anything they want from any of the files, and leave no signs of their presence."[36]

Dertouzos deliberately stresses an expansive view to avoid having a narrow vision applied to encryption, similar to what he finds was applied to radar in the 1940s. During World War II, radar was thought of only as an important military tool without any realization of its potential to become the backbone of an enormous civil air transportation and control system. Dertouzos also stresses an element of irrevocability in any decisions made to control the progress of cryptologic research. If computer-to-computer connections and general reliance on telecommunications progresses as rapidly as predicted, any foregone technological developments will prove costly. Vital communications and data bases will remain compromised for several years while the civilian sector attempts to catch up with the threats through cryptography.[37]

What, if anything, can be gleaned from these varied opinions on the future growth of the commercial crypto-market? All the studies agree that it currently exists and will expand at some point in the future--the question is by how much and when. In answering these questions, the studies seem to have shifted their emphasis. Early studies dwelt on the general decrease in the cost of computing, together with advances in integrated circuits and the growth of telecommunications; they assumed a more direct link between these factors and the increase in the demand for encryption technology. But subsequent research, including the Carnegie-Mellon report, has pointed out that other factors affect the cost of encryption; questions of key management, effective systems protocols, the cost of retrofitting, and the existence of alternate forms of protection must also be considered more carefully.

Another new element in current studies is their focus on the market implications of various government policies toward encryption. In his fifteen-year forecast of cryptography, Whitfield Diffie pays explicit "attention to the possible influence of government regulation" and assumes "that government influence will continue in an irregular pattern much like the present"; he concludes that "federal regulation will not be an all pervasive force in public cryptography."[38] Other contracted studies at SRI International seek to clarify the impact of various federal policy options. One study sponsored by the NTIA Special Project Office will explore the likely effect of three general policies--highly restrictive, no change from the present, and no restrictions--on such factors as private sector research investment, U.S. and foreign technological progress, and the U.S. share of world cryptographic sales.[39]

The other SRI study involves the application of decision analysis to a technology assessment of public-key cryptography. As part of the research, a simple model is used to simulate the impact of alternative federal policies.[40] Preliminary results suggest that market uncertainties, such as the level of computer crime and the growth of electronic communications, have a much greater influence on the use and consequences of commercial encryption than do the policies of either encouraging or discouraging public cryptography.

Examples of policies, aside from prior restraint systems for cryptologic publications, which would affect the commercial market include:

- stricter laws for wiretapping and computer crime which might alleviate the need for some encryption by reducing incentives to intercept or tamper with communications or data. Fewer than ten states have laws against computer crime, and there is no federal law on the books.
- authorization of licensed carriers to provide encryption services.
- tightened corporate disclosure laws.
- legal rulings affecting the extent to which the built-in encryption capability of mainframe computers allowed for intercompatibility.
- subsidies of or taxes on encryption. In addition, the extent of federally promulgated standards and sponsored workshops has already and would continue to affect the marketplace.

In summary, then, two sets of questions must be considered in commercial market studies of cryptography. First, to what extent can the general technological improvement and growth in communications and computers be linked to growth in the use of encryption? And second, what effect will government policies and statutes have on the potential market and vice versa?

The studies themselves also illustrate another activity opening up in commercial cryptography--talking and writing about encryption. Private companies, consulting firms, and institutes have sprung up in recent years to study problems of general computer security and particular encryption techniques. One such group, established in 1974, provides members with a bimonthly newsletter, a "hotline" for immediate help with computer security problems, and a variety of other seminars dealing with data security.[41] There are also several consulting groups which focus solely on encryption and sponsor conferences on the subject.[42] All this computer security discussion has made "the perfect computer crime that will bleed your company dry" a common conversation topic; some find that many of the groups are more hype than help. But overall, these groups have brought a greater awareness of commercial cryptography and dissemination of more sophisticated information on the subject.

As a final indicator of the interest in cryptology, consider the Aegean Park Press Company. The only publisher devoted significantly to cryptologic subjects, it has evolved in ten years to a substantial business.[43] For two years, beginning in 1977, the company printed a scholarly journal, Cryptologia. Its owner, a retired colonel of the Army Signal Corps, receives orders from hobbyists, corporations, and numerous foreign countries including China, Russia, Romania, and Iran. While all the books are based on publicly available information, many security sensitive readers may buy the writings just to be certain that no particularly valuable secrets slip by.

4. Public Cryptography - Policy Points and Problems

So far the analysis has been relatively manageable. The overall changes in the demand for encryption, the increased research in the area, and the existence of some kind of a commercial market were all readily observed. What is much harder to look at are the complex range of issues, from international security to individual privacy, that are raised by open work in cryptology. The first step is to identify the relevant organizations and individuals in and out of government whose interests and capabilities will shape the policy discussions and establish the procedures for coming to grips with the problems of modern cryptology.

One approach that has been taken involves the "dialogue" between the NSA and the academic community. The series of informal meetings and talks between Agency officials and academic cryptologists was institutionalized into a more formal Public Cryptography Study Group funded by the NSF and convened by the American Council on Education. The Group began with the assumption--put forth by Admiral Inman[1]--that open research in cryptology could be harmful to the mission of the NSA and thus the national security. This assumption was accepted as a working premise by most of the members of the Group; discussion was then confined to policies which allowed open research in cryptology but minimized the potential risks to national security. The Group's deliberations have been marked by increased cooperation and communication between the Agency and the academic community and have resulted in a recommendation for a voluntary pre-publication review system.[2]

Another approach to the problems of public cryptography involves the White House and the departments of Commerce and Defense. The two departments were requested by the Science Advisor to derive jointly the necessary elements of a national policy on cryptography.[3] This approach differs from that of the ACE Group in two noticeable respects. First, it considers a much broader range of questions: Who is to be entrusted with the management of encryption in a democracy? Is it necessarily damaging to the overall national security for private individuals to develop and publish cryptographic techniques? What role is the government to play in helping telecommunications carriers and private corporations secure their communications?

Efforts by Defense and Commerce to establish cryptography policy also differ from the efforts of the ACE Group in that cooperation and close communication is less evident. Individual actors within Commerce and Defense, as well as others from GSA, OMB, FCC, and Congress, all perceive markedly different roles for themselves in establishing national policies for cryptography. Each views the area as a small part of a different whole. Cryptology policy is seen in the context of exporting critical commercial or military technology, as a part of privacy protection in information technology, as one area in which the government classifies private ideas, as an important component of foreign intelligence surveillance, and as a vital technology needed to reduce the vulnerability of U.S. communications.

5. NSA and the Universities - The ACE Study Group

The eight-member Public Cryptography Study Group demonstrates one type of mechanism to deal with the issues of public cryptography. It is unusual in that it brings together those who wish to consider regulation with those who might be regulated. The Group has received by far the most publicity of any of the efforts to deal with the problems of non-governmental cryptology. Convened by the American Council of Education in March 1980, the Group included Daniel Schwartz, NSA legal counsel, Ira Heyman, chancellor of the University of California at Berkeley, and six other representatives from industrial and educational societies.

At the beginning, the Group was marked by disagreement. At an early meeting of the Group, Jonathan Knight, the authorized observer from the American Association of University Professors, was quoted in *Science*: "I am not optimistic that we will be able to draw up anything that will satisfy these people [of the study group] with such very, very diverse concerns."[1]

However, one factor--noted by W. Todd Furniss, the ACE coordinator of the Group--which encouraged the members to consider seriously restraints on cryptologic publications was the surprising openness of the NSA.[2] Admiral Inman, along with then legal counsel Daniel Silver, had admitted the problems of the Agency in dealing with previous secrecy orders and the need for a fair and more reasonable approach to limiting dissemination of critical cryptologic information. During the Group's second meeting in May 1980, members were advised by Schwartz and Heyman, a constitutional lawyer, that existing regulations require licenses from the Department of State's Office of Munitions Control for the export of cryptologic devices but not necessarily for scholarly papers, articles, or conferences not specifically related to hardware. The confusion over what constitutes "export" of "technical data" under the International Traffic in Arms Regulations (ITAR) was noted. Furthermore the Group was also made aware that existing statutes do not regulate the domestic publications of unclassified information relating to cryptography.[3]

In discussing whether there should be limits placed on the research, development, and publication of cryptography research, the Group followed Admiral Inman's criteria for such restraints.[4] They should apply only to a central core of critical cryptological information, should be made as clear as possible without revealing damaging information, should include some sort of judicial review and compensation for any loss incurred, and should impose the burden of proof for restriction on the government. The Group considered two basic statutory approaches which would follow the guidelines: (i) a system of subsequent punishment where it would be a criminal offense to disseminate certain defined cryptologic information; and (ii) a system of pre-publication review where publishing without obtaining clearance would be a criminal act.[5] The Study Group chose the pre-publication review system and eventually opted for a voluntary approach which involved no criminal penalties whatsoever.

Before its final recommendation of a purely voluntary system, the Group went through some deliberation regarding the use, as a last resort, of court orders to enforce restraints on publications. The idea had been considered, but Todd Furniss, in writing up the minutes of the meeting, gave the mistaken impression that the Group was in final agreement on the idea.[6] A Science article reported that the explanatory paper prepared for the Group members mentioned the government's authority, on behalf of the NSA, to seek an order from a court to enjoin publication or to proceed with a court enforceable Civil Investigative Demand.[7] The Science article pointed out that the NSA did not have authority to restrain publication and that Civil Investigative Demands applied only to the Justice Department and the FTC in antitrust suits. Furthermore the article mentioned the concern that the NSA might have "something up its sleeve" and might have been deliberately deceptive in light of the confusing paper and the rapid adjournment of the previous meeting. The article ended with a quote from Timothy Ingram, staff director of the House Subcommittee on Government Information and Individual Rights, who questioned the "statutory authority for the censorship" and declared it was hard to see what researchers received in exchange for adopting the review system "other than a cage."[8]

Co-Chairman Ira Heyman disputed the findings of the article in an unpublished letter to Science. He stated that the article suggested erroneously that final agreement had been reached, that the Group had been confused and deceived, and that much was conceded to the NSA. In response to Ingram's image of a cage, he added that researchers, in agreeing to voluntary review, "get an opportunity, after expert scrutiny, to determine for themselves whether or not they wish to risk compromising national security interests."[9]

Following both the Science report and the letter, the Group met again on February 6, 1981. David Kahn, as an observer, and George Davida continued to urge the Study Group to vote against the voluntary restraints.[10] However, except for Davida, the Group approved a purely voluntary system, carefully emphasizing in the wording of their final report the voluntary nature of the review and warning that the recommended system should not be constructed as an endorsement of legislation modeled after the proposed procedures.

The six guidelines of the voluntary system read as follows:

> (1) NSA would notify the cryptologic community . . . of its desire to review manuscripts concerning aspects of cryptology prior to publication. (2) NSA . . . would define as precisely as possible those aspects of cryptology to be covered. . . . (3) NSA would invite authors to send manuscripts to NSA for review prior to publication. (4) NSA would assure prompt review . . . with an explanation . . . of proposed changes, deletions, or delays in publication, if any. (5) NSA would provide . . . an Advisory Committee of five persons (two appointed by the Director of NSA and three appointed by the Science Advisor to the President from a list of nominees provided by the President of the National Academy of Sciences) which would make a recommendation to the Director of NSA and to the author concerning matters in issue. Members . . . shall have adequate clearance. . . . (6) There would be a clear understanding that submission . . . is voluntary and neither authors nor publishers will be required to comply with suggestions or restrictions urged by NSA.[11]

Appended to the committee's report is the dissenting opinion of George Davida. Among his complaints are: (i) restraints would adversely affect the quality and direction of basic research in computer science, engineering, and mathematics; (ii) restraints would enhance the government's ability to issue secrecy orders since existing law disallows the government from issuing such an order when the subject matter has been openly published; and (iii) restraints would be ineffective in achieving NSA's objectives since international publications and other countries would continue to generate their own cryptographic information.[12] Davida also objects to the entire approach of the Study Group in accepting as a working premise the NSA position that open research in cryptology could harm the national security; in his view the national security interests of the country are considerably broader than the narrow mission of the NSA.[13]

Other objections have been voiced from outside the eight-man Group. An editor of Crytologia magazine complained that cryptologic publishers were not represented on the board and also pointed to the fact that Davida was the sole active cryptologic researcher among the members.[14] (Davida was later joined by Professor Hellman, who represented the IEEE, after the previous representative dropped out.) Professor Michael Dertouzos of MIT was also disappointed that his university was not invited to send a representative to the meetings.[15] Dertouzos and others at MIT formed their own committee to look into questions of computer security and to formulate the university's policies for conducting cryptologic research. For over two years, MIT has kept the NSA informed of its research on cryptography by sending the Agency pre-publication copies of potentially sensitive papers at the same time as the papers are sent to professional colleagues.[16] Over thirty papers have been submitted to the Agency without a problem.[17]

However, the main difference between the system at MIT and the proposed system of the Study Group is that MIT researchers are not asking for, or implying any acceptance of, a review by NSA; the papers are sent simply to alert the Agency.[18] Dertouzos believes that the ACE Group's plan, despite its voluntary nature, sets up a potentially distorting relationship between the universities and the NSA. By adhering to the system, a university puts its research directions under the review of a separate government agency; Dertouzos finds that submitting to a review, regardless of its lack of statutory authority, causes the university to treat the NSA reviewers and the appeals board as "elders" and to recognize a subordinate relationship to the Director of the NSA to whom the board reports.[19] Dertouzos, as well as others both in and out of the academic community, also expresses concern that the present voluntary system might provide precedent for a stricter legislative approach in the future.

Legal Counsel Schwartz and others at NSA point out that NSA is not approaching the system with anything "up its sleeve."[20] In their view, Director Inman has approached the academic community with remarkable openness; the Agency itself does not know how the review system will work. It is approaching the idea as an opportunity to cooperate with academic researchers in clarifying and defining what cryptologic information may endanger national security.[21] Study Group member Martin Hellman "would like to encourage this openness" on the part of the NSA and feels a responsibility "to meet the Agency halfway."[22] Also, Jonathan Knight, the observer from AAUP who previously expressed doubts about the Study Group, stated, "I think that what is being proposed is a modest, useful step forward. For the first time an intelligence agency has entered into an open dialogue with the academic community. We're truly in virgin territory."[23]

Several problems lie ahead in this new territory. ACE published the Study Group's report and distributed it to the relevant institutions as a service--without taking a position on the system itself. The NSA will prepare guidelines for researchers to enable them to gauge potentially sensitive material. The balancing act here is to avoid guidelines which are so broad as to stifle basic research unnecessarily, while at the same time to prevent extremely narrow criteria which may tip off adversaries to the exact areas of interest to the Agency.

So far, officials of the NSA have indicated that open publication of cryptologic papers might both alert foreign targets and foster new cryptographic sophistication threatening to U.S. crypto-systems.[24] It is generally perceived by many in the academic community that the threat of decreased foreign signals intelligence is of greatest concern; cryptanalytic papers specifically detailing code-breaking methods and results might be seen as providing other countries with a greater understanding of the flaws in their own encryption systems.

Other potential problems anticipated at the NSA include the possibility that in-house reviewers will be swamped by submitted publications.[25] Each submission requires the valuable time of the Agency's most highly trained and knowledgeable personnel. A large number of submissions could produce a drain on the Agency's resources.[26] Furthermore, researchers may begin submitting papers purely out of interest in the NSA's comments without a direct concern for the national security implications.[27]

The Agency has already begun receiving pre-publication drafts from new sources because of the publicity surrounding the ACE Group. Eugene Yeates, Director of Policy for the NSA, anticipated no problem in issuing a prompt review from within the Agency.[28] What may take more time to establish is the five-member appeals board due to the process of nomination from the National Academy of Sciences and the final selection by the White House Science Advisor. However, Yeates and others at NSA expect the number of appeals reviewed by the board to be only a very small fraction of the number of papers submitted.[29]

From the researcher's point of view, several questions will have to be answered case-by-case. For instance, if the NSA should recommend against publication of a paper, how long will the recommendation hold? Will the Agency instruct the researcher as to what parts of the paper are particularly critical and enable him to rewrite and publish a less-sensitive piece? Researchers have envisioned several scenarios which could provide unique tests for the system. What if a graduate student made a major discovery that not only revealed how to break certain codes, but also had important consequences in scheduling theory? How would the situation change if the student was not American?[30] Professor Davida has also posed the possibility that new research could document new, efficient methods for factoring large numbers.[31] These results might have profound national security implications; if concealed, the results would leave any cryptosystem currently using the RSA public-key algorithm highly vulnerable.

6. In Search of a National Policy for Cryptography - White House, Commerce, and Defense

In addition to the narrowly defined arena of the ACE Study Group, a broader forum has been established to consider the issues of public cryptography. This broader forum first developed as a result of the classified Presidential Directive/National Security Council-24,[1] described as recognizing the vulnerability to interception of unclassified government telecommunications of value to a foreign adversary. The Directive assigned responsibilities to various government agencies and established national policy guidelines as follows:

> 1. Government classified information relating to defense and foreign relations shall be transmitted only by secure means.
> 2. Unclassified information transmitted by and between government agencies and contractors that would be useful to an adversary should be protected.
> 3. Non-governmental information that would be useful to an adversary shall be identified and the private sector informed of the problem and encouraged to take appropriate protective measures.[2]

The flow of authority outlined in this Directive proceeded from the National Security Council Special Coordination Committee to the Sub-committee on Telecommunications Protection. From there, authority split two ways: (1) through the Secretary of Defense, Executive Agent for Communications Security, to the Director, NSA; and (2) through the Secretary of Commerce, Executive Agent for Communications Protection, to Administrator, National Telecommunications and Information Administration (NTIA).[3]

The government apparatus to deal with cryptography was further defined in a Telecommunications Protections Policy Directive issued from the White

House on February 17, 1979.[4] The Directive placed responsibility for policy guidance with the NSC Subcommittee of Telecommunications Protection chaired by the Director, Office of Science and Technology Policy, with administrative support provided by the Secretary of Commerce and including representatives from the Cabinet departments, the CIA, the NSA, and others.[5] The Secretary of Defense was given responsibility for government-derived classified and unclassified information relating to national security; the Secretary of Commerce was to protect government-derived unclassified information (excluding national security information) and to deal with the commercial and private sector to enhance their communications security. The Directive also stated:

> It is recognized that there will be some overlap between the responsibilities of the Executive Agents, in that Defense will provide some non-cryptographic protection for government-derived unclassified information as it does now, and Commerce will have responsibilities in commercial application of cryptographic technology. The subcommittee [of the NSC] will review such areas on a case-by-case basis and attempt to minimize redundancies.[6]

With this structure in place, in November 1979 the White House Science Advisor asked the Secretaries of Defense and Commerce to draft guidelines for a national cryptography policy.[7] Elements to be considered included current practices and future needs for cryptography in the private sector, the issues of academic freedom, and NSA's missions of communications security and signals intelligence.[8] Although others throughout Commerce and Defense were included in the policy considerations, two principal groups involved were the NSA and the NTIA Special Project Office.

The results have not been conclusive as of April 1981. Defense has submitted a brief set of principles which many in Commerce feel have overemphasized NSA's national security concerns and overlooked the broader security concerns of the private and commercial sector. Commerce in turn has submitted a thick, detailed White Paper identifying numerous policy levers and recommending measures to encourage the development of commercial cryptography; officials at NSA and other parts of Defense find that the proposal is extremely questionable in light of its seeming neglect of the national security concerns involving signals intelligence, communications security, and the authority of the NSA.

Both proposals ended up being prepared separately. The NSC subcommittee designed to coordinate the joint efforts met only once while the working group, composed of mid-level officials, eventually broke apart as joint discussions became "very painful."[9] Part of the breakdown may be explained by the fact that the group never received the sustained attention of the higher level deputy and assistant secretaries of the respective departments; the heads of the involved agencies did not place the working group high on their agenda. However, part of the tension also stems from the different doctrines, ideologies, and organizational habits of the Commerce and Defense agencies and the unique perspective of the NSA. What follows is a brief caricature of opposing points of view which, while overstated to the point where it no longer represents any individual opinion, may be helpful in understanding the fundamentally different perspectives.

Those outside the Defense Department cannot shake the idea that the Department is pursuing a single-minded attempt to keep the high technology needed for encryption out of the hands of many in industry; they point to various policies including the ITAR, the new Defense regulations discouraging universities to allow foreign students to work on integrated circuits, and the inclusion of cryptologic equipment on the critical technologies list. They have the impression of Defense classifiers as technocrats "wearing green eye-shades." Furthermore, in their dealings with NSA personnel, they are left with the impression of a highly compartmentalized organization whose representatives have only a narrow understanding of both the Agency's dealings and the broader national security concerns of officials in Commerce and industry. It is also resented by some that the Agency has not seemed willing to negotiate and interact as closely with other government agencies as it has with the academic community and the ACE Study Group.

Officials within the Defense community and in NSA are inclined to view such Commerce organizations as NTIA as originating largely from political gestures. While NTIA has only existed a few years and does not have a great background of technical expertise, workers within NSA are conscious of the longer history of their Agency. The dramatic code-breaking work of American cryptanalysts during WWII are still vivid; more recent successes of the NSA during SALT negotiations and at other times are also salient to Agency employees. Furthermore, technicians and scientists in the Agency have managed, through careful planning, to stay several steps ahead of the outside cryptologic community. Those responsible for communications security have designed their crypto-systems using a fifty-year time frame--ten years for exhaustive testing, twenty to thirty years for guaranteed secure performance, and another ten years on the end to insure that the very last message transmitted is not compromised. These designers are very much aware of their responsibility to maintain the communications systems of the defense and diplomatic communities; they are inclined to see actions at Commerce as very short-term and not as carefully thought out. Finally, those at the Agency involved in the separate mission of monitoring and analyzing foreign communications are far more aware than outsiders of the fragility of their sources of intelligence--sources which are overlooked by or unknown to those outside the Agency.

As an example of where these mixed perceptions can lead, consider an account of the development of a national radio navigation plan.[10] Originally NTIA felt that it had the lead coordinating role, by Executive Order, to develop the plan involving the FAA, Defense, the Coast Guard, and others. OMB, on the other hand, felt that the matter was a question of management and that it should be in charge. After two months of argument a co-chaired interagency group under the NSC was established very similar to the one set up for cryptography issues. NTIA suggested Defense use its whole family of satellites to share its high-precision positioning data with other users; some at State felt this policy was sound since it would help international relations to make this precise navigational ability available to other parts of the world. Defense was "apoplectic" at this idea, since the system's precision was designed to improve ICBM accuracy; it did not want that type of information available to possibly hostile forces. After a struggle, OMB declared that the system was so expensive that it could only be funded if other navigational systems--including those used by civilian airliners--were cancelled.

Because of these kinds of mixed perceptions, because of a lack of sustained attention by the heads of the respective Departments, and because of pressing needs elsewhere, no action has been taken at the Office of Science and Technology Policy (OSTP) on a national cryptography policy. Prior to March 1981, the need for OSTP itself was being debated among White

House advisers. The Reagan Administration has decided to maintain the Office of Science and Technology Policy within the White House but has also reduced its budget and cut back its permanent staff.[11]

Colonel Wayne Kay, the senior analyst at OSTP responsible for cryptography, is not certain what direction the search for a national policy on public cryptography will take. He points out that Defense and Commerce were originally asked to derive the elements they thought a national cryptography policy should contain rather than propose the policy itself; Defense, in preparing its set of elements, seems more aligned with this original idea.[12] However, Colonel Kay said that he has not had the time or the resources in the early months of 1981 to fully evaluate the Defense or Commerce proposals. More pressing policy matters, including institutional adjustments and orientation of new administration leadership, have kept the public cryptography policy issue on the "back burner."[13]

Yet, according to Colonel Kay, the needs of the Defense and intelligence communities, as well as the needs of the public sector, must be recognized; information protection on a national scale is too compelling an issue to maintain a status quo attitude.[14] What is necessary today is a coherent national policy embodying a set of principles which recognize and account for our national security requirements, on the one hand, and the public need for legitimate cryptographic techniques, on the other. Striking the necessary balance between these entities will not be easy, but no one who understands the issue can disagree on the need for such a policy.[15]

7. Possible Directions for the Future

So far, government influence in both the development and application of public cryptography has not followed any clear path. NSA has begun to voice its doubts regarding open research in the area; other agencies outside the Defense Department have encouraged an awareness of the need for commercial and civil encryption throughout industry and government. While there is a broad range of conceivable government approaches to the management of public cryptography, three possibilities are easily imagined: (a) a more centralized development and application of civil sector cryptography under the umbrella of a single organization; (b) the creation of competing expertise by establishing a substantial communications security branch of government outside the military and intelligence community; and (c) a continuation of the irregular pattern visible today where federal regulation becomes less of a driving force than market conditions and privately developed standards.

a. More Centralized Management - The NSA

A more centralized development and application of cryptography for both classified and unclassified needs has already been considered in terms of the networks involved:

> By the early nineties voice and data communications networks using DES will be common throughout the federal government and these networks will exist side-by-side with comparable facilities for classified communications. The cost of this redundancy, coupled with a possible decline in cryptanalytic communications intelligence, may lead the government either to declassify one of its own cryptographic systems or to accept an outside system as adequate for classified use and thereby adopt a single system for all government

communications.[1] (emphasis added)

The organizational parallel for this combination of classified and unclassified networks into a single communications system would be the centralization of government communications protection efforts within a single agency or department. Any such effort must involve the NSA, the organization with the greatest interests and capabilities in cryptology.

The NSA currently operates within the Defense Department as a separately organized agency with two primary missions--communications security and signals intelligence.[2] To carry out these missions, NSA prescribes certain U.S. government security procedures, manages activities for the production of foreign intelligence information, and coordinates the research and engineering activities required to support the Agency's assigned functions.[3]

Congressional review of the NSA continually points out the Agency's lack of a statutory charter governing its activities. The primary concern has been over the Agency's foreign intelligence mission shading into domestic intelligence activities. Congressional investigations have noted that "no existing statutes control, limit, or define the signals intelligence activities of the NSA," and have pointed to occurrences in the late 1960s when NSA and other intelligence agencies were asked to produce "foreign intelligence" on domestic activists.[4]

What currently defines the role of the NSA is Executive Order 12333, along with the Foreign Intelligence Surveillance Act of 1978. On December 4, 1981, President Reagan's directive set forth new details on the tasks of various intelligence agencies including the NSA.[5] In the order, the NSA was given exclusive control over signals intelligence--both the collection and dissemination of "signals intelligence information for counterintelligence purposes" and "signals intelligence support for the conduct of military operations."[6] As to domestic surveillance, Director Inman responded in his unprecedented public speech:

> NSA has no interest, and indeed is legally precluded from intercepting domestic communications. These legal restrictions formerly imposed by Executive Order, have been embodied in the recently passed Foreign Intelligence Surveillance Act of 1978.[7]

Not everyone is satisfied with Admiral Inman's assurances, and even the most conscientious Agency imaginable will run into problems defining domestic and foreign when, for instance, it monitors transmissions abroad that tie into domestic conversations.

This general confusion over NSA's overall mission--and its role in the development of public cryptography--could conceivably be defined and clarified in a more expansive legislative charter. This would require further attention not only to the signals intelligence mission of the Agency, but also to its communications security responsibilities. Michael Dertouzos, of the MIT laboratory for Computer Science, expresses the opinion that the NSA might play a more effective role in the development of unclassified communications and data protection.[8] He is opposed to the ACE Group's system of voluntary review. However, he asserts that the experience and expertise of the Agency in protecting communications could be of great use to the civil sector. He suggests that NSA's role in the management and development of public cryptography might be explicitly outlined in legislation.[9]

The now defunct National Intelligence Reorganization and Reform Act

(S. 2525) nicely illustrates the complexities involved with this kind of approach. Under the Act, the National Security Council would develop "policies governing the circumstances . . . under which departments and agencies may furnish to United States persons information and materials regarding the vulnerability of non-governmental United States communications."[10] The bill would have given NSA responsibility to:

> evaluate, based upon policy guidelines from the Attorney General, the vulnerability of the United States communications to interception and exploitation . . . and, under the supervision of the Secretary of Defense and in accordance with policy guidance from the National Security Council . . . institute appropriate measures to insure the confidentiality of such communications.[11]

These provisions of the bill seem relatively uncontroversial. Furthermore, the benefits of using the unmatched expertise available at NSA for communications security could be considerable. Observers of the NSA have described the Agency as composed of three operational units--the research and development branch, the signals intelligence and data gathering branch, and the communications security (COMSEC) branch.[12] Officials at NSA describe COMSEC as a decidedly separate unit, housed in a separate building and operating with a different philosophy. Its interaction with other branches of the Agency is limited, and it is described as dedicated solely to the protection of classified and other information related to national security.[13] This kind of capability would presumably be necessary to perform the greater domestic role outlined in the now defunct bill.

While the bill would have expanded NSA's role in protecting domestic communications, it also would have increased the Agency's control over private cryptology development. A section would have modified the U.S. Code to include the following paragraphs:

> Patents and inventions in the provision of security, confidentiality, or privacy of communications or other forms of transmission of data, or incorporating sensitive cryptologic techniques, which in the opinion of the Director of the National Security Agency, if published, might be detrimental to the national security, shall be handled in accordance with the provisions of this section as if the Commissioner had determined that the publication or disclosure of any such invention by the granting of a patent might be detrimental to the national security.
>
> The Register of Copyrights shall take all such steps as may be specified by the Director of the National Security Agency to secure from disclosure any material which might otherwise be subject to copyright protection which involves the provision of security, confidentiality, or privacy of communications or other forms of transmission of data, or incorporating sensitive cryptologic techniques which in the opinion of such director, if available for public inspection and copying, might be detrimental to the national security.[14]

This is exactly the type of statutory control over private research and publication that has been rejected by the Public Cryptography Study Group and by researchers throughout the field of mathematics, engineering, and computer science.

Of course, S. 2525 is only one approach that gives NSA more control over management of unclassified cryptography applications. However, it points out two important questions that must be considered if NSA is to play a larger and more clearly defined role. First, what organizational structure can support the communications security needs of both the civil and military sectors of the U.S. without compromising the highly classified signals intelligence mission? And second, how can NSA provide expertise and advice without exerting undue control over research and development in the private sector?

To begin to address the first question, the internal organization of NSA must be considered. As mentioned previously, there is some potential that the COMSEC branch of the Agency might fulfill the requirements of a single unit for both classified and unclassified communications protection. As its current operations are described, the COMSEC branch is privy to the latest cryptanalytic techniques that are developed in the signals intelligence branch of the Agency.[15] However, COMSEC operates apart from this branch, relying on its own in-house adversarial system to test the adequacy of secure codes.[16] The COMSEC unit thus suggests possibilities for broadening the Agency's interests and capabilities in unclassified, and possibly non-governmental, communications protection; the two possible advantages of this approach are more available expertise from the COMSEC experts and an Agency more responsive to the broader encryption needs of the U.S.

The problems are seen as the second question--how the Agency provides expertise without exercising control--is addressed. Would a new encryption hardware manufacturer approach the NSA directly with his device and present it for design advice? Or should the NSA, in any advisory role, follow the example of the NBS and restrict its role to just certifying whether or not a given device or system meets a specified standard? Either approach raises problems inherent in any government aid to the private sector. The problems are magnified if any certification efforts become, or are viewed as becoming, methods by which the Department of Defense is controlling the civilian community.

Beyond the question of hardware devices on the market, there is also the area of future research and development. The question of NSA involvement in academic research has already been considered by the ACE Study Group. How the Agency works with industry in research and development has received far less public attention. It has been reported that much of NSA's research, including work on "standardization of cryptological devices and voice scramblers used by federal agencies,"[17] is contracted out to a private organization, the Institution for Defense Analysis (IDA). NSA and IDA are also reported to circulate periodicals and papers to a restricted set of readers who are involved in contract work. How much of this restricted work should be made public in order to aid civil and private users of encryption?

Any increased role by the NSA in the field of public cryptography will come under the scrutiny of the various Congressional Appropriations and Oversight Committees. The extent of NSA's dealings with Congress is no longer restricted to a short meeting each year with the Appropriations chairmen; the Agency now has far more public dealings with Congress. In 1978, Admiral Inman approached the House and Senate Select Committees on Intelligence with the idea that if NSA "had to go through an inquisition, we [NSA] ought to look for a forum."[18] He found that "if the congressional committees established the requisite security, you could engage in a steadily ongoing dialogue about the things you had to do to collect your information" and would more likely "get better support for a stronger, healthier intelligence structure."[19] Should NSA's structure be expanded to include more involvement in public cryptography, congressional oversight will presumably become central to maintaining the Agency's public accountability.

b. Greater Civil Sector Development - NBS, NTIA

Another possibility for future government efforts in unclassified cryptography, besides centralizing management of public cryptography within NSA, is the creation of greater expertise in communications security elsewhere in the government. The possible advantage of this approach would be a more balanced approach to the broader concerns of commerce and industry in secure telecommunications. The problems include a lack of comparable expertise available outside the NSA and a failure really to settle the conflict between signals intelligence concerns and civilian communications security.

If more expertise is to be institutionalized outside NSA, one place to look is at the Department of Commerce, particularly the NTIA and NBS where some governmental apparatus is already in place. As to which of the two offices would be more appropriate, past experience may give some clue. Officials at NTIA have typically been generalists; only a handful of "experts" are currently working on encryption-related topics and policies. Charles Wilk, of the NTIA Special Project Office, finds that more technical expertise may be available at NBS for work in encryption.[20]

At NBS, the Institute for Computer Sciences and Technology has been responsible for developing standards for protecting unclassified, non-national security information processed in computer systems. Also NBS has already made a significant impact on non-governmental cryptology through its workshops and development process with the DES. In addition, NBS Publication List 91 identifies its other work which includes Security

Audit Evaluation, Data Base Security, Network Security, Privacy, Security Controls Safeguards, and General Computer Security. In conjunction with the Federal Telecommunications Standards Committee, NBS has an ongoing effort in developing computer communication protection standards. Under the guidance of the NTIA, these efforts may be expanded to include standards for protection in broader areas of telecommunications. Within its own distributed data network, NBS is implementing the capability to protect communication between any nodes of the network, person-to-person secure digital "mail," secure "mailboxes" of digital information, and digital signatures appended to digital documents.[21]

Presumably NBS might begin applying some of this in-house expertise toward cryptography development outside the Bureau. The statutory authority for this work would come from the Brooks Act (P.L. 89-306) which authorizes Commerce to provide "scientific and technological advisory services relating to automatic data processing and related systems" and to make recommendations relating to "the establishment of uniform federal automatic data processing standards."[22] In addition, the Privacy Act of 1974 provides direction for establishing the security of record keeping systems.[23]

Currently the Bureau of Standards appropriations included about $11 million for computer science and technology for fiscal year 1981 with about $12 million for the subsequent year.[24] Activities under way at the Bureau include work on several proposed standards using DES in new modes of communication. The Bureau is expected to strengthen the current standard to meet requirements five to ten years from now. Whitfield Diffie, in his fifteen-year cryptology forecast, sees new directions available to the Bureau. By 1990, "the Data Encryption Standard is certain to need replacement but what form the replacement will take is as yet uncertain."[25] Diffie sees the "most obvious possibilities" as using the old DES and performing multiple encryption, increasing the key size or redesigning a similar system with a larger block size. He also sees that new developments in cryptographic technology provide other directions: (i) an adequate public-key system may be developed and achieve general acceptance; and (ii) advances in complexity theory may give rise to a provably secure system, making for a much higher degree of certainty in the security of crypto-systems.[26]

If NBS is to play a larger role in these suggested developments, a central question will have to be considered. To what extent will NBS be independent of NSA? Dennis Branstad, the leader of the computer security project, and several others involved in the development of DES are ex-NSA employees.[27] This had led some to speculate that the standard was designed more for the intelligence community than the public and that NBS "fronts for the NSA."[28] Although the Senate Intelligence Committee Report completely cleared NSA of any improper involvement in the DES, apprehension still remains among university and industry researchers regarding NBS connections with NSA. How much of the considerable expertise available at NSA should be used by the Bureau of Standards in its future work?

The difficulty in answering this question is clearly seen in the context of the new public-key technology. Outside cryptologists, such as Diffie, see great possibilities for public-key systems, yet officials at NSA continue to downplay the new technology. They point out that the security of public-key systems rests on the assumption that solutions to problems such as factoring large numbers will continue to remain unknown; in contrast to reliance on unknown principles, the DES uses relatively known methods to maintain the secrecy of tne message.[29] To what extent snould tne NSA's general comment on the new technology be considered? Some nave speculated NSA's view stems from a desire to limit the spread of metnods, such as public-key systems, which will result in greatly increased use of encryption. On tne otner hand, since NSA has claimed to have already developed practically every new form of cryptography now emerging,[30] it is not inconceivable tnat the Agency nas already examined public-key systems closely and determined definite weaknesses in tne methods used.

c. Uncontrolled, "Event-Driven" Development

As long as encryption remains a low priority for most federal agencies and large corporations, it is fair to speculate that no system at all will be establisned to manage tne development and application of civil sector cryptography. Tne possible advantages of a "hands off" approacn is tnat it allows tne encryption market to respond to the signals of price and demand without introducing any distortions or biases of a single regulatory agency. However, a lack of centrally determined standards or policy initiatives may also lead to incompatibility among various secure systems and a general unwillingness among network users to invest in encryption technology.

Without a central plan or system, tne series of separate actions now emerging from several government agencies can be expected to continue:

NTIA: The Special Project Office of NTIA nas, as of March 1981, a number of activities under way including publisning and updating a User's Guide for encryption devices on the market, evaluating existing carrier vulnerabilities and protection capabilities, and proposing a national policy for cryptography.[31]

The Special Project Office is collecting information on protection techniques ranging from limited protection terminals for voice and data facsimile to bulk encrypted services, possibilities for avoiding vulnerable transmission routes, as well as other network-oriented techniques. The Office is also interested in the problem of defining what level of protection is in the "national interest" and how costs should be allocated to meet that level.[32] One view might suggest protecting vast amounts of government telecommunications, leading to extensive bulk link protection for many common carrier facilities. On the other hand, if those communications worth protecting prove manageably small in proportion to the total, then end-to-end, terminal-oriented encryption might be used for a small number of protected carrier circuits.

How costs are allocated would obviously depend on the methods of protection chosen. Limited end-to-end protection terminals would represent a direct cost to all taypayers; carrier-provided bulk encryption would probably be realized through a special tariff--perhaps a less direct burden on taxpayers. The NTIA Office is also considering what form of legislation, regulation, or government subsidy may be needed to motivate carrier cooperation. Overall, the NTIA activities will strive to:

> encourage the development of protections and innovative technologies, with minimum disruptions to industry structure, and with consideration to total cost and future flexibility factors. Maintaining a competitive environment will remain an important objective.[33]

GSA: The General Services Administration, as the government's central procurement agency, has prepared technical specifications for procuring protected telecommunications services. GSA's Federal Property Management

Regulations require each government agency to review its operations "to ensure that threats and hazards to data confidentiality and security are properly identified, and that appropriate safeguards are implemented."[34]

Also, the GSA, as network manager for the Federal Secure Telephone System and the entire Federal Telecommunications System (FTS), may evolve as a major government user of encryption technology. Based on the facilities of commercial carriers, the FTS is a mammoth telecommunications system for government and agency users; it services some 200 million voice, data, and facsimile calls each year.[35] The services are used by most federal agencies to conduct day-to-day business, including providing general information such as weather forecasts and personal information such as Social Security, IRS, or Veteran's Administration records. The FTS also handles more sensitive information including plans to alter the government lending rate to banks, information regarding advanced technological research and development, levels of reserve stockpiles of critical materials, and certain government bargaining strategies for international negotiations.[36]

The GSA is selectively focusing its efforts toward reducing vulnerabilities. For example, expanded technical specifications have been prepared so that carriers and equipment manufacturers can bid on protected circuits.[37] For an Alaska-U.S. mainland satellite link, the GSA will use bulk-link encryption to provide protection. In another case, mainland-to-offshore service is being provided by coaxial cable rather than by satellite in order to reduce exposure to interception. Elsewhere, in the interest of economy as well as security, GSA plans to take advantage of opportunities to share some secure Defense Department circuits. This sharing emphasizes the continual blurring of civilian-military uses and needs for cryptography. The independent procurement activities of GSA raise questions of organizational authority and NSA's primary role in U.S. communications security needs.

OMB, FCC, and Congress: As mentioned previously, the Office of Management and Budget has instructed federal agencies to safeguard data processing and telecommunications systems. As a result, agencies are reviewing their requirements and reporting to OMB on their plans for any increased protection.[38] In addition, the Federal Communications Commission is involved in reviewing vulnerabilities in the public communications networks, and may initiate proceedings to assess the public demand for improved privacy and confidentiality.[39] Any actions the FCC might consider will raise the same questions faced by NTIA of who pays and how much. In 1977, the estimated cost of scrambling the 68 percent of all domestic calls now transmitted by microwave was as high as $3 billion.[40] Such a high price suggests that costs would have to be spread among private users--AT&T has already been asked to plan new ratings for telephone service that would allow the subscriber to choose and pay for various levels of security.[41]

Congressional interest, as indicated by the GAO report on federal telecommunications and the House Government Operations Committee hearings, can be expected to continue. Senator Max Baucus, of the Senate Judiciary Committee, and Representative Richardson Preyer, of the House Government Operations Committee, have both called for more investigation into the impact of new telecommunications technology on government information practices.[42]

Aside from the government activities mentioned, there is also the work of the American National Standards Institute, the clearinghouse for nationally coordinated voluntary standards. It remains to be seen if the

Institute can establish widespread standards to ensure compatibility among encryption products. It has been noted that "large computer manufacturers often do not collaborate in the setting of standards, since standards increase the possibility of competition."[43]

> Computer and terminal manufacturers with smaller market shares favor standards because they open up new markets that would not be economically viable without the resource-sharing advantages that standardization implies. Carriers, on the other hand, generally favor standards since (a) network interworking is an important user requirement, and (b) the monopoly situation often eliminates competition for the carriers anyway.[44]

Lack of compatibility--together with the lack of any powerful government agency concerned with compatibility and computer security--would prevent potential users from investing in cryptographic equipment that could close off their system from other networks. Given the trend toward computer-to-computer connections, this lack of compatibility could inhibit the use of encryption precisely where it is most needed.

However, in place of the compatibility argument, it can be argued that the lack of sufficient government or private standards is not the limiting factor. What is often said of the commercial cryptography market holds true for the policy areas as well: the field is "event-driven" or "event-oriented." Every field of research can be said to follow the course of certain striking events, but the case for cryptography is especially strong. In the policy arena, nothing is set. Inman's efforts to start an open dialogue have not been formalized; no specific legislation is dictating prior restraints. The effect of the Public Cryptography Study Group's recommendations is not yet evident, and there are no major deadlines forcing the pace of the policy debates within the federal government. Similarly, the commercial customers for encryption are in no big hurry. Many sectors are waiting for industry leaders to start the trend toward encryption. While they wait, many feel the time is ripe for a major wiretapping incident.

David Kahn is waiting for "the computer equivalent of Three Mile Island."[45] Others have gone so far as to estimate the amount--$50 million--that will have to be lost to wiretapping before any major shake-up in cryptography occurs.[46] Should such an event occur, it will undoubtedly accelerate the demand for encryption technology. However, it is not clear whether a major wiretapping incident would encourage more government control of cryptography and, if so, whether this control would fall to the intelligence agencies or to Commerce.

"Intelligence Community Can Look Forward to New Era of Secrecy" read a post-election headline in the Washington Post. The article went on to explain that "new directions . . . remain to be determined, but one thing appears certain: a new era of secrecy will be sought."[47] Barry Goldwater of Arizona, it was reported, was likely to prove a less critical watchdog of the intelligence community than defeated Birch Bayh, Jr. In speculating on the new head of the CIA, the new Intelligence Committee chairman was quoted: "'There's an awful lot of interest in Admiral Inman,' Goldwater volunteered; 'I think he's the most capable man in the field. I could put all my trust in him.'"[48]

The speculation contained in the article proved somewhat unreliable in regard to the CIA and may prove unfounded altogether. Admiral Inman has been chosen by President Reagan to take the number two position at the CIA,[49] but no specific predictions have been made on how this will affect

NSA and its stance toward public cryptography. Admiral Inman did comment, however, on the 1977 policy decision that two separate government elements (Commerce and Defense) were needed to deal with communications security. In April 1981, in remarks to a seminar on intelligence issues at Harvard University, he expressed the personal opinion that the reason for the joint management of crypto-policy stemmed from the belief that an intelligence organization could not be trusted with involvement in the part of communications security which related to the private sector.[50] Furthermore, he remarked:

> I do not find the result of four years of separate effort very productive, and if I were making the decision, this would be one area which I would do some early swift surgery to cut the size of the government bureaucracy and go back to a single body. But I do not know that that's what the decision will be at all, and I would be loath to make any predictions about how it will be.[51]

NSA Director of Policy Eugene Yeates stresses that NSA will not "go back in our shell"; he expects the Agency to continue its efforts to be more open with industry and the universities.[52] Lt. General Lincoln D. Faurer, Director of NSA as of March 1981, has said his Agency would try to establish the ACE Group's proposed review procedure and invited researchers, scholars, writers, and publishers to cooperate.[53]

The NSF also has a new director and plans to increase its support of engineering and applied science,[54] but the effect of this shift on cryptographic funding has not been discussed. The NTIA Director of the Special Project Office, Donald Kraft, "wouldn't look for a lot of change" from the new Administration but also added that the decisions were not his to make.[55]

Several legislative and judicial actions may also affect debate in the area of cryptography, though their immediate effect is not evident. On December 12, 1980, a wide-ranging amendment to patent and copyright laws extended copyright protection to computer programs.[56] The amendment (P.L. 96-517) also changes patent laws to "permit universities, small companies and non-profit organizations to retain ownership of patents gained as a result from federal grants and contracts."[57] The new amendments hold implications for current and future cryptographic research grants as well as any attempts to compensate parties for economic losses due to dissemination restraints. In addition, the Supreme Court ruling allowing some computer programs patent protection will have a bearing on these issues, but patent lawyers are "still digesting the decision."[58]

As a final indication of things to come, consider the following situation described in a 1980 issue of Security Management:

> A federal law enforcement agency has found its job complicated by interceptions of its mobile communications. Alert lawbreakers are sometimes forewarned of arrest, and unwanted onlookers show up beforehand at the site of arrest.[59]

Interception is even simpler for public safety and police communications using mobile radio-telephone systems. This is because of new, microprocessor-based scanner devices which provide automatic searching functions; the receiver need not know the frequency used by a particular organization. After the listener simply programs the system for the frequency limits of interest, these devices automatically scan the frequency ranges to intercept traffic. In fact, the newest scanners automate the frequency range selection process. Industry sources have estimated that about 10 percent of American households have a scanner device, and there are about a half-dozen manufacturers of the scanners, which sell in drug stores and hobby shops for a few hundred dollars.[60]

Now most of the scanners are used for recreational purposes; they have also encouraged public support and assistance to policy and emergency services. However, the same devices can be used by lawbreakers to stay one step ahead of the law. At what point, if any, should the ownership of these scanners be controlled to prevent such abuse? Or should the police and others begin encrypting and scrambling their messages? Would the benefits from such a practice outweigh the benefits of public assistance and the general right to know of policy actions? And, on another side of the issue, will the voice scramblers commonly available today impose significant cost on the police and the FBI in their wiretapping operations? Could these costs ever justify limiting the market for voice protection devices?

Whether these domestic concerns will affect other international issues involving cryptography remains uncertain. But there is little doubt that improvements in unclassified cryptologic technologies will continue to raise questions at local, national, and international levels which must be addressed.

NOTES

Section 1

1. Kahn, David. The Codebreakers (New York: Macmillan Company, 1967), p. 716.

2. Christian Science Monitor, December 5, 1980. p. B18.

3. The Economist, November 1, 1980, p. 95.

4. ACM Computing Surveys, December 1979, pp. 321-23.

5. Ibid. A less arcane application for public-key encryption is missing authentication. The point is covered on infra p. 41.

6. Time, November 3, 1980, p. 25.

7. Mathison, Stuart and Philip Walker, Computers and Telecommunications: Issues in Public Policy (Englewood Cliffs, N.J.: Prentice Hall, Inc., 1970), p. 12.

8. "User's Guide. Voice & Data Communications Protection Equipment," Special Project Office, NTIA, Department of Commerce, December 1980, p. 1.

9. Security Management, August 1980, p. 52. Wilbur Alderson of AT&T notes that, while the present mix of message transmissions is 70% microwave and 30% cable, by 1995 it may become more like 70% cable (largely optical fiber) and 30% microwave. Personal Communications, January 1982.

10. NTIA "User's Guide," p. 5.

11. Security Management, August 1980, p. 52.

12. NTIA "User's Guide," p. 5.

13. Ibid.

14. Progressive, November 1980, p. 19.

15. Security Management, August 1980, p. 52.

16. Ibid.

17. Parker, Conn B. Crime by Computer (New York: Scribner, 1976), p. 3.

18. Ibid., p. 4.

19. Ibid.

20. Information Privacy, September 1980, p. 185.

Section 1 Notes (Continued)

21. Washington University Law Quarterly, Vol. 1976:667, p. 670. See also, Hearings, Subcommittee on Constitutional Rights of Senate Committee on the Judiciary, 93rd Congress, 2nd Session, Federal Data Banks and Constitutional Rights.

22. Foreign Affairs, Fall 1979, p. 157. See also, Department of Commerce, NTIA, Selected Foreign Data Protection Law & Laws, Special Publication 78-19 (Washington, D.C.: GPO, 1978.)

23. Information Privacy, July 1980, p. 173.

24. The Privacy Act, Public Law 93-579, 93rd Congress. S. 3418, December 31, 1974.

25. Ibid.

26. Office of Management and Budget, "Security of Federal Automated Information Systems," Circular No. A-71, Transmittal Memorandum No. 1, July 27, 1978.

27. "Increasing Use of Data Telecommunications Calls for Stronger Protection and Improved Economies," General Accounting Office, November 12, 1980, LCD-81-1, p. 21.

28. Ibid., p. 7.

29. Ibid., p. 21.

30. Ibid., p. 22.

31. Ibid., pp. 35, 41, 42.

32. Ibid., p. 48.

33. Communications Security and Banking, published by Racal-Milgo Inc., 1980.

34. Results of an Initial Attempt to Cryptanalyze the NBS Data Encryption Standard, Stanford Electronics Laboratory, November 10, 1976, pp. 3, 4.

35. Science, July 29, 1977, p. 437.

36. Stanford Electronics Laboratory, op. cit., pp. 3, 4.

37. Washington Post, October 4, 1977, p. c17.

38. Ibid.

39. U.S. Government Manual, p. 401.

Section 1 Notes (Continued)

40. National Telecommunications Protection Policy Directive, February 17, 1979, p. 1.

41. NTIA "User's Guide," December 1980 (see note 8).

42. Victor Walling, Donn Parker, and Charles Wood, "Impacts of Federal Policy Options for Nonmilitary Cryptography," SRI International, Menlo Park, California, Project 1663, p. ix.

Section 2

1. Kahn, David. The Codebreakers (New York: Macmillan Company, 1967), p. 71.

2. U.S. Code Congressional and Administrative News, 1965, Volume 1, P.L. 89-306, par (f), p. 1135.

3. IEEE Communications Society Magazine, November 1978, pp. 6, 7. See also, Executive Order 11905.

4. United States Government Manual 1980-1981, Government Printing Office, May 1980, p. 259.

5. Executive Order 11905, February 18, 1976, section (e), 2(ii)(F).

6. J. L. Smith. The Design of Lucifer, A Cryptographic Device for Data Communications, Research Report RE - 3326, IBM, 1971.

7. Data Encryption Standard, FIPS Publication 46, U.S. Department of Commerce, National Bureau of Standards, January 15, 1977. As issued, the DES strictly applies only to Federal uses and is not an official U.S. standard for the private or non-federal public sector.

8. Information Privacy, May 1980, p. 109.

9. Ibid, p. 110.

10. Ibid.

11. Science, July 29, 1977, p. 438.

12. Ibid., p. 440.

13. Foreign Affairs, Fall 1979, p. 151.

14. Unclassified Summary: Involvement of NSA in the Development of the Data Encryption Standard, Staff Report of the Senate Select Committee on Intelligence, 95th Congress, 2nd Session (April 1978).

15. Personal Communications, Professor Martin Hellman, Stanford University.

Section 2 Notes (Continued)

16. Results of an Initial Attempt to Cryptanalyze the NBS Data Encryption Standard, Department of Electrical Engineering, Stanford, CA, September 9, 1976.

17. IEEE Transactions on Information Theory, November 1976, pp. 644-654.

18. Information Privacy, July 1980, p. 142.

19. Communications of the ACM, February 1978, pp. 120-126.

20. Reason, January 1981, p. 32.

21. Ibid., p. 33.

22. Foreign Affairs, Fall 1979, p. 154.

23. Reason, January 1981, p. 33.

24. Ibid., p. 27.

25. Ibid.

26. 35 U.S.C. 181. See also, Appendix A, "Summary: Invention Secrecy Act of 1951," Export Administration Report, Department of Commerce, November 17, 1980.

27. 35 U.S.C. 181.

28. Act of September 14, 1976, Public Law 94-412, 90 Stat. 1255, 50 U.S.C. 1621 (1976).

29. 35 U.S.C. 183, 186, 188.

30. 34th Report, House Committee on Government Operations, "The Government's Classification of Private Ideas," Report No. 96-1540, December 22, 1980, pp. 29-33. (Hereinafter cited as House Report No. 96-1540.)

31. Ibid., p. 120.

32. Ibid.

33. Personal Communications, NSA Director of Policy Eugene Yeates, Mel Klein, and others, Ft. Meade, Maryland, March 25, 1981.

34. Ibid.

35. House Report No. 96-1540, pp. 5, 7.

36. Reason, January 31, 1981, p. 35.

37. House Report No. 96-1540, p. 63.

Section 2 Notes (Continued)

38. Executive Order 12065, "National Security Information," January 28, 1978, section 1-205.

39. House Report No. 96-1540, p. 64.

40. Science, August 29, 1980, pp. 995, 996.

41. Ibid.

42. Personal Communications, NSA Director of Policy Eugene Yeates, Mel Klein, and others, Ft. Meade, Maryland, March 25, 1981.

43. Science, October 10, 1980, p. 134.

44. Science, November 28, 1980, p. 960.

45. Science, October 31, 1980, p. 511.

46. Personal Communications, John Cherniavsky, National Science Foundation, March 24, 1981.

47. Personal Communications, John Cherniavsky, National Science Foundation, June 9, 1982.

48. Science, October 10, 1980, p. 135.

49. Personal Communications, NSA Director of Policy Eugene Yeates, Ft. Meade, Maryland, March 25, 1981.

50. Science, May 16, 1980, p. 695.

51. Ibid.

52. Cryptologia, Volume 4, Number 3, p. 192.

53. Personal Communications, John Cherniavsky, National Science Foundation, March 24, 1981.

54. Science, March 13, 1981, p. 1140.

55. Science, September 26, 1980, p. 1504.

56. Speech before the Armed Forces Communications & Electronics Association, January 11, 1979.

57. Ibid.

58. Ibid.

59. Cryptologia, Volume 4, Number 3, p. 176.

Section 3

1. Cryptologia, January 1980, p. 42.

2. "Security and Encryption Hardware," Conference Proceedings: Communication Networks '80, p. 272.

3. Datamation, September 1979, p. 71.

4. Science, July 29, 1977, p. 40.

5. Personal Communications, Sales Representative, Technical Communications Corporation, Concord, MA.

6. EDP Analyzer, April 1978, "The Debate on Trans Border Data Flows."

7. Cryptologia, January 1980, pp. 42, 43.

8. Ibid.

9. Personal Communications, Harry B. DeMaio, Office of Director of Data Security Programs, IBM Corporation, Armonk, New York, December 1981.

10. Electronics, June 5, 1980, pp. 97, 98.

11. Ibid.

12. Ibid.

13. Cryptologia, October 1980, pp. 213, 214.

14. Ibid.

15. Ibid.

16. Enhancement of Teletex Procedures to Incorporate Encipherment and Signatures, National Physical Laboratory, Teddington, Middlesex TW11 OLW, UK, p. 1.

17. Personal Correspondence, Donald Davies, National Physical Laboratory, England.

19. Personal Communication, Victor Walling, SRI International.

20. Cryptologia, January 1980, p. 43.

21. Ibid.

22. Ibid.

Section 3 Notes (Continued)

23. "An Assessment of Civil Sector Uses of Digital Data Encryption," Department of Engineering and Public Policy, Carnegie-Mellon University, Pittsburgh, November 1980, p. 2. (Hereinafter cited as Carnegie-Mellon Study.)

24. Ibid., p. 45.

25. Ibid., p. 46.

26. Ibid., p. 50.

27. Personal Correspondence, Howard Crumb, Federal Reserve Bank of New York.

28. Carnegie-Mellon Study, p. 103.

29. Ibid., p. 104.

30. Ibid.

31. Foreign Affairs, Fall 1979, p. 147.

32. Reason, January 1981, pp. 28, 29.

33. Hearings before Subcommittee of the Committee on Government Operations, House of Representatives, "The Government's Classification of Private Ideas," February 28, March 20, and August 21, 1980, p. 418. See also David Kahn, The Codebreakers, p. 733.

34. Personal Communications, Michael Dertouzos, Laboratory for Computer Science, Massachusetts Institute of Technology, March 26, 1981.

35. Science, March 13, 1981, p. 1139.

36. Ibid.

37. Personal Communications, Michael Dertouzos, March 26, 1981.

38. "Cryptographic Technology: Fifteen-Year Forecast," Whitfield Diffie, BNR Inc., Mountain View, California, January 1981, pp. 14, 15. (Hereinafter cited as Diffie Forecast.)

39. "Emerging Federal Government Actions in Telecommunications Protections," Donald Kraft and Charles Wilk, NTIA, Department of Commerce, July 19, 1979, p. 4.

40. Personal Communications, Lee Merkhofer, SRI International, March 1981.

41. Computer Security Institute, Hudson, MA 10749.

42. Information Privacy, September 1980, p. 216.

Section 3 Notes (Continued)

43. Personal Communications, Wayne Barker, President, Aegean Park Press, December 1980.

Section 4

1. Speech before Armed Forces Communications & Electronics Association, January 11, 1979.

2. "Report of Public Cryptography Study Group," American Council on Education, 1 Dupont Circle, Washington, D.C., February 1, 1981. (Hereinafter cited as ACE Report.)

3. Reason, January 1981, p. 35.

Section 5

1. Science, June 27, 1980, p. 1443.

2. Personal Communications, W. Todd Furniss, American Council on Education, March 23, 1981.

3. Science, June 27, 1980, p. 1442.

4. ACE Report, p. 14.

5. Ibid., p. 15.

6. Personal Communications, W. Todd Furniss, March 23, 1981.

7. Science, October 31, 1980, p. 511.

8. Ibid., p. 512.

9. Unpublished letter to Science, from Ira Michael Heyman, Office of the Chancellor, University of California, Berkeley, November 20, 1980.

10. Personal Communications, David Kahn.

11. ACE Report, pp. 23-24.

12. Ibid., Appendix, pp. 6-10.

13. Ibid.

14. Cryptologia, January 1981, p. 43.

15. Science, March 13, 1981, pp. 1139-40.

16. Ibid.

Section 5 Notes (Continued)

17. Personal Communications, Michael Dertouzos, Laboratory for Computer Science, Massachusetts Institute of Technology, March 26, 1981.

18. Science, March 13, 1981, p. 1140.

19. Personal Communications, Michael Dertouzos, March 26, 1981.

20. Personal Communications, NSA Director of Policy Eugene Yeates, Legal Counsel Daniel Schwartz, and others, Ft. Meade, Maryland, March 25, 1981.

21. Ibid.

22. Science, February 20, 1981, p. 797.

23. Ibid.

24. Personal Communications, NSA Director of Policy Eugene Yeates, Mel Klein, Howard Rosenblum, and others, Ft. Meade, Maryland, March 25, 1981.

25. Ibid.

26. Ibid.

27. Ibid.

28. Ibid.

29. Ibid.

30. Science, March 13, 1981, p. 1140.

31. ACE Report, Appendix, p. 7.

Section 6

1. Presidential Directive/NSC-24, November 16, 1977 (classified).

2. "Private and Public Defenses Against Soviet Interception of U.S. Telecommunications: Problems and Policy Points," Greg Lipscomb, Programs on Information Resources Policy, Harvard University. See Appendix A, Policy Guidelines accompanying PD/NSC-24.

3. Ibid.

4. National Telecommunications Protection Policy Directive, February 17, 1979. See also, 34th Report, House Committee on Government Operations, "The Government's Classification of Private Ideas," Report No. 96-1540, December 22, 1980, pp. 113, 114. Also, see Lipscomb paper, note 36, Appendix B.

Section 6 Notes (Continued)

5. Ibid., part 4(a)-(f).

6. Ibid., part 4(d).

7. Reason, January 1981, p. 35.

8. Ibid.

9. Ibid.

10. Seminar on Command, Control, Communications and Intelligence, Harvard University, Program on Information Resources Policy, Spring 1980, Guest Presentations: Robert Rosenberg, p. 56.

11. *Science*, March 27, 1981, p. 1398.

12. Personal Communications, Colonel Wayne Kay, Senior Analyst, Office of Science and Technology Policy, April 20, 1981.

13. Ibid.

14. Ibid.

15. Ibid.

Section 7

1. Diffie Forecast, p. 17.

2. *U.S. Government Manual*, May 1, 1980, p. 259.

3. Ibid.

4. U.S. Senate, *Surveillance Technology*, a staff report of the Subcommittee on the Constitutional Rights of the Committee of the Judiciary, 1976, p. 22.

5. Executive Order 12333, December 4, 1981.

6. Ibid., Section 1.12, paragraphs 6,7.

7. Speech before Armed Forces Communications & Electronics Association, January 11, 1979.

8. Personal Communications, Michael Dertouzos, March 26, 1981.

9. Ibid.

10. Senate Bill 2525, Sec. 142(b)5.

11. Ibid.

Section 7 Notes (Continued)

12. Kahn, David. The Codebreakers (New York: Macmillan Company, 1967), pp. 705, 718.

13. Personal Communications, NSA Director of Policy Eugene Yeates, Howard Rosenblum, and others, Ft. Meade, Maryland, March 25, 1981.

14. S. 2525, Section 641.

15. Personal Communications, NSA Director of Policy Eugene Yeates, Howard Rosenblum, and others, Ft. Meade, Maryland, March 25, 1981.

16. Ibid.

17. Progressive, November 1980, p. 17.

18. Seminar on Command, Control, Communications and Intelligence, Program on Information Resources Policy, Harvard University, Spring 1980, Guest Presentations: B. R. Inman, p. 147.

19. Ibid.

20. Personal Communications, Charles Wilk, NTIA Special Project Office, March 24, 1981.

21. Donald Kraft and Charles Wilk, Emerging Federal Actions in Telecommunications Protection, National Electronics Conference, October 30, 1979, p. 6.

22. The Brooks Act, Public Law 89-306, October 30, 1965.

23. The Privacy Act, Public Law 93-579, 93rd Congress, S.3418, December 31, 1974.

24. P.L. 96-461, Section 2(a), 3.

25. Diffie Forecast, p. 16.

26. Ibid.

27. Science, July 29, 1977, p. 438.

28. Progressive, November 1980, p. 21.

29. Personal Communications, NSA Director of Policy Eugene Yeates, Mel Klein, and others, Ft. Meade, Maryland, March 25, 1981.

30. Ibid.

31. Personal Communications, Charles Wilk, NTIA Special Project Office, March 24, 1981.

Section 7 Notes (Continued)

32. Donald Kraft and Charles Wilk, Emerging Federal Actions in Telecommunications Protection, National Electronics Conference, October 30, 1979, p. 4. (Hereinafter cited as Kraft and Wilk.)

33. Ibid.

34. General Services Administration, Privacy and Data Security for ADP and Telecommunications Systems, Federal Property Management and Regulations: Subpart 101-35.1703(a) Amendment F-31, June 1978.

35. Kraft and Wilk, p. 2.

36. Ibid.

37. Science, March 20, 1981, p. 1327.

38. See discussion infra, pp. 10-11.

39. Kraft and Wilk, p. 6.

40. New York Times, August 29, 1977.

41. New York Times, July 17, 1977.

42. GAO Report, pp. 46-49.

43. Telecommunications Policy, December 1977, p. 386.

44. Ibid.

45. Personal Communications, David Kahn.

46. Communications Network '80, Conference proceedings, "Security and Encryption Hardware," p. 273.

47. Washington Post, November 16, 1980, A2.

48. Ibid.

49. Christian Science Monitor, January 29, 1981.

50. Seminar on Command, Control, Communications and Intelligence, Program on Information Resources Policy, Harvard University, Spring 1980, Guest Presentations: B. R. Inman.

51. Ibid.

52. Personal Communications, NSA Director of Policy Eugene Yeates, March 25, 1981.

53. Boston Globe, April 20, 1981, p. 5.

Section 7 Notes (Continued)

54. New York Times, November 20, 1980, Al.

55. Personal Communications, Donald Kraft, Director, NTIA Special Project Office.

56. Science, January 2, 1981, p. 37.

57. Ibid.

58. Science, March 20, 1981, p. 1325.

59. Security Management, November 1980, p. 52.

60. NTIA "User's Guide," p. 8.