# Private and Public Defenses Against Soviet Interception of U.S. Telecommunications: Problems and Policy Points

Greg Lipscomb

***Program on Information Resources Policy***

Harvard University

Center for Information Policy Research

Cambridge, Massachusetts

A publication of the Program on Information Resources Policy.

PRIVATE AND PUBLIC DEFENSES AGAINST SOVIET INTERCEPTION OF U.S. TELECOMMUNICATIONS: PROBLEMS AND POLICY POINTS
Greg Lipscomb
Publication No. P-79-3

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





Printing 6

September 1985

# PROGRAM ON INFORMATION RESOURCES POLICY

**Harvard University** | **Center for Information Policy Research**

## Affiliates

Action for Children's Television
American District Telegraph Co.
American Telephone & Telegraph Co.
Arthur D. Little, Inc.
Auerbach Publishers Inc.
Automated Marketing Systems
BellSouth Corporation
Bell Atlantic
Booz-Allen & Hamilton, Inc.
Canada Post
Cellular One
CBS Broadcast Group
Commission of the European Communities (Belgium)
Communications Workers of America
Computer & Communications Industry Assoc.
COMSAT
Copley Newspapers
Cowles Media Co.
Dai-Ichi Kangyo Bank, Ltd. (Japan)
Databit Inc.
Dialog Information Services, Inc.
Digital Equipment Corp.
Direction Generale
des Telecommunications (France)
Doubleday and Company, Inc.
Dow Jones & Co., Inc.
Dun & Bradstreet
Economics and Technology, Inc.
EIC/Intelligence Inc.
LM Ericsson (Sweden)
Gannett Co., Inc.
GTE Sprint Communications Corp.
Hitachi Research Institute (Japan)
Honeywell, Inc.
Hughes Aircraft Co.
E.F. Hutton and Co., Inc.
IBM Corp.
Information Gatekeepers, Inc.
International Data Corp.
International Resource Development, Inc.
Invoco AB Gunnar Bergvall (Sweden)
Knowledge Industry Publications, Inc.
Lee Enterprises, Inc.
Lotus Development Corp.
John and Mary R. Markle Foundation
Martin Marietta Corp.
MCI Telecommunications, Inc.
McKinsey & Co., Inc.
Mead Data Central
MITRE Corp.
Motorola, Inc.
National Telephone Cooperative Assoc.
The New York Times Co.
NEC Corp. (Japan)
Nippon Telegraph & Telephone Public
Corp. (Japan)
Northern Telecom Ltd. (Canada)
Northrop Corp.
NYNEX
The Overseas Telecommunications
Commission (Australia)
Pacific Telesis Group
Pitney Bowes, Inc.
Public Agenda Foundation
RCA Corporation
Reader's Digest Association, Inc.
Research Institute of Telecommunications
and Economics (Japan)
Salomon Brothers
Satellite Business Systems
Scaife Family Charitable Trusts
Seiden & de Cuevas, Inc.
Southern New England Telephone
State of Minnesota Funding
State of Nebraska Telecommunications
and Information Center
Telecom Futures, Inc.
Telecommunications Research
Action Center (TRAC)
Telecom Plus International, Inc.
Times Mirror Co.
TRW Inc.
United States Government:
Central Intelligence Agency
Department of Commerce:
National Oceanographic and
Atmospheric Administration
National Telecommunications and
Information Administration
Department of Health and Human Services
National Library of Medicine
Department of State
Office of Communications
Federal Communications Commission
Federal Emergency Management Agency
Internal Revenue Service
National Aeronautics and Space Admin.
National Security Agency
U.S. Army:
Office of the Assistant Chief of
Staff for Information Management
United States Information Agency
United States Postal Rate Commission
United States Postal Service
US West
United Telecommunications, Inc.
The Washington Post Co.
Wolters Samsom Group (Holland)

## ACKNOWLEDGMENTS

Special thanks are due to the following persons who reviewed the study plan, supplied data, or who 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.

Hendrik W. Bode

Dean Gillette

Walter W. Haase

J. Roy Henry

John C. LeGates

Elliott E. Maxwell

Harry B. DeMaio

J. H. Pomerene

Private and Public Defenses Against Soviet Interception of U.S. Telecommunications: Problems and Policy Points

Table of Contents

## SUMMARY

For some time the Soviet Union reportedly has been listening in on American domestic long distance telephone calls. The interceptions are made during the line-of-sight microwave portion of the calls' transmission across the country. The intercepting equipment is housed in the Soviet embassy in Washington, and in Soviet consulates and diplomatic residences in other U.S. cities.

The Soviets are not only seeking protected government or defense information. They are seeking economic information being transmitted between private parties, mostly corporations. Such information, in the aggregate, is of significant strategic value.

According to news reports, the Carter Administration has decided not to interfere directly with the Soviet embassy, even though such eavesdropping, if done by American citizens or the U.S. governemnt, would be illegal unless done under a search warrant. The reasons for the decision seem twofold: (1) the Soviets could make the same interceptions from satellites, off-shore ships or listening posts in Cuba, so restricting the Soviets within U.S. borders would have little real protective effect; and (2) the U.S. is permitted to do the same thing in the Soviet Union.

At the same time, the Administration apparently has decided that it will do what it can indirectly to frustrate the Soviet effort. A White House task force led by presidential science adviser Frank Press is to

encourage private industry to secure their communications so that eavesdropping will be more difficult.

Press's assignment is a formidable one. The nature of the problem respects no traditional boundaries. Its features are both domestic and foreign, military and civilian, and public and private. At least two scenarios appear: (1) closely controlled development under the umbrella of centrally determined standards; or (2) relatively uncontrolled development without centrally determined standards.

The implications of both are dramatic. The first scenario leads to more compatible equipment with common encryption methods, but raises the issue of privacy and trust. Can a centralized unit, be it government, quasi-government or private, be trusted to exercise its powers for only legitimate purposes? The history of such efforts is mixed.

The second scenario poses the problems of security and convenience. Types of equipment would vary, some of it sophisticated and secure, some of it not, some of it generally compatible with other systems at a reasonable cost, some of it compatible only at high costs or not at all. Meanwhile, the mobile corporate executive may find himself inconvenienced if not isolated as he moves from one security system to another.

Cost raises other questions. It has been estimated that to secure the 68% of domestic long distance calls that are transmitted by microwave would cost two to three billion dollars. One system costs $35,000 per telephone. What portion of these costs should be undertaken, who should pay for them and by what means? Should corporations be asked to absorb the costs of what is, in essence, a national security problem? Should

the public pay, through taxes or their telephone bills?

The key players who most likely will determine the answers to these questions include the White House; the Congress (in particular, Senator Moynihan); the intelligence agencies (especially NSA); the press (through a few interested military reporters); certain corporations; and certain defense and consumer coalitions.

As the problem invariably goes international, the players and issues increase. Economic data become a kind of currency over which and through which power is gained and lost. "Contraband data" are sent over internationally secured channels. Data become a product, taxable at borders just as any other product. Data havens, much like tax havens and flags of convenience, develop and, gradually, information vital to the security of one country is stored in another country. Alliances transpire, and the plethora of international organizations and conventions enter the arena. In such a setting, the problems of compatibility and trust take on new dimensions.

But in the end, all effort only buys time. The pace of interception and compromise presses closely on the heels of resources and ingenuity.

## Editor's Note

On March 26, 1979 the New York Times (p. A16) reported the creation of a Special Projects Office in the Commerce Department's National Telecommunications and Information Administration (NTIA) that "seeks to prevent Russians from spying on [the] U.S. phone system".

The appendices present two documents which were made public around that time, one a set of NTIA briefing charts on policy guidelines set forth in Presidential Directive/NSC 24 (Appendix A), the other headed "National Telecommunications Protection Policy" (Appendix B).

To the best of our knowledge, these documents reflect U.S. government policy on the subject of this paper as of June 1979.

I. Introduction

A. Carter Administration decision. On November 20, 1977, the New York Times reported that the Carter Administration had reached a decision on what to do about the continuing Soviet practice of eavesdropping on many American long-distance telephone calls.[1] The calls, according to the story, were being intercepted -- during the tower-to-tower line-of-sight microwave portion of their transmission across the country -- by equipment housed in the Soviet embassy, consulates and diplomatic personnel residences, including country residences.

In essence, the Administration's decision was to allow the Soviets to continue their practice, but to frustrate the Soviet's efforts by securing critical transmissions wherever possible. The United States would complicate, but not terminate, the Soviet action.

This outwardly curious decision was, according to the story, the results of four years of deliberation.

B. Brief history and background. According to another news report, the Soviet interceptions began several years ago in retaliation against similar American activities that began around 1972 from the American embassy in Moscow.[2] It was these American interceptions that apparently led to the heavy microwave bombardment of the American embassy by the Soviets in an attempt to jam the American equipment. The bombardment allegedly caused some American embassy employees to experience radiation sickness. Diplomatic protests ensued.

Nevertheless, the American equipment was allowed to stay in the U.S.S.R., and the Soviet equipment is to be allowed to stay in this

country. Jeremy J. Stone, director of the Federation of American Scientists, has speculated that there is a ". . . tacit agreement between the American intelligence and the Soviet intelligence communities to let each other listen in. This could be called 'open telephone,' in analogy to the proposal of President Eisenhower for 'open skies'."[3]

In the face of such known eavesdropping, it can be assumed that neither government is going to allow tightly held classified secrets to idly float through the microwaves (although there have been embarrassing exceptions, as when the Americans plucked some critical information from the Kremlin's automobile telephone).[4] However, the Soviets are not only after formally classified government information that may unintentionally slip into the airwaves. They also are after what might be called strategic economic information--privately held, unclassified data about U.S. techno-developments, industrial processes and investment plans. Most of this information flows from corporation to corporation, without the U.S. government's ever being a party to the conversation. In fact, much of it flows over private, or "dedicated," circuits used by many corporations.[5]

The Soviets' interest is twofold: (1) in the aggregate, such information can be significant in a military and economic world power struggle. "Increasingly, this is where the (intelligence) game is being played," the Atlanta Constitution quoted one official.[6] Jeremy Stone told Science magazine the Soviet actions were equivalent to "economic warfare," and pointed to the Soviet's manipulation of the grain market during the wheat deal as one of the skirmishes.[7] Similarly, Business Week quotes one government official as saying that the Soviets "have become deeply involved in a whole variety of ways in the Western economic system, and are intensely interested

in, for example, what U.S. banks and the Federal Reserve Board may have to say to one another."[8] (2) But at a more prosaic level, the Soviets simply are interested in protecting their increasing investments in the Western world. Business Week says the same official "cites a Central Intelligence Agency report . . . that documents the tripling--from 28 to 84--of Soviet foreign based business, including five in the U.S., in the past six years."

C. Mechanism to carry out decision. Against this backdrop, the Administration, according to the news stories, has vested in the President's Science Adviser, Dr. Frank Press, the authority to head the government's counter-intercept effort.[9] According to the November 20, 1977 Times report, Press will head a "special committee" that will "monitor the various parts of the program to be carried out by the Defense Department and a recently created office to be headed by an assistant secretary of commerce for communications and information policy." Specifically, the program is to include, "in addition to negotiations with the Soviet Union," the following elements:[10]

> ---Financing for Government research on telecommunications privacy will be increased from $10 million in the current fiscal year to $15 million next year.
>
> ---Government telephone calls subject to Soviet surveillance are in the process of being routed through underground cables rather than through microwave radio towers. The process, which will cost $10 million, is virtually complete in Washington and will be completed in New York and San Francisco next year.
>
> ---An experimental program to equip key surveillance targets with Executive Secure Voice Network units, which scramble conversations, is being enlarged. The Government has 100 of these $35,000 units in place and will purchase an additional 150 units.
>
> ---Industry and such agencies as the Federal Communications Commission will be encouraged to speed the development and use of equipment and procedures that will make it more difficult for eavesdroppers to secretly record telephone messages.

II. Questions, problems and policy points.

The Administration's decision, and the chosen form of carrying it out, raises at least the following issues:

A. A problem without dimensions

Analysis frequently begins with limits. Problems are perceived in parameters, so they can be dealt with, for by defining what the problem is not, one can deal with what is. Limits imply boundaries, and the more standard the boundaries, the more the problem lends itself to the tools of standard analysis.

But a foreign power's plucking domestic microwaves from the air poses a problem for the intercepted power not only of policy, but also of boundaries. Who, for example, in the intercepted power is going to be sensitive to the problem, respond to the problem, handle the problem?

"The problem . . . was unprecedented in several ways," one official told a reporter. "First, the threat of Soviet surveillance of non-classified but strategically important information was not the responsibility of any single agency."[11]

Interestingly, the official was discussing the early efforts, in 1974, of the U.S. government to deal with the problem. It can be speculated that at least part of what could be said to be the slowness of the U.S. government to deal with the problem is due to the fact that the problem did not fall within our government's traditional agency boundaries.

The organization of American government agencies has tended to mirror, for functional or philosophical reasons, certain separations that are deemed significant, if not semi-sacred: the separation of the domestic from the foreign, the civilian from the military and the private from the public. But the problem at hand seemed irreverent of these boundaries.

Example: In 1970 the National Security Agency (NSA), a subdivision of the Department of Defense (DOD), is reported to have picked up information about Korean government payments to members of Congress, long before the payments became an issue in American domestic politics. The information, although of a domestic nature, was gathered while eavesdropping on the electronic cable traffic of the Korean government.[12] Where does the domestic separate from the foreign here? Similarly, of what effect are domestic privacy laws if domestic long distance communications, beamed through hovering satellites, can be picked up by Cuban antennas or Soviet off-shore ships, as they apparently can?[13]

Example: In 1977, according to news reports, NSA approached a private telecommunications company with an offer to "enter into a 'classified contract' under which the Government . . . would assist the private company to improve its defenses against eavesdropping."[14] This might seem reasonable to a private company. NSA, after all, is responsible for the security of the government's communications, and possesses possibly the most sophisticated telecommunications capability in the country.[15] But NSA also is part of the Department of Defense, and in setting up the Press committee, Administration officials are reported to have stressed, "We didn't think it appropriate to have the Department of Defense controlling the private sector."[16]

NSA's move could be said to be contrary to the assumed boundaries, and the White House is reported to have said as much: "Another White House official, who requested anonymity, said the agency's action was surprising and appeared to go beyond its normal range of concerns."[17]

The line between the civilian and the military seems to have grown thin in this instance.

Example: The telecommunications industry in this country, unlike most countries, is privately held. Moreover, competition and diversification are being encouraged through decisions of the Federal Communications Commission (FCC) to permit non-carrier terminal attachments to common carrier networks and competing microwave satellite networks, such as Satellite Business Systems, Inc. (SBS).[18] With such private diversity, who assumes responsibility for foreign intrusion, an essentially public problem? At what point does private information become so strategically significant that its availability to foreign powers could jeopardize the security of our country? Who determines such a status and what, if anything, should be done about it? Should the umbrella of the government's uniform classification system be radically changed to include such information? By what means? By whom and by what criteria? As one news report stated, "A number of sources said the intelligence agencies--the NSA and the Central Intelligence Agency--felt the situation warranted a vast enlargement of what was handled as secret information: 'They wanted to secure the world,' said one official."[19]

Again, another tidy distinction, this one between the public and private sectors, seems to have grown blurred.

B. <u>The players: casting</u>

Even if the boundaries of the problems are mercurial, the major players can perhaps be identified with some certainty.

As mentioned on page 3, news accounts indicate that, at least for the near term, the White House will remain central to the decision making, through the offices of the President's science adviser, Dr. Frank Press.[20] Under Press, as indicated earlier, will be the Departments of Defense and Commerce.

The White House committee seems to be the latest generation of working panels that began in 1974, under the auspices of the National Security Council.[21] The original group was headed by Dr. Edward E. David, Jr. then science advisor to President Nixon. It included government and non-government members and it performed its work in confidence, out of the public eye. Within a year, in June of 1975, the "Rockefeller Commission" on the CIA was reporting that" . . . we believe that these countries can monitor and record thousands of private telephone conversations. Americans have a right to be uneasy if not seriously disturbed at the real possibility that their personal and business activities which they discuss freely over the telephone could be recorded and analyzed by agents of foreign powers."[22] In June of 1976, then Vice-President Rockefeller emphasized this statement in remarks to the National Broadcast Editorial Association in Washington.[23]

These government actions brought two additional players into the arena: the press and the public. The press reported the Rockefeller remarks, but the matter generally dropped from the public view. Then, in March of 1977, President Carter is reported to have authorized a special coordinating committee of the National Security Council (NSC) to pick up the work of the David panel. The committee was headed by the Zbigniew Brzezinski, and included officials of the Departments of Justice, Commerce, the Federal Communications Commission (FCC), the White House Office of Telecommunications Policy and the CIA and NSA.[24] That committee also was to work confidentially.

In April of 1977 the Atlanta Constitution ran a major article on the work of the Brzezinski committee.[25] In May, according to later news reports, Senator Moynihan of New York raised the issue of eavesdropping at a closed

White House meeting, and President Carter supposedly responded that his administration was at work on the matter and preferred to keep it confidential so as not to impair the work of NSA. Moynihan made no public statement at the time.[26]

On Sunday, July 10, 1977, the New York Times ran a major page-one article discussing the entire matter. Senator Moynihan made a public statement that day, printed in Monday's Times, saying that the Soviets were "committing crimes on a staggering unprecedented scale" by secretly intercepting American phone calls. He called on the Carter Administration to demand "that the Soviet Union cease and desist in its espionage campaign."[27]

On Tuesday, at a press conference, President Carter was asked about the Moynihan statement. He seemed prepared for the question: "I would not interpret this use by the Soviet Union or by other embassies to be an act of aggression. And although it may be an intrusion into our security, I think we are taking adequate steps now to prevent its creating a threat to our country."[28]

But news editorials supported the Senator and, on July 27, Moynihan introduced legislation that would require the President to "expel from the country foreign diplomats who persisted in eavesdropping on Americans."[29]

The initial cast, then, has begun to emerge: the White House, Senator Moynihan and the press; also federal agencies, such as the FCC, the Departments of Defense, Justice and Commerce. Commerce, under the President's reorganization plan, is taking on a new assistant secretary to head the National Telecommunications and Information Administration (NTIA). NTIA assumes the functions of Commerce's Office of Telecommunications (OT) and of the White House Office of Telecommunications Policy (OTP).[31]

Justice, especially the FBI, may get more involved if a warning by the Director of Central Intelligence (and of the CIA), Stansfield Turner, bears true. He has warned, speaking of the information flowing over commercial microwave transmission, that "... if calls were being transmitted 'on a microwave link, hijackers, gangsters, foreign intelligence operators, industrial spies and all [will] work to get that information.'"[32]

Another major player will be Congress, especially in its increased watchdog role over the intelligence community and, within Congress, the Senate Select Committee on Intelligence. Senator Moynihan's tack into the process has been as a member of that committee.[33]

The public may get indirectly involved through matters of the pocketbook (see section on "Who pays" p. 32). As regulatory agencies, such as the FCC, become involved, consumer groups that regularly examine these agencies may become involved. And there is a growing coterie of "public interest" lobbying organizations that are beginning to watch the intelligence community. Examples are the Project on National Security Studies, Common Cause, the Public Citizens Litigation Group, the American Civil Liberties Union and the Center for National Security Studies.[34]

Other sectors of the public, the "private sectors," are the companies and common carriers that either are in the telecommunications business or use telecommunications to transmit business information that is regarded by some in the government to be of increasingly national value. Certainly American Telephone and Telegraph (AT&T) is the prime regulated communications general common carrier and will play a centerpiece role as the problem

unfolds.[35] The new communications specialized common carriers encouraged by more recent FCC pro-competitive policies could become involved.[36] One company, MCI Communications Corporation, already has.[37] Other telecommunications equipment companies are springing up rapidly (e.g., TDX Systems, Inc.),[38] as are the unregulated teleprocessors, such as Tymshare, that provide" . . . retail data processing services to multiple customers sharing common computing facilities."[39]

As for the companies whose business information is of possible strategic value to foreign powers, there are the defense contractors. But they are in a special, identifiable category, and at least some of them are being included in an experimental government network of relatively secure communications known as Electronic Secure Voice Network (ESVN).[40] Less well defined, but of growing importance, are the general business firms--banks, investment houses, scientific labs and manufacturers--whose aggregate efforts compose much of the American economy, and therefore are of interest to the Soviets.[41] Twenty-eight such general business firms and eleven telecommunications companies reportedly were called in for a security briefing by the government,[42] and it is speculated that one reason why the Carter Administration is so prone to discuss the security issue publicly is to catch the attention of the many other firms whose business may fall in this category of growing sensitivity.[43]

Of special importance as players are the agencies and leaders of the U.S. intelligence community.[44] They are important because the problem at issue here is one of alleged breach of national security, and how to seal that breach. As the traditional guardians--indeed definers--of that security, this community can be expected to play a large role.

The CIA and the Department of Defense (DOD) are among the chief intelligence community players. Within DOD is DOD's general intelligence unit (called the Defense Intelligence Agency, or DIA). DOD's primary specialized intelligence units are the National Reconnaissance Office (NRO), covering satellite intelligence, and the National Security Agency (NSA), the communications intelligence and cryptographic agency. It is NSA that will command special attention in this case.

Also significant are the intelligence coordinating councils, such as the National Security Council (NSC). It has been through the Director of Central Intelligence (DCI), the NSC and the NSC's committees that organizations like NSA got their assignments.[45] Specifically, although it is by no means certain, it appears that NSA at one time received some of its directives from the DCI upon advice of the U.S. Intelligence Board (USIB), which was made up of representatives of the FBI, CIA, Treasury, State, Defense and the Energy Research and Development Administration.[46] The USIB was abolished in 1976 and replaced by the Committee on Foreign Intelligence (CFI).[47] It appears from the latest reorganization of the intelligence community (by virtue of the President's Executive Order of January 24, 1978) that assignments for NSA will now emanate from the National Intelligence Tasking Center (NITC) which, in peacetime, is under the DCI.[48] It should be noted that among the major players in setting up the latest reorganization were Vice President Walter Mondale and a senior NSC official, David Aaron.[49] Aaron was an aide to Mondale when Mondale was a Senator serving on the Senate Select Committee on Intelligence in 1975 and 1976. Aaron served as one of four task force leaders for the committee when the committee dug deeply into the operations, and misdeeds, of NSA.[50]

C. <u>The players: centrifugal and centripetal forces</u>

The players obviously do not exist in isolation. They exist in orbit,

spinning in a criss-cross of relationships that represent various gravitational tugs and separations. But, as will be seen, it can be argued that this particular solar system seems to have no sun.

1. The Pentagon vs. the DCI. With tasking set under the new NITC, and with the DCI as chairman of the NITC, it might seem to be a relatively simple matter for the DCI to carve out and assign for implementation the intelligence community's role in the resolution of the microwave intercept problem. But, in this writer's judgment, this is unlikely to be the case.

It is reasonable to assume NSA will have a major role in representing the intelligence community in the resolution of the problem. According to section 1-1202(a) of the new executive order, NSA's responsibilities shall include

> Establishment and operation of an effective unified organization for signals intelligence activities, except for the delegation of operational control over certain operations that are conducted through other elements of the Intelligence Community. No other department or agency may engage in signals intelligence activities except pursuant to a delegation by the Secretary of Defense.

NSA has, since its creation in 1952, been a primary player in electronic communication intelligence and, consistent with this role, it reportedly has been active in the developments of the microwave issue to date.[51]

But while the DCI (through the NITC) would have the authority for assigning tasks to NSA, the responsibility for carrying them out rests with the Secretary of Defense (by virtue of section 1-1105 of the executive order). In fact, according to news reports, it was principally the tug-of-war between the Secretary of Defense and the DCI over DOD's NRO and NSA that held up for several months the issuance of the President's executive order.[52] In that struggle, the Secretary of Defense apparently won. As the New York Times story states, "The new regulations give Adm. Stansfield Turner, the Director

of Central Intelligence, some added powers in preparing the intelligence community budget and in other areas. But, according to knowledgable Administration officials, he was blocked in his request for added authority over the Defense Department's reconnaissance and surveillance operations."[53]

This divided accountability over NSA's activities could contribute to a lack of clarity in the intelligence community's role in the microwave issue. And, it could perpetuate the kind of vague "floating authority" that a Senate committee has said contributed to a record of transgressions on the rights of Americans by NSA--an important point if NSA is to have a role in securing private domestic communications.[54]

Meanwhile, there has been speculation that NSA is eager to move into the microwave issue, for among other reasons to assert an authority that has been under challenge from several sides.[55]

2. NSA: responsibility without accountability? NSA is a service organization and a military organization. It was created in 1952 to coordinate and control the cryptographic capabilities of the armed services, and it is directed by a military officer of at least three-star rank.[56] As a service organization, it "provides foreign intelligence information at the request of consumer agencies."[57] Its "consumers" have tended to be federal agencies in the foreign policy, intelligence and law enforcement areas, including the FBI, CIA, DOD and the Secret Service.

As a service organization, it has tended, at least until 1973, to be customer oriented and to satisfy customer needs uncritically, according to a Senate report, not questioning the propriety or legality of the needs.[58] This detached view has in part been possible because of the nature of NSA's legal status. A 1976 report by the Senate Select Committee to study Governmental Operations notes that

> NSA does not have a statutory charter: its operational responsibilities are set forth exclusively an executive directives first issued in the 1950's. . . . According to NSA's General Counsel, no existing statutes control, limit or define the signals intelligence activities of NSA. Further, the General Counsel asserts that the Fourth Amendment does not apply to NSA's interception of American international communi cations for foreign intelligence purposes.[59]

Drafts of charters for NSA and other intelligence organizations are circulating in Congress.[60] But if the charters are based on the President's executive order, NSA still may be left with the kind of flexibility it historically has had.

a) Signals Intelligence

Sections 1-1202(c) and (e) of the President's order give NSA the responsibility for collecting and disseminating ". . . signals intelligence information for national foreign intelligence purposes. . ." in accordance with tasking and guidance by the NITC. The words "foreign intelligence" have established the traditional limits on NSA's power. But as the same 1976 Senate report states,

> Foreign intelligence is an ambiguous term. Its meaning changes, depending upon the prevailing needs and views of policy makers, and the current world situation . . . This flexibility was illustrated in the late 1960's when NSA and other intelligence agencies were asked to produce "foreign intelligence" on domestic activitists in the wake of major civil disturbances and increasing antiwar activities.[61]

Thus, according to the Senate report, some of the NSA interceptions in the past apparently have not been tied to foreign intelligence, and required a search warrant.[62] Even where tied to foreign intelligence, the Attorney General raised the issue of "questionable illegality," but his arguments were rejected by NSA.[63] In 1976, The Department of Justice had to firmly circumscribe NSA's activities with guidelines.[64] The new order does affirm the Attorney General's power to oversee compliance of intelli-

gence activities with American laws[65] but, with respect to NSA, the order does not appear to create any substantially new law. It could be that critical portions of the order dealing with NSA have been kept confidential. The Times story describing the President's briefing on the new order said ". . . Mr. Carter acknowledged that there are some elements of foreign intelligence operations so sensitive that even an Administration committed to openness had to keep the applicable executive orders confidential. These presumably relate mainly to photographic satellite reconnaissance and electronic communications interception."[66]

The Senate also found in its report on past activities that in the course of NSA's intelligence work between 1952 and 1974, NSA collected records on 75,000 Americans, including ". . . many prominent Americans in business, the performing arts, and politics, including members of Congress."[67]

Finally, the Senate found in NSA the danger of "drifting" or "floating authorization." This occurs when authority for an activity, once given, is assumed year after year, director after director. Such "floating authorization" occurred during NSA's Operation Shamrock. Shamrock began in 1945 when the Army Signals Security Agency approached RCA Global, ITT World Communications and Western Union International, commercial carriers of international telegraphs, for access to their transmissions. The Agency desired to monitor foreign government traffic passing over the facilities of the companies. Understandings were reached with officials as high as the Secretary of Defense, despite advice from the companies' attorneys that the interception would be illegal during peacetime. The arrangements generally gave the Agency access to telegrams of all parties, not just those of foreign governments (the traffic was later used to build files on individuals). The last known

authorization by either company or government officials was in 1949. From that time the authority "floated" to NSA and was assumed to continue for over twenty years, although apparently no high level officer of either the government or the companies reviewed the policy.[68]

Considering these practices, the Senate committee concludes:

> The watch list activities and the sophisticated technological capabilities that they highlight present some of the most critical privacy issues facing the nation. Space age technology has out-paced the law. The secrecy that has surrounded much of NSA's activities and the lack of Congressional oversight have prevented, in the past, bringing statutes in line with NSA's capabilities. Neither the courts nor Congress have dealt with the interception of communications using NSA's highly sensitive and complex technology.[69] (emphasis added)

b) Communications Security

It should be noted that the President's order does not give substantial guidance in determining what role, if any, NSA should play in the microwave issue. As has been stated, the words "foreign intelligence" do not address with certainty the issue of private domestic communications that might have national security significance. Section 1-1202(h) gives NSA the responsibility for "Executing the responsibilities of the Secretary of Defense as executive agent for the communications security of the United States Government," but, again, that wording does not directly address the problem of private communications under examination here. Perhaps the wording of section 1-1202(i) comes closest to our problem, giving NSA responsibility for the "Conduct of research and development to meet needs of the United States for signals intelligence and communications security." But that section deals only with research and development and, following section 1-1202(h) so closely, a strong argument can be made that the words "communications security" refer only to the ". . . communications security of the United States Government" discussed in section 1-1202(h).

3. Congress: a reform agenda. The 1976 report of the Senate Select Committee on Intelligence concluded its study of NSA by posing a specific set of policy questions it felt should be resolved by legislation.[69] Interestingly, the questions are primarily "boundary" questions. Should NSA be barred from operating domestically? Should it be prohibited from the field of law enforcement or internal security? Should it be allowed to target the international communications of Americans? And when there is an incidental interception of Americans' messages in international communications, what should NSA do?[70]

The ticklish side of these questions is not in the area where NSA has been culpable in the past -- the area in which the Senate has done most of its research. Culpability -- deliberately flying in the face of established law or traditions -- can be dealt with, given the will and the wording. And NSA is hardly unique among major American institutions that have a record -- even a long historical record -- of violations of good will and law (e.g., the F.B.I., many large corporations, the Presidency).

The real challenge raised by these questions rests in establishing policy for areas in which at present no intelligence community operator, however well intentioned, can do right. For example, assume that NSA studiously attempts to avoid conflict with domestic privacy laws, yet is assigned to protect unsophisticated domestic communicators from foreign intrusion, or is ordered to monitor transmissions abroad that tie into domestic conversations. How can NSA deal with one (the foreign) and avoid the other (the domestic)? It is not a matter of deliberate violation, but of stumbling through a boundaryless area into the trip wires of more established procedures. In this new nether land (that the microwave interception problem represents) there is no right -- or wrong -- no set body of traditions or legal standards. It is a dilemma born of technology and mordern times,

and it is against this challenge of the uncharted that any Congressional "reform" proposals must be measured.

Already legislation has been introduced (Senate Bill 2525, National Intelligence Act of 1978, Sen. Huddleston, D-Ky.) that attempts to deal with these questions. Senate Bill 2525 proposes that the National Security Council

> develop policies governing the circumstances and terms and conditions under which departments and agencies may furnish to United States persons information and materials regarding the vulnerability of non-governmental United States communications to unauthorized interception and exploitation and regarding appropriate means of securing such communications from unauthorized interception and exploitation.[71] (emphasis added)

The bill would give NSA the responsibility to

> evaluate, based upon policy guidance from the Attorney General, the vulnerability of the United States communications to interception and exploitation by unintended recipients 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.[72] (emphasis added)

Thus the bill would give NSA authority, under certain conditions, to operate domestically.

In another section, the bill states that information not publicly available may be kept on individuals without the individuals consent "... only if ... such information was collected in the course of authorized foreign intelligence, counterintelligence, or counterterrorism intelligence collection and is essential for understanding or assessing such intelligence."[73] Moreover, there is a provision that "... information collected by means of electronic surveillance within the United States or foreign electronic or signals intelligence activities shall be retained or disseminated only in accordance with the provisions of Title III of this Act."[74]

The bill, then, begins to struggle with the overlap of boundaries that confuse the current picture, and to give the intelligence community operator more guidelines by which to operate. And, in terms of management, it proposes to make the director and deputy director of NSA Presidential appointments, and to limit their terms.[75]

4. FCC, the Department of Commerce and the private sector. One of the uncertainties in this interplay of forces is how autonomous private companies will relate to the various parts of the government that are involved in the microwave problem.

The FCC has been encouraging proliferation and competition among communications companies and, in response, a number of specialized communications companies have emerged.[76] As a result, the private players are more numerous and generally smaller than they might have been had previous policies prevailed.

The government forces, on the other hand, have tended to be large in size and growing and, as we have seen, often not cooperative with each other, but rather even competitive with each other.

Will these large agencies compete for the attentions of the smaller businesses? Will the small companies, being numerous, be unable to organize and be unable to bargain effectively with the large agencies? Will some companies scurry to the protective wing of NSA, while others deal only with the White House or Commerce? And will the relationships be ones of symbiosis, dominance, collusion or combat?

In dealing with the microwave problem, there are not many clues to the outcomes of these questions. We know that during NSA's Shamrock program, the agency had a relatively unchecked access to all of the international commercial traffic of Western Union, RCA Global and ITT World Com-

munications.[77] And more recently, it was reported that representatives of NSA approached the president of a small Washington-based communications company (MCI) and asked him ". . . to enter into a 'classified contract' under which the Government agency would assist the private company to improve its defenses against eavesdropping."[78] According to the company president, the representatives ". . . requested and were given a great deal of proprietary information about the internal workings. . ." of the firm.

Without attaching a value judgment to the alleged contact, we can at least say, as did the news article reporting the incident, that "The reported effort of employees of the National Security Agency to work out arrangements with the private communications companies therefore has significant economic, as well as national security, implications."[79]

As for one much larger company, AT&T, it has been speculated that AT&T will benefit mightily from the government's decision to go to underground cables for many government lines, since AT&T has the largest number of underground cables in place.[80] But AT&T's primary regulator is the FCC, not NSA or the White House. The FCC is supposed to be able to make decisions on grounds independent of the executive branch. It has been reported that the FCC was included in the early deliberations on the microwave interception problem.[81] One can speculate on what independent force it carried in these meetings in the face of NSA, the CIA, DOD and the White House.

The development in the late 1960's of a pro-competition policy at the FCC has been ascribed, in part, to pressure from the White House at that time.[82] This policy led to a proliferation of services and companies. Yet this proliferation may now very well cause a problem for the White House, which reportedly wants to centralize the intelligence services[83] and, possibly, the controls on organization and technology in countermeasures to microwave interception.

While the FCC deals with the regulated carriers, the Department of Commerce may well seek to perform its traditional role as protector of general business. And most likely those businesses will deal quietly and directly with Commerce and the White House.

5. The press and the public. Articles regarding microwave interception first began appearing in 1975, and even though some government officials were discussing the matter openly, the problem seemed to attract little public or press attention.[84]

In the summer of 1976, then Vice-President Nelson Rockefeller is reported to have successfully argued for "open discussion of the danger for fear the Republicans might be accused of a cover-up."[85]

It is reported that NSA has consistently opposed public discussion of the matter, and that for a while President Carter acceded to this view.[86] But by the time the Administration made its informal announcement in November of 1977 about the Press committee program, it was felt that the matter had to be discussed more openly, if only to "encourage industry to take security measures."[87] It also was speculated that "Another factor in the decision to unveil the program may have been the political need to meet the charge of inactivity on this issue that has been made by Senator Daniel Patrick Moynihan. . ."[88]

The persistence of the press seems to be continuing, going around Administration officials when necessary, occasionally informing one branch of the government of another branch's activities.[89] No doubt the tenacity of Senator Moynihan will continue using, as he can, the fulcrum of his membership on the Senate Select Committee on Intelligence .

But the degree to which the Administration agrees to go public on the matter could be viewed to be a function of the pressure by the Senator and the press. One wonders, for example, whether the Administration is as likely to go public once communications have been established with critical industries whose security procedures the Administration hopes to influence.

The public has yet to be ignited in any broad sense about the microwave interception issue, and unless the public's pocketbook is strongly affected, it does not seem that it is likely to get more involved than it is through its growing awareness of the intelligence community. In that respect, the new "public interest" lobbies, and particularly and constituencies that have developed around the "central government computer" issue (the "anti-big brother" constituency), might become involved.

6. The White House: can it create a system? Can the White House control the activities of the various players? Apparently the White House hopes so. According to the news account discussing the execution of the Carter plan:

> One official said that one of the most difficult decisions involved in the deliberations was deciding who would be responsible for carrying out the Government program. Mr. Carter's decision was to establish a special committee headed by Dr. Frank Press, his science advisor, to monitor the various parts of the program to be carried out by the Defense Department and a recently created office to be headed by an assistant Secretary of Commerce for communications and information policy. 'We didn't think it appropriate to have the Department of Defense controlling the civilian sector,' the official said.[90] (emphasis added)

But the power to "monitor" is not necessarily the power to control. And being "responsible" does not necessarily lead to realistic accountability. We do not know the full import of the use of the words "monitor" and "responsible," because the President's directive setting up the program remains undisclosed, probably, according to the news report, because it touches on the work of NSA.

But can a "monitoring" office, can any small White House staff office, be expected to rope in the divergent interests in orbit here? Can it in any real way assume a command posture? It would take an extraordinary amount of what can be called system-building.

Since the problem of microwave interception did not seem to conveniently fall into the lap of any particular agency, it was natural that an interagency task force would be looked to as at least an initial means of developing a solution. The Press committee is itself the latest version of prior multi-agency efforts that have attempted to deal with the problem.

But task forces and multi-agency efforts are generally best suited to particular sets of circumstances. Their attempts at brokering can be loaded with trip wires. Task-forcing smacks of temporariness.[91] It attempts to create a system--a set of working operational boundaries--where none existed before. In this case, the lines of the system must lay across hundreds of prior system lines, not only the traditional and formal lines (domestic/foreign, civilian/military, private/public), but also lines of standing jurisdictional compromises, budgetary processes and personal relations.

An attempted new, or overlaying, system can build on these old alliances and procedures, or it can try to remake them or even fight them. But now add to this snapshot view of systems the fact that the structural nerves of the existing systems are not static. In their own right, even without the new problem, the lines are constantly shifting, even fluid. Then the complexity of the task facing the White House begins to emerge.

Thus, with regard to the microwave interception problem, who can rein the NSA when that organization has no operating charter, is used to floating authority, is moving into uncharted territory, is under attack and apparently is maneuvering for authority? Will it be the DCI, with his budget and task assigning authority, or the Secretary of Defense, with his operational authority? Or will NSA be able to run, somewhat unchecked, down corridors of divided authority?

And who will broker between the Department of Justice and NSA if Justice attempts to look over the shoulder of NSA's operations? Who will goad Justice if Justice does not keep a watch on NSA?

How can the President's Science Advisor make sure the boundaries he wants to establish are reflected in the charters being written by congressional staff? Shall NSA be given total authority over encryption and key control? Who decides? Who gives? If NSA is not given such authority, who will "monitor" all of the "keys"? Who is to determine what is sensitive anyway? And at the very rudimentary level of securing government telephones, a task traditionally assigned to NSA, how can the Science Advisor, who has "responsibility" after all, have a strong voice in what is or is not secured?

Who has the clout, or enough vested interest in this project, to force and focus enough money into the project to keep it afloat? Shall money go to the FCC to spur innovation? Who responds to the possibly thousands of companies that must be involved in sensitive data flow? Shall the Department of Commerce work with these companies? NSA?

How can the Press committee allay public fears, perhaps real or misplaced, of "big brotherism" on this issue? How can the Press committee decide how much should be made public, or respond to media calls, when the particulars of the issue are flung through a dozen agencies that are not under its control?

It is fair to speculate that a system of the magnitude necessary here cannot be created by the stroke of a pen, even the President's pen. In reality, the President is merely another player here, and he and his close advisers, including the science advisor, are fighting a number of other battles with the same players, battles that inevitably will bear on this

struggle. There is, for example, the technology export battle.[92] The B-1 bomber decision concerned many of the same players, and the 200-mile ocean boundary limit dispute does too, since it would affect our off-shore electronic eavesdropping of alien countries.[93] And, of course, there is the intelligence community reorganization battle.

It is significant that in the intelligence community reorganization struggle, the DCI, with the apparent backing of the President and the Senate, has not been able to come away with the kind of powers he felt he should have over defense intelligence organizations, such as NSA.[94] There simply are forces larger than Presidents and Congresses, at least in the short run.

Granted the stakes are larger in the reorganization struggle than in the shiftings for authority in the microwave interception issue. But the question can be raised: if the DCI, a high profile line manager, could not maneuver organizations as he saw necessary, can the relatively low profile staff position of Science Adviser?

D. Strategies and consequences: compatibility or fragmentation?

The consequences of centralization and decentralization, of control or the lack of control, are not only in the areas of authority and prestige. The consequences manifest themselves in a very real way in the technological equipment that is the product of a system or of mere chance.

It is not clear from publicly available information what strategy, if any, the White House has for the development of telecommunications security equipment for private sector communications. At least two scenarios, however, can be reasonably imagined: (1) closely controlled development under the umbrella of centrally determined standards; and (2) relatively uncontrolled development without centrally determined standards.

The first alternative better positions the White House to fulfill

its assignment"... to monitor the various parts of the program..." There are other possible benefits as well: better protection of communications (and communicators); equipment quality control; and equipment compatibility.

But these benefits are not without a concurrent condition, and that condition is one of "trust." The promoters and benefactors of central security control must be prepared to vest in the controlling unit the trust that the controlling unit will exercise its power only for legitimate purposes. And this is a confidence not easily generated. Practically every institution that has been trusted with information (government, business, education, etc.) has at one time or another violated that trust. The history of confidential information is pockmarked with breaches of that confidence.[95]

Thus, it would be with some legitimacy that users of a centrally secured system might suspect, for example, that an announced goal of a centralized system for reasons of protection or compatibility is really a ruse for access to private or commercial information. And this suspicion could well be justified, at least in an historical context, however honorable may be the intentions of the central securing power.

This balancing of caution and trust, then, becomes a policy issue for the White House and others, for if the factors of mistrust are too great (because, e.g., the system is too centralized in the view of given players, or because the system is centralized in particular organizations), the system simply may not be used and thus may not work.

A controversy centering on NSA's control of computer encryption equipment serves as an example. The exportation of any computer encryption device requires a license from the Office of Munitions Control at the State Department. That office says it routinely refers all such license requests

to DOD, where the matter is referred to NSA for approval or disapproval. The reported pattern of approval has been to approve only those devices with a key size (or string of bits) about the same as or smaller than the 56-bit Data Encryption Standard (DES), designed by IBM and put forth by the National Bureau of Standards. NSA is alleged to have worked closely with IBM in the development of the DES.[96]

The DES is used by a number of domestic companies, probably in no small part due to the fact that it is the standard for export. But according to Science magazine the DES also is shunned by a number of American companies.[97] It is felt by some that NSA's being so tightly tied to the development and control of the DES can lead to a reasonable conclusion that NSA can crack any code developed with the DES. And that raises the issue of trust. Citibank plans to use the DES, but as one Citibank official is reported to have told Science magazine: "Few people in the U.S. trust our intelligence agencies."[98]

This suspicious postulate assumes NSA will use its control for, among other things, privileged access to private communications. The issue of privacy is raised. But NSA could as well be exercising its power in a protective sense: to protect unsophisticated private companies from purchasing computer encryption equipment that would make the companies, and hence the nation, vulnerable to interception.

If trust is a condition of centralized security, how offsetting are the benefits? An examination of one possible benefit--equipment compatibility--gives some indication.

The benefits of compatibility can perhaps best be realized by examining the absence of compatibility. A DES computer, for example, might have difficulty "talking" securely with a non-DES computer. A connection probably

is technically possible, but it has at least two costs: time and money. The time cost is the additional time it would take for signal processing through the interconnecting devices--not insignificant when signal pulses are measured in millionths of seconds.

The financial cost can be a genuine barrier. Theoretically, almost any two telecommunicating devices can be interconnected, if the money is available. The policymaker has to ask at what point does financial cost become so expensive as to amount to a practical barrier to compatibility.

If, for example, private industry telephones are to be secured with encoding and scrambling devices, but the various devices have not been made technically compatible, then secure communications becomes much more cumbersome, if not impossible. Since most security devices are terminal based, or attached to a particular telephone, convenience and security are impaired when a caller wishes to make a secure call, but is not near a secured telephone. This may happen frequently when a company official is away from his office.

The Electronic Secure Voice Network (ESVN) is just such a terminal based security system. Procured by NSA, it has been operated on an experimental basis, but under the President's counter-interception program, its number of terminals is being expanded from 100 to 250.[99] According to one writer, ESVN works as follows: the caller's speech is digitalized, and the digitalized signals

> . . . are then encrypted, using a code generated by the central computer, transmitted over the regular telephone circuits, and decoded by the ESVN equipment at the other end. . . . Because the computer . . . generates a random code which is used only once for each phone call and then discarded, the resulting signal is regarded by most cryptologists as virtually unbreakable. Furthermore, the theft of the equipment would not compromise the codes, since they are constantly changing.[100]

But ESVN is a closed system---it can talk only to its own kind. The system probably could be expanded almost indefinitely (assuming the current $35,000 cost per terminal would be reduced by large scale), and thus ESVN could fit within either scenario. But the issue of ESVN is not technological gadgetry or perhaps even financial cost. The issue of ESVN is generic to the issue that separates the two scenarios, and that, again, is the issue of trust.

Other dynamics of security compatibility also should be mentioned. They can perhaps best be understood by examining an analogous situation Canada is facing with its two independent public "packet-switched" data networks. It is only through considerable effort that the two systems can be made compatible.[101] "The fact that two different access protocols are needed for accessing the Datapac and Infogram services discourages the joint use of both networks," says Gregor Bochmann of the University of Montreal.[102] Other dynamics, Bochmann points out, are that

> Large computer manufacturers often do not collaborate in the setting of standards, since standards increase the possibilities of competition. Computer and terminal manufacturers with smaller market shares favor standards because they open 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.[103]

These pressures result in a direct, and limiting, impact on users: "In the absence of standards, competition between different service offerings is limited to the initial period when the user makes the choice of buying one or the other of the services offered. Once a service has been adopted, it is very difficult for the user to change to a different service or manufacturer. . ."[104]

Bochmann concludes that progress can be made

> . . . only if the users exert sufficient pressure on computer manufacturers to develop and adhere to higher level protocol standards. . . . Government policies and regulations could assist in the development of telecommunications standards by promoting interworking between different data networks. . . ."[105]

It is not difficult to imagine analogies of what Bochmann describes being played out in the microwave interception arena. Small manufacturers of security devices might strive for features that make their devices compatible with the devices of other companies, since the small manufacturers do not have a commanding share of the market. But manufacturers, as Bochmann says, might tend to develop incompatible equipment, so as to discourage competitive link-ups.

Major carriers, on the other hand, might argue before their regulators for compatibility, but only so long as the regulators tend to sanction monopolistic conditions on behalf of the carriers. As has been stated, the trend with the FCC is toward more competitive conditions, and this might affect the arguments of the major carriers.

As in the Canadian situation, the critical time point might be during early user hook-ups. The early decisions set the conditions for compatibility for future decisions. It can be speculated that, for telephone security devices, the critical time point is now.

As for "user pressure," most likely that would come through the actions of the corporations most directly affected by government pressure or by the threat of a security breach. But whom would these corporations pressure? The FCC? The Department of Commerce? NSA?

Most likely the users would pressure the White House. After all, it has been reported that it was the White House that called the executives

of the eleven telecommunications companies and twenty-seven other companies together in the first place.[106] But as has been discussed, it is far from certain that the White House can command the kind of control necessary (and the kind of assistance Bochmann suggests) to bring about compatibility.

As has been stated, a White House strategy approaching the centralized/decentralized control issue has not been made apparent. It is known, from news reports, that at least at one time the White House was looking at the option of

> A well-publicized effort to encourage private corporations and business groups, such as the New York Stock Exchange, to purchase protective devices to better secure their telephone communications. This approach would include urging the Federal Communications Commission to require that telephone companies offer various types of secure telephone service, and making public some of the technical security devices developed by the National Security Agency.[107]

At least substantial parts of this option appear to have been later adopted ("Industry and such agencies as the Federal Communications Commission will be encouraged to speed the development and use of equipment and procedures that will make it more difficult for eavesdroppers to secretly record the telephone messages"[108]). But there still is no solid clue on the degree of control that will be exercised or the amount of compatibility that will be encouraged.

The trend of FCC equipment decisions since the late 1960's, not incidentally at the behest of the White House at that time, already has set a pattern of encouraging the diversity of design and ownership of equipment.[109] If this pattern were extended to security devices, the competition could be healthy, but compatibility could suffer. Islands of security technology could develop without sufficient links between the islands. This would seem to make the "system" more vulnerable to inter-

ception, and make tougher the White House led committee's assigned task to ". . .monitor the various parts of the program. . . ."[110]

E. Who pays? News stories of the Administration's anti-intercept program give some beginning figures that portend the magnitude of costs that may lie ahead.[111] Telephone security research will be increased from $10 million in fiscal year 1977 to $15 million in fiscal year 1978. Rerouting of government telephone calls into underground cables will cost an additional $10 million. And the ESVN program--the Electronic Secure Voice Network for key surveillance targets--will be increased from the current 100 units by an additional 150 units, at $35,000 each.

All of these costs are to be paid by the government, but they are only beginning costs. The underground cable program applies only to Washington, New York and San Francisco--the only places where, we are led to believe, the Soviets have listening posts.[112] As the use of interception technology becomes more facile, and as more and more domestic calls are sent by satellites, with their continental and extracontinental beams,[113] where does logic draw a limit as to the number of government lines that must be placed underground or undersea?

Likewise, what dent will 250 ESVN telephones put in the total non-governmental telephones that need security? An ESVN telephone cannot talk securely, through the ESVN device, to a non-ESVN telephone.

"Experts" are quoted as saying that scrambling the 68% of all domestic long distance calls that are now transmitted by microwave would cost between $2 billion and $3 billion.[114] That is approximately equal to all the funds the Carter Administration plans to set aside in its current budget to boost the American city.[115]

With such large dollar magnitudes, it could be speculated that the costs will be at least partially spread among private users of the secure phones, and possibly among non-users--the general public--as well. The Administration's announcement gives credence to this possibility. The Federal Communications Commission (FCC), it is stated, is being "...encouraged to speed the development and use of equipment and procedures that will make it more difficult for eavesdroppers to secretly record telephone messages."[116] American Telephone and Telegraph (AT&T) has been asked "to plan new ratings for telephone service that would allow the subscriber to choose and pay for various levels of security."[117] There could be arguments before the FCC as to what is "necessary or desirable in the public interest."[118] It could become a trade-off among users, the government, and non-users. The non-users, through increased telephone rates, would be absorbing some of the costs directly, and other costs indirectly as consumers and taxpayers. If so, it could be argued that the American public would be paying for what essentially is part of the defense budget through their telephone bills. Charges of taxation might arise, together with studies of the incidence of the alleged tax. With the increasingly high visibility of many of the regulatory bodies, including the FCC, the entire matter, including the security devices for which any funds are spent, might come under close public scrutiny.

Among the questions that might be asked would be those asked by the New York Times, in its editorial of November 24, 1977, in which it protested even the current program of spending $10 million to reroute government telephone lines. "Even if successful, this strategy is rather like taxing homeowners for bars on their windows because the police prefer not to catch burglars," the Times said.[119]

There is, however, a dissenting view of the potential costs that lie ahead. Richard Garwin, a consultant to the Senate's Select Committee on Intelligence, states that,

> Voice links carrying defense information are all encrypted. Other important information of the federal government can be rerouted to avoid some small number of possible listening posts. Direct-distance-dial calls eventually will be relayed with the destination and origination information going over separate channels. When all-digital transmission is used to carry voice, encryption can be available at negligible cost. It could be implemented with separate keys for each microwave link, or encryption could be done at the point of digitizing each signal, or both.[120] (emphasis added)

Moreover, Garwin adds, with respect to the growing use of satellite relay systems,

> Although some satellite relay is digital in nature and thus readily protected by encryption at negligible added cost, the voice communication is primarily analog.... Encrypted voice communication would require a wider channel at present than is needed by analog voice, but the additional cost for privacy via encryption might be small even so, since the satellite resource is a small part of the end-to-end communication cost.[121] (emphasis added)

The leap from the problems of scrambling to the apparent ease of encryption is one of time and technology. Telecommunications networks are being transformed from an analog to a digital base. Once in digital form, encryption is relatively easy, but the conversion from analog to digital will be slow. To speed it up would be expensive.

Moreover, some "senior Administration sources" have been quoted comparing the costs of both analog and digital scrambling or encryption with underground cables, and in their view, all three were extremely expensive.[122]

The Times quotes an Administration source as saying:

> He said basic studies showed that there were three main ways to maintain security. They are the following: Telephone carriers could install a special set of underground high-security lines. This is the most costly option, said one source, and the "most unlikely". Another source familiar with communications costs said the price of underground lines could be in the "billions".
>
> An electronic system similar to one now used on some Government curcuits could be installed to "scramble" the sounds of calls on certain lines. An efficient scrambler can cost $5000 for each terminal, according to one electronics expert. A senior Administration source called the Scrambler phone "no solution".
>
> Long-distance telephone communications could be coded.... The N.S.A. is testing a special limited model of this system, Electronic Secure Voice Networks, in 100 Government offices. This method, one source said, is the most secure, but is also vastly expensive.[123]

It appears that the matter of cost could be with us as a very substantial issue.

F. Privacy. The privacy debate, as it applies to microwave interception, seems to be divided between those who are prepared to permit considerable erosions of privacy, simply because they feel it is too difficult or impossible to do otherwise, and those who are determined that the fundamental application of our freedom from unwarranted search shall continue.

The issue is well stated by Richard Garwin, consultant to the Senate Select Committee on Intelligence: ". . .the expectation of privacy for the contents of a post card sent through the mails is quite different from that of a first-class letter in a sealed envelope, and the cost of an envelope is not regarded as an excessive charge for the guarantee of privacy. As the human senses and capabilities of vision, hearing and memory are expanded by the use of new tools, what is the place for the analog of better envelopes?" [124]

A news report on the development of telephone security costs comments:

> ...others in private communications suggest that, in fact, many in this country may have to give up the idea that a telephone communication will have any privacy. Congressional experts on wiretapping and eavesdropping concede that even the Administration's new wiretapping legislation does not comprehend the ease with which the technology lets someone listen in. "I'm not sure communications privacy isn't passe", a Senate Intelligence Committee aide said last week. But others, including several Administration officials, still believe that laws and protections must and can be worked out for an era in which the air waves carry not only voices and pictures but also bank transfers and business files.[125] (emphasis added)

As noted earlier, the Senate Select Committee, in looking at NSA's Shamrock program, concluded, with regard to legal restrictions and privacy, that NSA has violated the Fourth Amendment, Section 605 of the Communications Act of 1934 (47 U.S.C. 605), and the National Security Council Intelligence Directive under which NSA was operating.[126]

The Department of Justice has, at several points, attempted to check some of the activities of NSA described above, but not always with success.[127]

And the New York Times editorialized recently that current Soviet monitoring of American microwaves "would be illegal if our intelligence agents did it and is surely illegal for foreign agents".[128]

Finally, by way of summary, a subcommittee of the Senate Judiciary Committee states in a report on "Surveillance Technology" that "...the relevant basic constitutional rights of U.S. citizens are those articulated in the First, Fourth and Fifth Amendments and implied in the concepts of the right of privacy and protection against a 'chilling effect'."[129]

The right of privacy is the particularly subtle and significant protection of the American people that possibly is jeopardized by the microwave interception, by whatever power. The Senate Judiciary Subcommittee states

that "the right of privacy involves two distinguishable aspects: 1) the 'right to be let alone', which suggests that certain surveillance practices and technology utilization might be prohibited, and 2) the 'right to control information about oneself', which assumes the legitimacy of the actual collection of information".[130]

Historically, the right arose in the Bill of Rights in response to the practice by authorities of seizing private papers, by breaking and entering if necessary. "Protection against such an invasion of 'the sanctities of a man's home and the privacies of life' was provided in the Fourth and Fifth Amendments", wrote Justice Louis Brandeis, in his dissent in Olmstead v. United States, 277 U.S. 438 (1927). The right had deeper roots, Brandeis said, in the effort

> ...to secure conditions favorable to the pursuit of happiness. They (the Founding Fathers) recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone--the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means, be deemed a violation of the Fourth Amendment.

Brandeis went on to find that "...the defendant's objections to the evidence obtained by a wire-tapping must, in my opinion, be sustained. It is, of course, immaterial where the physical connection with the telephone wires leading to the defendant's premises was made." (emphasis added)

Brandeis' dissent eventually was adopted forty years later in Burger v. New York (388 U.S. 41) and Katz v. United States (389 U.S. 347).

With respect to individuals, the right of privacy in domestic microwave telephone transmissions would seem to be a clear one, regardless of where the domestic interception takes place. It is a right with such deep roots that it is not likely to be given up easily. In fact, refinement of existing privacy protection laws is an ongoing process and one of current concern to Congress.[131] An acknowledged problem is the law and its lag behind the rapidly advancing technology.[132]

The thrust of the Soviet interests and efforts is said to be directed against private commercial interests, namely the decisions, interests and activities of corporations. In the matter of privacy, it could be argued that the rights of corporations should be quite different than the rights of persons.[133]

However, the effects on corporations of the absence of the right of privacy (the "chilling" effects, the discouragement of dialogue and exchange) could be very similar to the effects on individuals, so that the reasons for including corporations in the privacy protection would be sound. And, in fact, it has been held that corporations are due the same privacy rights as individuals.[134]

However, a right can be surrendered by consent of the holder, and, as we have seen, several corporations during the Shamrock program (RCA Global, ITT, Western Union) seemed to have surrendered their right of privacy to NSA. Arguments can be made that the consent must be an informed consent, but that is a legal issue probably more successfully argued by individuals than by corporations.

Here again, however, the microwave interception problem has placed a government agency in the awkward position of possibly impairing corporate

privacy in an effort to enhance corporate security. It is not difficult to imagine a corporation's accepting Defense Department offers to assist in corporate communications security. And it is not difficult to imagine Defense Department officials' dealing with general business firms as if the firms were defense contractors, since the defense contractor possibly is the department's strongest current operating model of how to deal with the private sector. Yet placing general business firms in the same category as defense contractors could be viewed as a subtle usurpation of the traditional protections of the civilian from the military.

Centralized control of encryption also can jeopardize privacy, particularly if the U.S. follows the British pattern whereby the U.K. Post Office "must be able to monitor all data transmissions that cross the U.K. borders. If a transmission is coded or encrypted, the Post Office has rights of access to the codes or keys".[135]

Then there is the matter of technology. Assuming again there are clear laws against microwave interception, is it possible to detect such an interception so that at least it is known that there is a violation? The answer is "probably so". A Senate Judiciary Subcommittee report states at page 36:

> Message interception by microwave and other advanced technologies, presents an important development in surveillance technology. These innovations permit the interception of messages without visible communication linkages. Although they might be detectable through emission monitoring and other techniques, they remain a new and undetermined force in surveillance operations.[136] (emphasis added)

Moreover, in the news report disclosing the announcement of the Press Committee, the question of our knowledge of the Soviet intercept practice was raised: "The officials, who said that for security reasons they could not describe 'how we know what we know' said that the Soviet Union is conducting surveillance from four sites in three cities."[137]

However, there is a view that the principal means of detection would be nothing more sophisticated than physical observation of the intercepting antennae. According to the "Mitre Report", a study of electronic interception done by the Mitre Corporation for the Office of Telecommunications Policy, "the principal form of detection of radio interception activities is physical surveillance. The principal observable would be intercept antennae".[138]

Even supposing land based interception of microwave could be detected and stopped, off-shore and satellite pickup present another set of privacy problems. According to a report in the Atlanta Constitution,

> The government also is believed to be concerned about the possibility that Cuban intelligence agents may be using spy ships or powerful satellite "earth stations" in Cuba to eavesdrop on domestic telephone calls within the United States. According to telecommunications experts, the microwave relay signals from the new Comstar domestic communications satellites, which are now handling a significant portion of the nation's domestic long-distance phone calls, could be picked up as far south as Cuba by an earth station with an antenna about 200 feet in diameter. The signals also are accessible over many square miles of international waters, the experts say. Richard Garwin, a consultant to the Senate Intelligence Committee, said in a paper that "...non-U.S. citizens on non-U.S. territory are completely free to receive satellite relay of domestic U.S. communications and to do with this information whatever they will. Domestic satellite relay, as presently practiced," Garwin wrote, "is an example of a case in which the indisputable benefits of technology bring with them a threat to privacy."[139]

As an example of off-shore intelligence gathering, our own ill-fated Pueblo ship allegedly was collecting communications signals off the Korean coast in 1968 when it was captured.[140]

Garwin states in a Senate Select Committee report that the signals can be protected by encryption, and by avoiding fixed assignment schemes.[141] However, others dispute his optimism, either for reasons of cost or because of the time it will take for technological transformation.

Another writer has said AT&T has developed a system that "separates the communications channel of the number that the caller dials from the channel on which the conversation is carried. To a Soviet computer programmed to correlate conversations with call-up numbers, this would be tantamount...to receiving 'a letter without an address on the envelope'"[142] (The reference is to Common Channel Interoffice Signaling (CCIS)).

But the same writer goes on to add that "Such innovations only buy time...until Soviet computer-analysis programming catches up."

One also has to ask whether even underground cabling is technically secure. The Mitre report concludes that open-wire and underground multipair cabling are "relatively easy to tap". Only pressurized coaxial cable seems relatively secure, but even with it, "There are a number of... tactics that when coupled with judicious selection of time and place would render detection impossible."[143]

In light of all this, one can speculate that it is no wonder the Carter Administration decided to allow the Soviets to continue exercising what appears to be an inevitable ability to intercept many of our communications. The President seemed to say as much at his news conference on July 13, 1977 when he was asked about the microwave interception problem: "...the intercept on a passive basis of these kinds of transmissions has become a common ability for nations to pursue. It's not an act of aggression or war. It's completely passive."[144]

As a footnote to the privacy issue, it can be assumed that the one-half of American long-distance international calls that go by satellite are vulnerable to interception.[145] Moreover, there remains the issue of privacy in the Korean interception case mentioned earlier.[146] What privacy should an American citizen or corporation expect when information about them develops during the interception of foreign telecommuni-

cations by our intelligence agencies?

Thus, in the face of foreign policy and modern international technology, the effectiveness of domestic privacy laws seems to be a genuine problem.

G. Foreign policy: WARC's,data flows and data havens.

Peter L. Szanton, in his essay "The Future World Environment: Near Term Problems for U.S. Foreign Policy",[147] sketches several alternative environments the United States may face in the near future. His comments summarize, in his role as research director, part of the views of the Commission on the Organization of the Government for the Conduct of Foreign Policy (June, 1975).

Among the common themes in the several environments, are increasing economic interactions and interdependence and the growing role of international collaborations and possibly institutions.

Under one scenario, for example,

> The foreign-domestic policy distinction nearly disappears. From the point of view of U.S. decisionmaking, the most important implication may be that the distinction between foreign and domestic policy, eroding for 50 years, may virtually disappear. As to all major economic, monetary, and budgetary decisions, there will inevitibly be important foreign policy implications; and vice versa.[148]

In another "Most Nearly Agreed" future, "...the tasks of U.S. foreign policy...will be two-fold: to help build the processes and institutions for world collaboration and order and to foster the evolution of the major states in ways conducive to a cooperative order."[149]

From the standpoint of the issue addressed in this paper, these comments seem particularly pertinent in these two respects: (1) economic data may become a kind of currency over which and through which power is gained and lost; and (2) data flows will become increasingly transnational, subject to whatever "processes and institutions" are the products of com-

peting international pressures.

Already there is a lexicon and a body of practitioners focusing on the issues of trans-border data flows (TBDF). A conference was held in Vienna in September 1977, sponsored by the Organization for Economic Cooperation and Development (OECD), to address "problems raised by the rapid growth in volume of data crossing national boundaries on computer networks".[150]

When flung across the international matrix, the issues of costs, vulnerability, and compatibility are dramatically complicated.

The following are examples of the kinds of issues being raised:

(1) Satellite transmission interception. One review of the OECD conference stated that "...we suspect that the transmission of encrypted data by satellite will soon be recognized as a potential problem area".[151] This raised the problem of extensive encryption, since there could easily be "'tapping' of satellite transmissions for surreptitious reception". ..."If everything is encrypted, everything would be hidden--and anything could be transmitted as 'data'. This means that national security information, sabotage instructions, trade secrets, and so on could be sent out of a country disguised as routine data, and who would know except the senders and recipients. Moreover, because satellite transmissions can be received at so many places on the earth, there would be no way to know just who the true recipient really was".[152]

(2) Sovereignty and storage. The review continued: "The other main thread was the loss of national sovereignty that could occur when records of great value to organizations within one country were stored and processed in another country. The economy of the first country might thus be somewhat under the control of the government of the second country".[153] Even if the second country's government were friendly,

strikes, bankruptcies, or changes in governments could make the first country's data vulnerable. Another type of vulnerable access develops where, "Many U.S. organizations have used data entry (key punch) services in other countries to obtain lower costs for large volume data entry jobs".[154]

(3) Data havens and Swiss bank accounts. A U.S. House of Representatives Communications Subcommittee background report notes that even if international conventions on interceptions and privacy are arrived at, there are the dangers of "data havens" developing. Like "tax havens' or "flags of convenience" nations, these nations might "...proliferate as users in countries with strict regulations move their operations to contries having either no law or very liberal practices".[155] Representative Barry M. Goldwater, Jr. foresees, according to the report, "that individual nations or powerful financial interests could deliberately implement a data communications and service operation that would have as its sole objective the circumvention of various national information statutes. There is apparently some practice of 'data piracy', although no one seems to know the extent or seriousness of the situation".[156] The report also says there is concern over the emergence of "data cartels" from agreements among select nations with common economic interest.[157]

(4) Licenses and products. The OECD conference review raises the issue of whether or not "data is to be considered a 'product'. If data is considered a product, it may then be subjected to many of the export and import controls to which products are subjected".[158] This, in turn, could lead to the requirement of licenses for those involved in producing or processing the data.

(5) Privacy laws and harmonization. The House background report

notes that "...only Sweden, West Germany, and the United States have national privacy acts. Sweden and West Germany extend their laws to data transported, processed, and accessed outside of the country. Except for Sweden, none of them deal with the activities of private enterprise".[159] The conference review paper says we can expect a number of other nations to begin writing privacy laws but that it will be some time before the laws are "harmonized". In the meantime, data producers and processors may operate at the peril or adhering to one nation's laws while breaking another's.

Harmonization at the very basic level of coordinating frequencies is being worked on through the International Telecommunications Union (ITU) and its World Administrative Radio Conference (WARC).[160]

(6) Compatibility. Finally, if compatibility of equipment within a country raises the kinds of issues that were raised under Section II.D. ("Strategies and consequences: compatibility or fragmentation?") of this paper, one can anticipate that the compatibility problems might increase geometrically in the international sphere.

At the very least, then it is clear that the arena of "strategic economic warfare" is moving to a much higher international plane and that our problems of domestic microwave interception might in time seem small in comparison. Already "the U.S. has the most companies dealing in international trade of any country".[161] And already other international bodies, including the United Nations, the Nordic Council, the European Economic Community, and the Council of Europe have all expressed an interest in becoming involved in the issues.[162]

Peter Szanton's prediction of the increasing role of economics and internationalism in domestic decision making seems to be coming true.

The arm-load of problems and policy points which the Press Committee must "monitor" and for which the committee is "responsible" may be just the beginning.

## NOTES


1. New York Times, November 20, 1977.
2. Boston Globe, July 16, 1977, p. 25.
3. Washington Star, July 23, 1977; U.S. Senate. Surveillance Technology. A staff report of the Subcommittee on Constitutional Rights of the Committee on the Judiciary, p. 1026. 1976.
4. Boston Globe, July 16, 1977, p. 25.
5. Atlanta Constitution, April 3, 1977.
6. Ibid; Washington Star, April 27, 1977.
7. Kolata, G.B. 1977. Computer Encryption and the National Security Agency Connection. Science 197:438-439.
8. Business Week, December 12, 1977, p. 57.
9. New York Times, November 20, 1977.
10. Ibid.
11. New York Times, August 29, 1977, p. 1.
12. Wall Street Journal, October 12, 1977.
13. U.S. Senate. Supplementary Detailed Staff Reports on Foreign and Military Intelligence. Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities. Book IV, p. 114.
14. New York Times, December 27, 1977, p. 11.
15. New York Times, August 29, 1977; Atlanta Constitution, 1977.
16. New York Times, November 20, 1977.
17. New York Times, December 27, 1977, p. 11.
18. Oettinger, Anthony G., Paul Berman and William H. Read. High and Low Politics: Information Resources for the 80s, Ballinger Publishing Company, Cambridge, Ma., 1977, pp. 64, 95.
19. New York Times, July 10, 1977, p. 1.

20. New York Times, November 20, 1977.

21. New York Times, August 29, 1977, p. 1.

22. Report to the President by the Commission on CIA Activities Within the United States, 1975. U.S. Government Printing Office, p. 8.

23. Remarks of the Vice President At the National Broadcast Editorial Association Annual Meeting, Mayflower Hotel, Washington, D.C., June 9, 1976. Office of the Vice President.

24. New York Times, July 10, 1977, p. 1.

25. Atlanta Constitution, April 3, 1977.

26. New York Times, July 10, 1977, p. 8.

27. New York Times, July 11, 1977.

28. New York Times, July 13, 1977.

29. Press Release, Office of Senator David Patrick Moynihan, July 27, 1977.

30. New York Times, November 20, 1977.

31. Computer World, March 27, 1978, p. 1.

32. New York Times, November 20, 1977.

33. New York Times, July 10, 1977, p. 1.

34. New York Times, December 20, 1977.

35. Business Week, December 12, 1977, p. 57.

36. Oettinger, Anthony G., Paul Berman and William H. Read, 1977. Op.cit., p. 103.

37. New York Times, December 27, 1977, p. 11.

38. New York Times, December 25, 1977, p. F5.

39. Oettinger, Anthony G., Paul Berman and William H. Read, 1977. Op.cit., p. 107.

40. Atlanta Constitution, April 3, 1977; New York Times, August 29, 1977.

41. Business Week, December 12, 1977, p. 57.

42. Business Week, December 12, 1977, p. 57.

43. New York Times, November 20, 1977.

44. Defined in Presidential Executive Order #12036 (U.S. Intelligence Activities), issued January 24, 1978; 43 Fed.Reg. 3674-3692, Jan. 26, 1978.

45. U.S. Senate. Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans. Final Report of the Select Committee to Study Governmental Operations with respect to Intelligence Activities. Book III, p. 738. 1976.

46. Ibid.

47. U.S. Senate. Foreign and Military Intelligence. Final Report of the Select Committee to Study Governmental Operations with respect to Intelligence Activities. Book I, p. 44. 1976.

48. Presidential Executive Order, January 24, 1978. Op.cit., at Secs. 1-5, 1-1202; New York Times, January 23, 1978, p. 11.

49. New York Times, January 23, 1978, p. 1.

50. Ibid., at 649; 1977/1978, U.S. Government Manual, p. 95; New York Times, December 25, 1977, Sec. 4, p. 1.

51. Atlanta Constitution, April 3, 1977; New York Times, July 10, 1977, August 29, 1977, November 20, 1977, December 27, 1977, p. 11.

52. New York Times, January 23, 1978, p. 1.

53. Ibid.

54. U.S. Senate. Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans. Final Report of the Select Committee to Study Governmental Operations with respect to Intelligence Activities. Book III, p. 764. 1976.

55. Boston Globe, July 16, 1977, p. 25.

56. U.S. Senate. Supplementary Detailed Staff Reports, Book III, p. 736.

57. Ibid., at p. 761.

58. Ibid., at p. 739.

59. Ibid., at p. 736.

60. New York Times, January 23, 1978, p. A21; 95th Congress, 2d Session, Senate Bill 2525 Sec. 142(6)(5).

61. Ibid; U.S. Senate. Surveillance Technology. A staff report of the Subcommittee on Constitutional Rights of the Committee on the Judiciary. 1976. p. 22.

62. U.S. Senate. Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans. Final Report of the Select Committee to Study Governmental Operations with respect to Intelligence Activities. Book III, p. 757. 1976.

63. Ibid., at p. 739.

64. New York Times, July 10, 1977, p. 1.

65. New York Times, January 25, 1978, p. A14.

66. Ibid.

67. Ibid., at p. 778.

68. Ibid., at pp. 740, 763, 770, 771.

69. Ibid., at p. 764.

70. Ibid., at p. 742.

71. Senate Bill 2525 Sec. 142(b) (5).

72. Ibid., at Sec. 613 (a) (20).

73. Ibid., at Sec. 231(a)(5).

74. Ibid., at Sec. 231(c).

75. Ibid., at Sec. 612(b).

76. Oettinger, Anthony G., Paul Berman and William H. Read, 1977. Op.cit., p. 103.

77. U.S. Senate. Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans. Final Report of the Select Committee to Study Governmental Operations with respect to Intelligence Activities. Book III, pp. 749-777.

78. New York Times, December 27, 1977, p. 11.

79. Ibid.

80. Ibid.

81. New York Times, July 10, 1977, p. 34.

82. Oettinger, Anthony G., Paul Berman and William H. Read, 1977. Op.cit., p. 64.

83. New York Times, December 24, 1977, p. 1.

84. U.S. Senate, Surveillance Technology. A staff report of the Subcommittee on Constitutional Rights of the Committee on the Judiciary. 1976, pp. 1023, 1059, 1061; New York Times, July 10, 1977, p. 1.

85. New York Times, July 10, 1977, p. 1.

86. Ibid.

87. New York Times, November 20, 1977.

88. Ibid.

89. New York Times, December 27, 1977, p. 11.

90. New York Times, November 20, 1977.

91. Benningson, Lawrence. 1971. The Strategy for Running Temporary Projects. Technology Communications, Inc. The Innovation Group. New York; Donnelly, J.H., Jr., Gibson, J.L., Ivancevich, J.M. 1975. Fundamentals of Management, Functions, Behavior, Models. Business Publications, Inc. Dallas, p. 283.

92. New York Times, January 4, 1978, p. A7; December 11, 1977.

93. New York Times, July 17, 1977; January 8, 1978, p. 20.

94. New York Times, December 24, 1977, p. 1; New York Times, January 23, 1978, p. 1.

95. Seipp, David J.; The Right to Privacy in American History, Program on Information Resources Policy, Harvard University, June, 1977.

96. Kolata, G.B. 1977. Computer Encryption and the National Security Agency Connection. Science 197:438-439.

97. Ibid.

98. Ibid.

99. New York Times, November 20, 1977.

97. Ibid. (See also: News Release, Senate Select Committee on Intelligence, April 12, 1978, entitled "Involvement of NSA in the Development of the Data Encryption Standard" and "The NSA Perspective on Telecommunications Protection in the Nongovernmental Sector," an address by Vice Admiral B.R. Inman, Director, National Security Agency, to the Armed Forces Communications and Electronics Association, February, 1979.)

98. Ibid.

99. New York Times, November 20, 1977.

100. Atlanta Constitution, April 3, 1977.

101. Bochmann, G. 1977. Standards Issues in Data Communications. Telecommunications Policy, December, 1977, p. 386.

102. Ibid.

103. Ibid., at p. 386.

104. Ibid., at p. 387.

105. Ibid., at p. 388.

106. Business Week, December 12, 1977, p. 57.

107. New York Times, August 29, 1977.

108. New York Times, November 20, 1977.

109. Oettinger, Anthony G., Paul Berman, and William H. Read, 1977. Op.cit., pp. 64, 95.

110. New York Times, November 20, 1977.

111. Ibid.

112. Atlanta Constitution, April 3, 1977.

113. U. S. Senate. Supplementary Detailed Staff Reports on Foreign and Military Intelligence. Final Report of the Select Committee to Study Governmental Operations with respect to Intelligence Activities. 1976. Book IV, p. 114.

114. New York Times, August 29, 1977.

115. New York Times, December 6, 1977.

116. New York Times, November 20, 1977

117. New York Times, July 17, 1977

118. 47 U.S.C. s. 201

119. New York Times, November 24, 1977

120. U.S. Senate. Supplemtary Detailed Staff Reports on Foreign and Military Intelligence. Final Report of the Select Committee to Study Governmental Operations with respect to Intelligence Activities. 1976. Book IV, p. 113.

121. Ibid, at p. 114.

122. New York Times, July 10, 1977 p. 1

123. Ibid.

124. U.S. Senate. Supplementary Detailed Staff Reports on Foreign and Military Intelligence. Final Report of the Select Committee to Study Governmental Operations with respect to Intelligence Activities. 1976. Book IV, p. 110.

125. New York Times, July 17, 1977.

126. U.S. Senate. Supplemtary Detailed Staff Reports on Intelligence Activities and Rights of Americans. Final Report of the Select Committee to Study Governmental Operations with respect to Intelligence Activities. Book III, p. 765. 1976.

127. Ibid. at p. 739; New York Times, July 10, 1977.

128, New York Times, November 24, 1977.

129. U.S. Senate. Surveillance Technology. A staff report of the Subcommittee on Sonstitutional Rights of the Committee on the Judiciary. p. 73. 1976.

130. Ibid, at p. 25.

131. Ibid, at pp. 68,81.

132. Ibid, at p. 46; U.S. Senate. Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans. Final Report of the Select Committee to Study Governmental Operations with respect to Intelligence Activities. Book III, p. 764. 1976.

133. U.S. Senate. Suplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans. Final Report of the Select Committee to Study Governmental Operations with respect to Intelligence. Book III, p. 742. 1976,

134. Seipp, D.J. 1977. The Right to Privacy in American History. Working Paper, Program on Information Resources Policy, Harvard University. p. 59.

135. Canning, R. The Debate on Trans-Border Data Flows. EDP Analyzer, Vol. 16, No. 4, April 1978.

136. U.S. Senate. Surveillance Technology. A staff report of the Subcommittee on Constitutional Rights of the Committee on the Judiciary. p. 36. 1976.

137. New York Times, November 20, 1977.

138. Mitre Corporation, Metrek Division. Study of Vulnerability of Electronic Communications Systems to Electronic Interception. Vol. 1, p. 17. McLean VA. Prepared for Office of Telecommunications Policy, Executive Office of the President, January, 1977.

139. Atlanta Constitution, April 3, 1977. See also Business Week, December 12, 1977, p. 58; U.S. Senate. Supplementary Detailed Staff Reports on Foreign and Military Intelligence. Final Report of the Select Committee to Study Governmental Operations with respect to Intelligence Activities. 1976. Book IV, p. 114.

140. New York Times, July 17, 1977. p. E6.

141. U.S. Senate. Supplementary Detailed Staff Reports on Foreign and Military Intelligence. Final Report of the Select Committee to Study Governmental Operations with respect to Intelligence Activities. 1976. Book IV, p. 114.

142. Business Week, December 12, 1977, p. 58

143. Mitre Corporation, Metrek Div. Study of Vulnerability of Electronic Communications Systems to Electronic Interception. Vol. 1, pp. 15, 16, 47, 48, 53, 54. McLean, VA. Prepared for Office of Telecommunications Policy, Executive Office of the President, January, 1977.

144. New York Times, July 13, 1977.

145. Atlanta Constitution, April 3, 1977; U.S. Senate. Supplementary Detailed Staff Reports on Foreign and Military Intelligence. Final Report of the Select Committee to Study Governmental Operations with respect to Intelligence Activities. 1976. Book IV, p. 114.

146. Wall Street Journal, October 12, 1977.

147. Szanton, P. The Future World Environment: Near Term Problems for U.S. Foreign Policy. Commission on the Organization of the Government for the Conduct of Foreign Policy (June, 1975). Appendices, Volume 1. U.S. Government Printing Office, Washington, DC.

148. Ibid, at p. 8.

149. Ibid, at p. 9.

150. Canning, R. The Debate on Trans-Border Data Flows. Op.cit.

151. Ibid, at p. 34.

152. Ibid, at p. 33.

153. Ibid, at p. 11, 27.

154. Ibid, at p. 34

155. Casey, L. Trans-Border Data Flows. Memo to Members, Subcommittee on Communications, Committee on Interstate and Foreign Commerce. October 3, 1977. U.S. House of Representatives. p. 23.

156. Ibid.

157. Ibid, at p. 30.

158. Canning, R. The Debate on Trans-Border Data Flows. Op.cit.

159. Casey, K. Trans-Border Data Flows. Memo to Members, Subcommittee on Communications, Committee on Interstate and Foreign Commerce. U.S. House of Representatives. October 3, 1977. p. 11.

160. FCC Reports 76-677, 60 FCC 2d, In the Matter of An Inquiry Relating to the Preparations for the 1977 World Administrative Radio Conference of the International Telecommunication Union for Planning of the Broadcasting-Satellite Service in the 11.7-12.2 GHz Bank, Adopted July 15, 1976, Released August 6, 1976.

161. Canning, R. The Debate on Trans-Border Data Flows. Op.cit.

162. Casey, K. Trans-Border Data Flows. Memo to Members, Subcommittee on Communications, Committee on Interstate and Foreign Commerce. U.S. House of Representatives. October 3, 1977. p. 24 et seq.

Appendix A

PRESIDENTIAL DIRECTIVE/NSC-24

Policy Guidelines

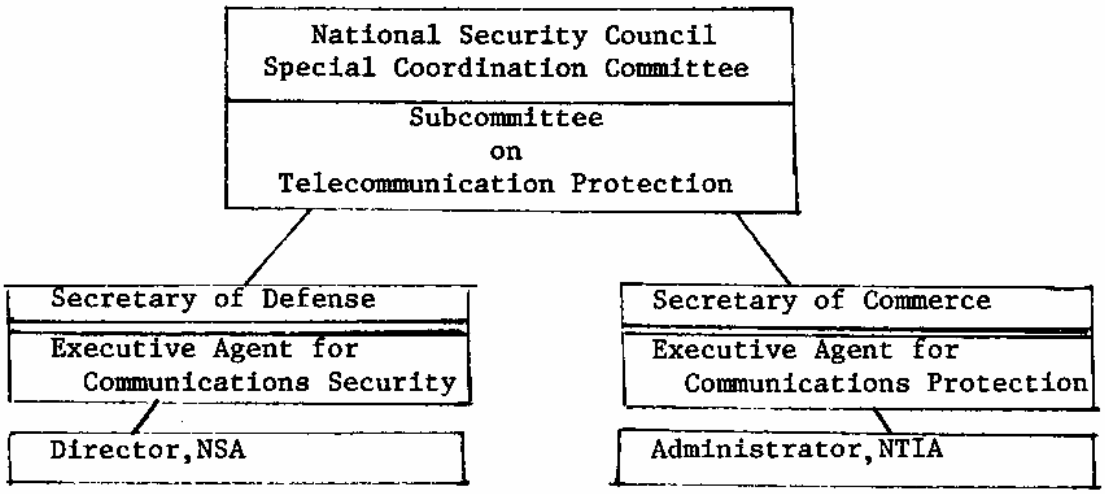
1. Government classified information relating to national defense and foreign relations shall be transmitted only by secure means.

2. Unclassified information transmitted by and between government agencies and contractors that would be useful to an adversary should be protected.

3. Nongovernmental 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.

* * * * *

ORGANIZATIONAL STRUCTURE



SENSITIVE UNCLASSIFIED
INFORMATION OF VALUE TO A
FOREIGN ADVERSARY

- Financial information
  - Planned changes in prime interest rate
  - Support of the dollar in foreign exchange markets
- Commodity market forecasts
- Supply of critical materials
- Strategies for international negotiations
- Selected high-technology information

* * * * *

GOALS

- Assure adequate protection is available, as warranted, against appropriate threats for selected U.S. government, U.S. government contractors, and private sector elements.
- Formulate a national policy on public cryptographic research.

* * * * *

SHORT-TERM OBJECTIVES

- Continued progress will be made in recommending interim protection measures for identified users in selected metropolitan areas based on available technologies, private sector services and equipment availability, and U.S. government resources.
- A national strategy and implementation plan will be formulated based upon:
  1. Policy analyses concerning key issues and national impacts, legal and regulatory requirements.
  2. System analysis to select a system concept and recommended specific technical solutions, consistent with available technology, industry plans, effectiveness.
  3. User-requirements analyses to specify user protection needs, user priorities and vulnerabilities.

## INTERMEDIATE-TERM OBJECTIVES

- All U.S. government and private sector related protection efforts will have been harmonized under a national strategy and implementation plan.
- Satisfactory protection measures will be available against known threats for identified government users in selected metropolitan areas.

* * * * *

## LONG-TERM OBJECTIVES

- U.S. government involvement in nonnational security protection will be harmonized and minimal, consistent with the evolving nature of the threat.
- As appropriate, adequate protection measures will be incorporated into network designs for new carrier, private sector, and U.S. government networks.
- Commercial limited-protection services and terminals will be widely available on demand at reasonable cost.
- Satisfactory protection measures will be available for appropriate U.S. government, U.S. government contractor, and private sector elements.

INTERMEDIATE-TERM OBJECTIVE

- A national policy on public cryptographic research will have been achieved.

* * * * *

SHORT-TERM OBJECTIVE

- A national policy will be formulated on public cryptographic research; an assessment of the appropriate role of cryptography in providing limited protection will be completed.

* * * * *

IDEAL PROTECTION

- Customer can specify protection services desired.
- Tariffed services for particular certified protection quality.
- Low cost/widely available services and equipment/interoperable.
- Competitive marketplace/innovation.
- Minimum government presence.

* * * * *

GOVERNMENT ACTIONS

* Transfer applicable government research and development information.

* Help to aggregate agency demand.

* Promote awareness in sensitive elements of private sector.

* Analysis of private sector technical alternatives for remedy.

* Promote federal communications commission regulations, or legislation as needed.

* Establish suitable government policy.

VULNERABILITY TO EXPLOITATION

- Terrestrial microwave radio
- Satellite communications

* * * * *

ON HOW CARRIERS CAN CONTRIBUTE:
*THOUGHTS WELCOMED*

- Best ways to enhance protection,
- Carrier capabilities to provide protection,
- Obstacles,
- Best ways for government to assist.

## Appendix B

### NATIONAL TELECOMMUNICATIONS PROTECTION POLICY

1. The President has reviewed the results of the NSC Special Coordination Committee's consideration of the PRM/NSC-22 study and has reached the following conclusions. It is the President's intention that the following statement of national policy be used to guide the conduct of U.S. government activities in and related to security of telecommunications.

2. The National Telecommunications Protection Policy shall consist of the following major elements:

   a. Government classified information relating to national defense and foreign relations shall be transmitted only by secure means.

   b. Unclassified information transmitted by and between government agencies and contractors that would be useful to an adversary should be protected.

   c. Nongovernmental information that would be useful to an adversary shall be identified and the private sector informed of the problem and encouraged to take appropriate measures.

   d. As a precautionary measure, the responsible agencies should work with the Federal Communications Commission and the common carriers to adopt system capabilities which protect the privacy of individual communications and to carry out changes in regulatory policy and draft legislation that may be required.

      Further, the laws which protect against criminal domestic acts such as wiretaps or intercept shall be strictly enforced.

3. The following activities should be pursued in support of the above policy.

   a. The private sector telecommunications carriers should be briefed on the nature of the threat and appropriate government research and development information shall be made available so as to help and encourage them to devise adequate protection strategies. A similar program shall be pursued for government contractors and other most likely affected industries, corporations and private sector entities.

b. The Secretary of Defense shall initiate through the industrial security mechanism, new and improved personal and telecommunications security measures among business organizations holding classified defense contracts.

c. All departments and agencies shall revitalize programs of security training for U.S. government personnel who use telephones and other means of communication for both unclassified and classified purposes.

d. Subject to continuous review of available technology and reassessment of the foreign intercept threat, the following immediate technical actions shall be undertaken:

(1) The Government shall conduct a multifaceted research and development program covering both system and user oriented protection approaches.

(2) Phase I and II of the DUCKPINS cable program shall be completed as soon as possible.

(3) Executive Secure Voice Network (ESVN) systems shall be installed when appropriate high priority requirements can be validated.

4. Management and policy review responsibilities for telecommunication protection shall be organized as follows:

a. The NSC Special Coordination Committee (SCC) shall be responsible for providing policy guidance and for ensuring full implementation of this policy, including effective protection techniques for the Government and maximum assistance to the private sector, to enhance its protection from interception. The SCC shall exercise this responsibility through a special Subcommittee on Telecommunications Protection chaired by the Director, Office of Science and Technology Policy, with administrative support provided by the Secretary of Commerce. The Subcommittee shall include, but not be limited to, representatives of the following departments and agencies: State, Treasury, Justice, Commerce, Defense, Transportation, Energy, Central Intelligence Agency, General Services Administration, the National Security Agency, and the National Security Council Staff.

b. The Secretary of Defense shall act as the Executive Agent for Communications Security (COMSEC) to protect government-derived classified information and government-derived unclassified information which relates to national security. COMSEC is concerned with protective measures designed for the security of

classified information and other information related to national security.

c. The Secretary of Commerce shall act as the Executive Agent for Communications Protection for government-derived unclassified information (excluding that relating to national security) and for dealing with the commercial and private sector to enhance their communications protection and privacy.

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

e. The subcommittee should choose a future implementation strategy based on cost-benefit analysis, legal considerations, and regulatory policy.

f. The heads of all departments and agencies of the Federal Government shall organize and conduct their communications security and emanations-security activities as they see fit, subject to the provisions of law, the provisions of this policy and other applicable directives, and the decisions of the subcommittee. Nothing in this policy relieves the heads of the individual departments and agencies of their responsibilities for executing all measures required to assure the security of federal telecommunications and the control of compromising emanations.