NATIONAL SECURITY AGENCY SURVEILLANCE AFFECTING AMERICANS

CONTENTS

	Page
I. Introduction and Summary	735
A. NSA's origins and official responsibilities	736
B. Summary of interception programs	738
C. Issues and questions	742
II. NSA's Monitoring of International Communications	743
A. Summary of watch list activity	743
B. History	744
C. Types of names on watch lists	749
D. Overlapping nature of intelligence community requests	750
E. Drug watch lists: United States-South American intercepts	752
F. Termination of the civil disturbance watch list activity	756
G. Authorization	761
H. Conclusions	764
III. A Special NSA Collection Program: SHAMROCK	765
A. Legal restrictions	765
B. The committee's investigation	766
C. The origins of SHAMROCK	767
D. The participation of the companies	770
E. NSA's participation	774
F. Termination of SHAMROCK	776
IV. NSA Personnel Security and Related Matters	777
A. Background	777
B. Questionable activities	777

NATIONAL SECURITY AGENCY SURVEILLANCE AFFECTING AMERICANS

I. INTRODUCTION AND SUMMARY

This report describes the Committee's investigation into certain questionable activities of the National Security Agency (NSA).[1] The Committee's primary focus in this phase of its investigation was on NSA's electronic surveillance practices and capabilities, especially those involving American citizens, groups, and organizations.

NSA has intercepted and disseminated international communications of American citizens whose privacy ought to be protected under our Constitution. For example, from August 1945 to May 1975, NSA obtained copies of many international telegrams sent to, from, or through the United States from three telegraph companies. In addition, from the early 1960s until 1973, NSA targeted the international communications of certain American citizens by placing their names on a "watch list." Intercepted messages were disseminated to the FBI, CIA, Secret Service, Bureau of Narcotics and Dangerous Drugs (BNDD), and the Department of Defense. In neither program were warrants obtained.[2]

With one exception,[3] NSA contends that its interceptions of Americans' private messages were part of monitoring programs already being conducted against various international communications channels for "foreign intelligence" purposes. This contention is borne out by the record. Yet to those Americans who have had their communications—sent with the expectation that they were private—intentionally intercepted and disseminated by their Government, the knowledge that NSA did not monitor specific communications channels solely to acquire their messages is of little comfort.

In general, NSA's surveillance of Americans was in response to requests from other Government agencies. Internal NSA directives now forbid the targeting of American citizens' communications. Nonetheless, NSA may still acquire communications of American citizens as part of its foreign intelligence mission, and information derived from these intercepted messages may be used to satisfy foreign intelligence requirements.

NSA's current surveillance capabilities and past surveillance practices were both examined in our investigation. The Committee recog-

[1] See the Committee's Foreign Intelligence Report for an overview of NSA's legal authority, organization and functions, and size and capabilities.

[2] Since the NSA programs involving American citizens have never been challenged in court, the necessity of obtaining a warrant has not yet been determined. Although there have been court cases that involved NSA intercepts, NSA's activities have never been disclosed in open court. See pp. 765–766 of this Report and the Committee's Report on Warrantless FBI Electronic Surveillance for a discussion of warrant requirements for electronic surveillance.

[3] Between 1970 and 1973, NSA intercepted telephone calls between the United States and various locations in South America to aid the BNDD (now the Drug Enforcement Administration) in executing its responsibilitiees. See pp. 752–756.

nizes that NSA's vast technological capability is a sensitive national asset which ought to be zealously protected for its value to our common defense. If not properly controlled, however, this same technological capability could be turned against the American people, at great cost to liberty. This concern is compounded by the knowledge that the proportion of telephone calls and telegrams being sent through the air is still increasing.

In addition to reviewing facts and issues relating to electronic surveillance, the Committee also examined certain questionable activities of the NSA's Office of Security. See pp. 777–783.

A. NSA's Origins and Official Responsibilities

NSA does not have a statutory charter; its operational responsibilities are set forth exclusively in executive directives first issued in the 1950s. One of the questions which the Senate asked the Committee to consider was the "need for specific legislative authority to govern the operations of . . . the National Security Agency." [4]

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 Americans' international communications for foreign intelligence purposes.[5]

1. Origins

NSA was established in 1952 by a Top Secret directive issued by President Truman.[6] Under this directive, NSA assumed the responsibilities of the Armed Forces Security Agency, which had been created after World War II to integrate American cryptologic efforts.[7] These efforts had expanded rapidly after World War II as a result of the demonstrated wartime value of breaking enemy codes, particularly those of the Japanese.

2. Responsibilities

(*a*) *Subject Matter Responsibilities.*—The executive branch expects NSA to collect political, economic, and military information as part of its "foreign intelligence" mission.[8] "Foreign intelligence" is an ambiguous term. Its meaning changes, depending upon the pre-

---

[4] Senate Resolution 21, Section 2(8).

[5] Roy Banner deposition, 2/4/76, pp. 13, 16, 39.

Banner stated that signals intelligence activities are authorized by the President under Article II of the Constitution and "the Fourth Amendment does not restrict these signals intelligence activities" if the "purpose is solely to obtain foreign intelligence." (*Ibid.*, p. 39.)

[6] Memorandum from President Harry S. Truman to Secretary of State and Secretary of Defense, "Communications Intelligence Activities," 10/24/52.

[7] NSA exercises technical control over the three Service Cryptologic Agencies: the Army Security Agency, Naval Security Group Command, and Air Force Security Service. NSA's Director is always a military officer of at least three-star rank. He reports to the Secretary of Defense, but responds to requests from other intelligence agencies for intelligence information.

[8] "The purpose [of forming NSA] was to maintain and improve this source of intelligence which was considered of vital importance to the national security, to our ability to wage war, and to the conduct of foreign affairs. This mission of NSA is directed to *foreign intelligence*, obtained from foreign electrical communications and also from other foreign signals such as radars." [Emphasis added.] Lew Allen, Jr. testimony, 10/29/75, Hearings, Vol. 5, p. 6.

vailing needs and views of policymakers, and the current world situation. The internal politics of a nation also play a role in setting requirements for foreign intelligence; the domestic economic situation, an upcoming political campaign, and internal unrest can all affect the kind of foreign intelligence that a political leader desires. Thus, the definition constantly expands and contracts to satisfy the changing needs of American policymakers for information. This flexibility was illustrated in the late 1960s, when NSA and other intelligence agencies were asked to produce "foreign intelligence" on domestic activists in the wake of major civil disturbances and increasing antiwar activities.

NSA's authority to collect foreign intelligence is derived from a Top Secret National Security Council directive which is implemented by directives issued by the Director of Central Intelligence.[9] These directives give NSA the responsibility for "Signals Intelligence" (SIGINT) and "Communications Security" (COMSEC). SIGINT is subdivided into "Communications Intelligence" (COMINT) and "Electronics Intelligence" (ELINT). COMINT entails the interception of foreign communications and ELINT involves the interception of electronic signals from radars, missiles, and the like. The COMSEC mission includes the protection of United States Government communications by providing the means for enciphering messages and by establishing procedures for maintaining the security of equipment used to transmit them.

NSA's interception of communications—the area on which the Committee focused—arises under the COMINT program. The controlling NSCID defines COMINT in broad terms as "technical and intelligence information derived from foreign communications by other than the intended recipients."[10] The same NSC directive also states that COMINT "shall not include (a) any intercept and processing of unencrypted written communications, press and propaganda broadcasts, or censorship."[11]

The specific exclusion of unencrypted *written* communications from NSA's mandate would appear to prohibit NSA's interception of telegrams. NSA contends that this exclusion is and always has been limited to mail and communications other than those sent electronically.[12]

---

[9] These are referred to as NSCIDs (National Security Council Intelligence Directives) and DCIDs (Director of Central Intelligence Directives).

[10] The effect of the "other than intended recipients" language is to make clear that the communication is intercepted by someone other than a party to the communication—in this case, the Government.

[11] The relevant DCID contains the same definition. The exclusion is the same, except that after "communications" the words "except written plaintext versions of communications which have been encrypted or are intended for subsequent encryption" have been added.

[12] Banner disposition, 2/4/76, p. 71.

The "written communications exclusion was added in 1958; the CIA's New York mail opening project had been underway since the early 1950s. See the Committee's Report on CIA and FBI Mail Opening Programs. The exclusion of "press and propaganda broadcasts" may reflect the fact that CIA had been granted responsibility for intercepting, analyzing, and disseminating such foreign press broadcasts under its Foreign Broadcast Information Service (FBIS) program. In support of NSA's contention that "unencrypted written communications" refers to mail, it might be argued that the exclusion was designed to ensure that NSA would not engage in mail opening, which was under the CIA's jurisdiction.

The same NSCID which discusses foreign communications also states that NSA is to produce intelligence "in accordance with objectives, requirements, and priorities established by the Director of Central Intelligence with the advice of the United States Intelligence Board." USIB was composed of representatives from the FBI, CIA, Treasury Department, Energy Research and Development Administration, State Department, and Defense Department.[13] Since 1966, NSA annually received general requirements from USIB for the collection of foreign intelligence. These requirements ordinarily identified broad areas of interest, such as combating international terrorism, and were supplemented by more specific "amplifying requirements" periodically submitted to NSA by other USIB members.

(*b*) *Geographic Responsibilities.*—Although none of the applicable executive directives explicitly prohibit NSA from intercepting communications which occur wholly within the United States, internal NSA policy has always prohibited such interceptions. In practice, NSA limits itself to communications where at least one of the terminals is in a foreign country. This means that when Americans use a telephone or other communications link between this country and overseas, their words may be intercepted by NSA.

(*c*) *Jurisdiction with Respect to Nationality.*—Although the controlling NSCID contains no limitation relating to the citizenship of persons whose "foreign communications" may be intercepted, the relevant DCID does exclude messages "exchanged among private organizations and nationals, acting in a private capacity, of the U.S." This restriction is designed to prevent NSA from processing communcations between two Americans, regardless of their location.

In the late 1960s and early 1970s, however, NSA did intercept and disseminate some messages exchanged between two Americans where one of the terminals was foreign. NSA does not now knowingly process or disseminate messages where both the sender and recipient are American citizens, groups, or organizations.

B. Summary of Interception Programs

The Committee's hearings disclosed three NSA interception programs: the "watch lists" containing names of American citizens; "Operation SHAMROCK," whereby NSA received copies of millions of telegrams leaving or transiting the United States; and the monitoring of certain telephone links between the United States and South America at the request of the Bureau of Narcotics and Dangerous Drugs. In addition, the Committee's investigation revealed that although NSA no longer includes the names of specific citizens in its selection criteria, it still intercepts international communications of Americans as part of its foreign intelligence collection activity. Information derived from such communications is disseminated by NSA to other intelligence agencies to satisfy foreign intelligence requirements.

---

[13] USIB was formally abolished by Presidential directive of February 18, 1976. No comparable group was established to replace it, but the directive authorized the Director of Central Intelligence to create such a body.

1. Watch Lists Containing Names of Americans

From the early 1960s until 1973, NSA intercepted and disseminated international communications of selected American citizens and groups on the basis of lists of names supplied by other Government agencies. In 1967, as part of a general concern within the intelligence community over civil disturbances and peace demonstrations, NSA responded to Defense Department requests by expanding its watch list program. Watch lists came to include the names of individuals, groups, and organizations involved in domestic antiwar and civil rights activities in an attempt to discover if there was "foreign influence" on them.[14]

In 1969, NSA formalized the watch list program under the codename MINARET. The program applied not only to alleged foreign influence on domestic dissent, but also to American groups and individuals whose activities "may result in civil disturbances or otherwise subvert the national security of the U.S." [15] At the same time, NSA instructed its personnel to "restrict the knowledge" that NSA was collecting such information and to keep its name off the disseminated "product." [16]

Prior to 1973, NSA generally relied on the agencies requesting information to determine the propriety and legality of their actions in submitting names to NSA.[17] NSA's new director, General Lew Allen, Jr., indicated some concern about Project MINARET in August 1973, and suspended the dissemination of messages under the program. In September 1973, Allen wrote the agencies involved in the watch lists, requesting a recertification of their requirements, particularly as to the appropriateness of their requests.

In October 1973, Assistant Attorney General Henry Petersen and Attorney General Elliot Richardson concluded that the watch lists were of "questionable legality" and so advised NSA.[18] In response, NSA took the position that although specific names had been targeted, the communications of particular Americans included on the watch lists had been collected "as an incidental and unintended act in the conduct of the interception of foreign communications." Allen concluded:

> [NSA's] current practice conforms with your guidance that "relevant information acquired [by NSA] in the routine pur-

---

[14] Although the agencies submitting names to NSA were members of the United States Intelligence Board, USIB never approved a watch list requirement on civil disturbances, or discussed the monitoring of American citizens' communications.

[15] MINARET Charter, 7/1/69, Hearings, Vol. 5, Exhibit No. 3, pp. 149–150.

[16] *Ibid.*

[17] Allen, 10/29/75, Hearings, Vol. 5, pp. 31–32.

[18] Letter from Elliot Richardson to Lew Allen, Jr., 10/1/73, Hearings, Vol. 5, Exhibit No. 7, pp. 160–161.

Petersen reported to Richardson that he had discovered the watch list program ("of which we had no previous knowledge") as a result of inquiries made to the FBI and other intelligence agencies with respect to possible electronic surveillance undertaken by such agencies in connection with a criminal prosecution. In one case in which NSA reported that it had conducted such surveillance, the Government elected to drop the prosecution. See pp. 757–758, 761. Memorandum from Henry Petersen to Elliot Richardson, 9/4/73.

suit of the collection of foreign intelligence information may continue to be furnished to appropriate government agencies.[19]

2. Obtaining Copies of Messages from International Telegraph Companies: Operation SHAMROCK

From August 1945 until May 1975, NSA received copies of millions of international telegrams sent to, from, or transiting the United States. Codenamed Operation SHAMROCK, this was the largest governmental interception program affecting Americans, dwarfing CIA's mail opening program by comparison. Of the messages provided to NSA by the three major international telegraph companies, it is estimated that in later years approximately 150,000 per month were reviewed by NSA analysts.

NSA states that the original purpose of the program was to obtain the enciphered telegrams of certain foreign targets. Nevertheless, NSA had access to virtually all the international telegrams of Americans carried by RCA Global and ITT World Communications.[20] Once obtained, these telegrams were available for analysis and dissemination according to NSA's selection criteria, which included the watch lists.

The SHAMROCK program began in August 1945, when representatives of the Army Signals Security Agency approached the commercial telegraph companies to seek post-war access to foreign governmental traffic passing over the facilities of the companies. Despite advice from their attorneys that the contemplated intercept operation would be illegal in peacetime, the companies agreed to participate, provided they received the personal assurance of the Attorney General of the United States that he would protect them from suit, and that efforts be immediately undertaken to legalize the intercept operation. Apparently these assurances were forthcoming, because the intercept program began shortly thereafter.[20a]

In 1947, representatives of the companies met with Secretary of Defense Forrestal to discuss their continued participation in SHAMROCK. Forrestal told them that the program was "in the highest interests of national security" and urged them to continue.[21] The companies were told that President Truman and Attorney General Tom C. Clark approved and that they would not suffer criminal liability, at least while the current Administration was in office. Those assurances were renewed in 1949, when it was again emphasized that future administrations could not be bound. There is no evidence that the companies ever sought such assurances again.

---

[19] Letter from Lew Allen, Jr. to Elliot Richardson, 10/4/73, Hearings, Vol. 5, Exhibit No. 8, pp. 162–163.

[20] Western Union International provided NSA only with copies of the messages of the foreign targets, except for messages to one country, where it provided everything.

[20a] A letter, dated August 24, 1945, from the Army officer responsible for making the arrangements with the companies states that ITT would begin participation in SHAMROCK the last week in August. Another letter, dated October 9, 1945, from RCA to the Army states that it would begin participation immediately. See pp. 768–769.

[21] Testimony of Robert Andrews, Special Assistant to the General Counsel, Department of Defense, 9/23/75, p. 34.

Throughout the operation NSA never informed the companies that it was analyzing and disseminating telegrams of Americans. Yet the companies, who had feared in 1945 that their conduct might be illegal, apparently never sought assurances that NSA was limiting its use to the messages of the foreign targets once the intercept program had begun.

3. Monitoring of South American Links for Drug Traffic Control Purposes

From 1970 to 1973, at the request of the Bureau of Narcotics and Dangerous Drugs, NSA monitored selected telephone circuits between the United States and certain countries in South America to obtain information relating to drug trafficking.

The BNDD was initially concerned about drug deals that were being arranged in calls to a South American city from public telephone booths in New York City. The Bureau determined that it could not legally tap the public telephones and enlisted NSA's help to monitor international communications links that carried these telephone calls. Thus, instead of intercepting calls from a few telephone booths, as the BNDD would have done with a wiretap, NSA had access to international calls placed from, or received in, cities all over the United States that were switched through New York.[22]

In addition, BNDD submitted the names of 450 Americans to NSA for a "drug" watch list. This list resulted in the dissemination of about 1,900 reports on drug traffickers to BNDD and CIA.

The CIA began to assist NSA's monitoring effort in late 1972, but later determined that the program served a law enforcement function and terminated its participation in February 1973.[23] NSA was affected by the CIA decision, as it had come to view this program as possibly serving a law enforcement function and thus beyond the scope of its proper mission. NSA terminated this activity in June 1973, but continued to monitor some of the *same* United States-South American links for foreign intelligence purposes until July 1975.

4. "Incidental" Intercepts of Americans' Communications

Although NSA does not *now* target communications of American citizens, groups, or organizations for interception by placing their names on watch lists, other selection criteria are used which result in NSA's reviewing many communications to, from, or about an American. The initial interception of a stream of communications is analogous to a vacuum cleaner: NSA picks up all communications carried over a specific link that it is monitoring. The combination of this technology and the use of words to select communications of interest results in NSA analysts reviewing the international messages of American citizens, groups, and organizations for foreign intelligence.

The interception and subsequent processing of communications are conducted in a manner that minimizes the number of unwanted mes-

---

[22] According to the International Telephone and Telegraph Company, calls from American cities to South America are routinely switched through New York.

[23] CIA's participation in this activity violated provisions of its charter, the National Security Act of 1947, which prohibit the Agency from exercising law enforcement powers. NSA does not have a charter prohibiting such activity, but recognizes that it has no law enforcement function.

sages. Only after an analyst determines that the content of a message meets a legitimate requirement will it be disseminated to the interested intelligence agencies. In practically all cases, the name of an American citizen, group, or organization is deleted by NSA before a message is disseminated.

Internal NSA guidelines ensure that the decision to disseminate an intercepted communication is now made on the basis of the importance of the foreign intelligence it contains, not because a United States citizen, group, or organization is involved. This procedure is, of course, subject to change by internal NSA directives.

In short, NSA's pursuit of international communications does result in the incidental interception and dissemination of communications which the American sender or receiver expected to be kept private. This issue of the latitude NSA should be given in disseminating incidental intercepts must be dealt with if we are to resolve the dilemma between the need for effective foreign intelligence and the need to protect the rights of American citizens.[24]

C. Issues and Questions

Pursuant to its mandate, the Committee has studied whether NSA's jurisdiction and operations should be governed and controlled by a legislative charter. The facts discovered by the Committee with respect to NSA's programs and capabilities suggest that the following questions should be posed for legislative resolution:

1. Should NSA, which like the CIA has vast powers intended for "foreign" purposes, be barred from using those powers domestically?
2. Should NSA, like the CIA, be prohibited from exercising "law enforcement powers" or "internal security functions"?
3. Should NSA be permitted specifically to target the international communications of Americans? If so, for what purposes and should a warrant be required?
4. Should NSA be permitted to disseminate information derived from the "incidental" interception of Americans' mes-

[24] The establishment of guidelines relating directly to this issue poses an ongoing problem. Some may argue that NSA's current policy to disguise the identity of an American corporation in a communication is misguided. It could be held that, in the case of companies, their right to privacy does not extend as far as with individual citizens. For example, if an intercepted communication indicates that an American company executive is negotiating with a foreign government for the sale of large quantities of a crucial material, should the Federal Government be entitled to know the identity of the company? If NSA discovered that an American firm is exporting material to a foreign country that is prohibited by law, should the Government be allowed to know the name of that company? Or, does NSA violate the Fourth Amendment rights which protect Americans from unreasonable searches and seizures by disseminating such messages without deleting the names? Should special procedures be instituted—such as approval of the Attorney General or acquisition of a warrant—before messages containing U.S. names can be disseminated?

A discussion of these issues of interception and dissemination occurred in an open session of the Committee between Attorney General Edward H. Levi and Professor Philip B. Heymann. Levi supported the dissemination by NSA of incidentally intercepted foreign intelligence information involving Americans without a warrant; Heymann maintained that dissemination should require a warrant. See Edward H. Levi and Philip B. Heymann testimonies, 11/6/75, Hearings, Vol. 5, pp. 66–143.

sages obtained by monitoring an international communications link for foreign intelligence purposes? If so, to whom, for what use, and under what controls?

II. NSA'S MONITORING OF INTERNATIONAL COMMUNICATIONS

A. Summary of the Watch List Activity

Lists of words and phrases, including the names of individuals and groups, have long been used by the National Security Agency to select information of intelligence value from intercepted communications. These lists are referred to as "watch lists" by NSA and the agencies requesting intelligence information from them, such as the Federal Bureau of Investigation, Central Intelligence Agency, Bureau of Narcotics and Dangerous Drugs, Secret Service, and Department of Defense. The great majority of names on watch lists have always been foreign citizens and organizations.

The Committee examined two types of watch lists which included Americans. One focused on domestic civil disturbances, the other on drug trafficking. Messages selected on the basis of these watch lists were analyzed and forwarded to other Federal agencies, including the FBI, CIA, BNDD, and DOD. The Secret Service also received information from NSA regarding potential threats to persons under its protection.

Between 1967 and 1973, NSA received watch lists from these agencies which included the names of Americans as well as foreign citizens and organizations. These lists were used to select messages from intercepted traffic and to discover whether there was foreign influence on, or support of, domestic antiwar and civil rights activities. From 1970 until 1973, similar lists were used to gather intelligence on international drug traffic.

NSA itself added names to the watch lists to enhance the selection criteria used to support the requirements levied by other agencies.[25] NSA's Office of Security also added names to the lists for counterintelligence and counterespionage purposes.[26]

Between 1969 and 1973, NSA disseminated approximately 2,000 reports (e.g., the text or summaries of intercepted messages) to the various requesting agencies as a result of the inclusion of American names on the watch lists.[27] No evidence was found, however, of any significant foreign support or control of domstic dissidents.

---

[25] General Lew Allen, Jr. said this process "was a matter of adding aliases . . . of adding addresses in some cases where an organization had been specified, and it would assist picking up messages of that organization, the names of officials of the organizations [were thus] added to enhance the selection process." Allen, 10/29/75, Hearings, Vol. 5, p. 27.

Another NSA official later advised the Committee that names were added by NSA in its amplification of watch lists and that this "was usually done either by adding the name of an executive officer of an organization, or by adding the organization name associated with a person who was placed on the watch list by another agency." (Letter from NSA to Senate Select Committee, 11/6/75.)

[26] NSA response to Senate Select Committee interrogatories, 8/22/75, pp. 3–6. (Cited hereinafter as NSA Response, 8/22/75.) See pp. 781–782.

[27] The material collected between 1967 and the fall of 1969 was destroyed by NSA which only retains documents less than five years old. The approximately 2,000 reports are only for the post-1969 period.

Information generated by the watch list activity was the product of collection conducted against channels of international communications ("links") with at least one terminal in a foreign country. Nevertheless, the messages NSA intercepted and disseminated were sometimes between two American citizens, one in the United States and one abroad. With one exception, NSA intercepted messages only from "links" it was already monitoring as part of its foreign intelligence mission.

This exception occurred in 1970, when the Bureau of Narcotics and Dangerous Drugs asked NSA to provide intelligence on international drug trafficking. NSA began to monitor certain international communications links between the United States and South America to acquire intelligence on drugs entering the United States. The BNDD also supplied NSA with the names of Americans suspected of drug trafficking for inclusion on a watch list. Reports on drug-related activities of American citizens were disseminated to both the BNDD and CIA.

Both the drug and "nondrug" watch lists of United States citizens were discontinued in 1973 as a result of questions concerning their legality and propriety, raised by the Justice Department and by NSA itself.

B. History

1. Early Period: 1960–1967

The exact details of the origin of the watch list activity are unclear. Testimony from NSA employees indicates that the early 1960s marked the beginning of watch lists and the inclusion of names of American citizens. According to a senior NSA official, "the term watch list had to do with a list of names of people, places or events that a customer would ask us to have our analysts keep in mind as they scan large volumes of material." [28]

Originally these lists were used for two purposes: (1) monitoring travel to Cuba and other communist countries; and (2) protecting the President and other high Government officials. According to NSA, neither of these tasks involved a regular program for including American names on the lists: requests from other agencies were infrequent and generally *ad hoc*.[29] Prior to 1962, NSA did not have an office specifically in charge of interagency dealings, which also limited the number of requests for information from other agencies.

In the early 1960s requesting agencies, usually the FBI, submitted names of United States citizens and business firms having dealings with Cuba to NSA. In turn, NSA provided the FBI with intelligence on American commercial and personal communications with Cuba. A May 18, 1962, internal FBI memorandum from Raymond Wannall, Chief of the Nationalities Intelligence Section of the Domestic Intelligence Division, to Assistant Director William Sullivan reported on a meeting with NSA officials concerning Cuba. The purpose of the meeting was to devise a way for the FBI to make better use of NSA intercepts relating to "commercial and personal communications be-

[28] Senior NSA official No. 1 testimony, 9/16/75, p. 47.
[29] *Ibid.*, pp. 47–49; senior NSA official No. 2 testimony, 9/18/75, p. 13.

tween persons in Cuba and in the United States." [30] The memorandum stated:

> of the raw traffic now available, the material which would be most helpful to us would consist of periodic listing of firms in the U.S. which are doing business with individuals in Cuba and the Cuban government. . . . With regard to personal messages, we feel that those relating to individuals travelling between Cuba and the U.S. would be the most significant. . . . *We will furnish NSA a list of persons in whom we have an investigative or an intelligence interest.* [Emphasis added.][31]

The second area of concern in the early 1960s was protection of the President. According to NSA, the Secret Service submitted the names of the Presidents and others under its protection, possibly as early as 1962.[32] This activity, however, was not instituted for the purpose of acquiring the communications of the protectees, but to determine possible threats to their well-being. After President Kennedy was assassinated in November 1963, interest in presidential protection naturally intensified, and NSA's joint efforts with the Secret Service were expanded.

This early activity was not directed against American citizens; no intelligence program called for the systematic inclusion of American citizens on a watch list. The evidence indicates, however, that NSA did intentionally monitor certain international activities of some American citizens as early as 1962. These objectives, which began as legitimate concerns for the life of the President, expanded when the watch list activity intensified in 1967.

2. Systematic Inclusion of American Names: 1967

The major watch list effort against American citizens began in the fall of 1967. In response to pressures from the White House, FBI, and Attorney General, the Department of the Army established a civil disturbance unit. An area of special interest was possible foreign involvement in American civil rights and antiwar groups. General William Yarborough, the Army Assistant Chief of Staff for Intelligence (ACSI), directed the operations of this unit.[33]

---

[30] Memorandum from Raymond Wannall to William Sullivan, 5/18/62.

[31] *Ibid.*

Wannall testified that names were, in fact, sent to NSA by the FBI in the early 1960s. Raymond Wannall testimony, 10/3/75, p. 18.

[32] NSA Response 8/22/75, p. 12.

[33] William Yarborough testimony, 9/10/75, p. 8.

"*Question:* Did you ever have the feeling that these instructions were coming from the President or somebody else in the White House?

"General YARBOROUGH: There was a lot of evidence to indicate that the President was deeply interested, as were the Attorney General and the Director of the FBI. There was a great deal of public interest. In other words, the interest was not just within the military at all.

"*Question:* But you don't have any evidence or knowledge of a direct order from the President to the Secretary of Defense with regard to setting up a civil disturbance unit within the Department of the Army?

"General YARBOROUGH: I would not have a way to know about that direct relationship unless I found it out by chance. I did not know.

A complete examination of the U.S. military's participation in collecting intelligence on domestic dissidents is contained in the Committee's Report: "Improper Surveillance of Private Citizens by the Military."

On October 20, 1967, Yarborough sent a message to the Director of NSA, General Marshall Carter, requesting that NSA provide any available information concerning possible foreign influence on civil disturbances in the United States. Yarborough specifically asked for "any information on a continuing basis" concerning:

> A. Indications that foreign governments or individuals or organizations acting as agents of foreign governments are controlling or attempting to control or influence the activities of U.S. "peace" groups and "Black Power" organizations.
>
> B. Identities of foreign agencies exerting control or influence on U.S. organizations.
>
> C. Identities of individuals and organizations in U.S. in contact with agents of foreign governments.
>
> D. Instructions or advice being given to U.S. groups by agents of foreign governments.[34]

A senior NSA official knowledgeable in this area testified that such a request for information on civil disturbances or political activities was "unprecedented. . . . It is kind of a landmark in my memory; it stands out as a first." [35] The initial request was also vague; it did not discuss the targeting of American citizens, or what specific organizations or groups were of interest. The Army was "interested in determining whether or not there is evidence of any foreign action to develop or control these anti-Vietnam and other domestic demonstrations." [36]

The following day, Carter sent a cable to Yarborough, Director of Central Intelligence Richard Helms, and each member of the United States Intelligence Board, informing them that NSA was "concentrating additional and continuing effort to obtain SIGINT" in support of the Army request.[37] Although USIB members were notified of this new requirement, there is no record of discussion at USIB meetings of the watch list, nor did USIB ever validate a requirement for monitoring in support of the civil disturbance unit.[38]

Watch list names were submitted directly to NSA by the FBI, Secret Service, Defense Intelligence Agency, the military services, and the CIA. These same agencies received reports of intercepted communications pertaining to their areas of interest. The State Department also received some reports on international terrorism and drug activities, but it is unclear whether they submitted any American names.[39]

Between 1967 and 1973, a cumulative total of about 1,200 American names appeared on the civil disturbance watch list. The FBI submitted the largest proportion, approximately 950. The Secret Serv-

---

[34] Cable from Yarborough to Carter, 10/20/67, Hearings, Vol. 5, Exhibit No. 1, pp. 145–146.

[35] Senior official No. 1, 9/16/75, pp. 57, 54.

[36] Cable from Yarborough to Carter, 10/20/67; Hearings, Vol. 5, Exhibit No. 1, pp. 145–146.

[37] Cable from Carter to Yarborough, 10/21/67, Hearings, Vol. 5, Exhibit No. 2, pp. 147–148.

[38] Allen, 10/29/75, Hearings, Vol. 5, p. 28.

[39] Senior NSA official No. 1, 9/16/75, p. 76.

ice's list included about 180 American individuals and groups active in civil rights and antiwar activities. The DIA submitted the names of 20 American citizens who traveled to North Vietnam, and the CIA submitted approximately 30 names of alleged American radicals. The Air Force Office of Special Investigations, the Naval Investigative Service, and the Army Assistant Chief of Staff for Intelligence all submitted a small number of names to NSA. In addition, NSA contributed about 50–75 names to support the watch list activity.

At its height in early 1973, there were 600 American names and 6,000 foreign names on the watch lists.[40] According to NSA, these lists produced about 2,000 reports that were disseminated to other agencies between 1967 and 1973. NSA estimates 10 percent of these reports were derived from communications between two American citizens.[41]

3. Increasing Security and Concealment of Programs Involving American Citizens

The watch list activity was always a highly sensitive, compartmented operation.[42] The secrecy was not due to the nature of the communications intercepted (most were personal and innocuous) but to the fact that American citizens were involved. NSA requested that some of the agencies receiving watch list product either destroy the material or return it within two weeks.[43] This procedure was not followed with even the most sensitive of NSA's legitimate foreign intelligence product.

When NSA intercepts, analyzes, and disseminates a foreign communication, the regular procedure is for the communication to be classified, given a serial number, and filed. From 1967–1969, much of the watch list material was treated in this manner, and given the same classification as the most sensitive NSA intercepts. As a senior NSA official testified:

> During the 1967–1969 period, communications that had a U.S. citizen on one end and a foreigner on the other were given [a high level security classification] . . . and went out as serialized product, through a limited by name only distribution.[44]

Other material was even more highly classified. Whenever communications between *two* Americans were intercepted, they were classified Top Secret, prepared with no mention of NSA as the source, and disseminated "For Background Use Only." [45] No serial number was assigned to them, and they were not filed with regular communications

---

[40] Allen, 10/29/75, Hearings, Vol. 5, p. 12.

[41] Ibid.

[42] In an effort to prevent disclosure of the program, NSA "compartmented" the activity by restricting the number of officials within the agencies who had access to the material. General Allen stated: "in my judgment the controls which were placed on the handling of the intelligence were so restrictive that the value was significantly diminished." Allen, 10/29/75, Hearings, Vol. 5, p. 13.

[43] Staff summaries of Michael Mastrovito (Secret Service) interview, 10/17/75; and of Philip Smith and Gerald Strickler (Drug Enforcement Administration) interviews, 10/7/75.

[44] Senior NSA official No. 2, 9/18/75, pp. 39–40.

[45] *Ibid.*, p. 40.

intelligence intercepts. This effectively limited access to the material and prevented its use in any official study or report. As Benson Buffham, Deputy Director of NSA, testified:

> first it is true that we maintain permanent type records of all of our product. However, it is my understanding that this material was dealt with separately. It was not serialized and put out in regular distribution lists. These items were produced as display items, show-to items and thus the normal procedures that would be followed for our serialized product were not followed. So as best as I know, there would not be any record of this material held in other places within the Agency in the permanent files.[46]

The project's sensitivity was due to a number of factors. The requirements—protection of the President, terrorism, civil disturbances, drug activities—involved sensitive subjects. NSA also wanted to ensure protection of the SIGINT source and of other intercept operations, which could be jeopardized by unauthorized release of the watch list material.[47] Finally, American citizens, firms, and groups were involved, and this was "different from the normal mission of the National Security Agency." [48]

The fact that NSA did not serialize and file the intercepted communications between Americans indicates they did not view this activity as part of their "normal" mission. Buffham stated that he believed the interception and dissemination of communications between American citizens to be outside NSA's mission, as defined in applicable executive directives.[49]

4. Project MINARET: Further Expansion and Increased Secrecy

The civil disturbance watch list program became even more compartmented in July 1969, when NSA issued a charter to establish Project MINARET.

MINARET established more stringent controls over the information collected on American citizens and groups involved in civil disturbances. To enhance security, MINARET effectively classified all of this information as Top Secret, "For Background Use Only," and stipulated that the material was *not* to be serialized or identified with the National Security Agency. Prior to 1969, only communications *between two Americans* were classified in this manner; with the adoption of MINARET, communications to, from, or mentioning United States citizens were so classified.

The MINARET charter established tighter security procedures for intercepted messages which contained:

> a. information on foreign governments, organizations, or individuals who are attempting to influence, coordinate or control U.S. organizations or individuals who may foment civil disturbance or otherwise undermine the national security of the U.S.;

---

[46] Benson Buffham testimony, 9/12/75, p. 34.
[47] Senior NSA official No. 1, 9/16/75, p. 69.
[48] Senior NSA official No. 2, 9/18/75, p. 38.
[49] Buffham, 9/12/75, p. 73.

b. information on U.S. organizations or individuals who are engaged in activities which may result in civil disturbances or otherwise subvert the national security of the U.S. *An equally important aspect of MINARET will be to restrict the knowledge that such information is being collected and processed by the National Security Agency.* [Emphasis added.] [50]

This charter was prepared within NSA and issued by an NSA Assistant Director. According to testimony given the Committee, the charter was discussed with NSA Deputy Director Louis Tordella and probably with the Director, but other agencies involved in the watch list activity were not informed of the new procedures until the charter had been adopted.[51]

In addition to regulating the distribution and format of watch list product, MINARET also initiated a more formal procedure for submission of names. No longer were names accepted over the telephone or by word of mouth.[52] According to NSA, the watch list "was handled less systematically prior to 1969 . . . some watch lists entered NSA during that time via direct channels, including secure telephone." [53] NSA maintains, however, that the regular procedure was for agencies submitting names by secure telephone or in person to confirm them with written requests. A senior NSA official testified: "From 1969 on [the watch list] was handled in a very careful, reviewed and systematic way." [54]

The MINARET charter was an effort both to restrict knowledge of the watch list program and to disguise NSA's participation in it. NSA maintains that its concern for the security of SIGINT sources, i.e., NSA's intercept operations, was the primary reason for initiating these measures.[55] NSA further maintains that it was concerned with the privacy of U.S. communications and, by imposing the MINARET restrictions, sought to ensure that dissemination was made exclusively to those outside NSA who had a legitimate need for the information. It is apparent that the MINARET restrictions also protected NSA's role from exposure. Dissemination of foreign communications to domestic agencies was obviously a sensitive matter. It involved considerable risk of exposure which would increase if the number of people within the intelligence community who were aware of the activity grew. Therefore, NSA placed more restrictive security controls on MINARET material than it placed on other highly classified foreign intercepts in order to conceal its involvement in activities which were beyond its regular mission.

C. Types of Names on Watch Lists

The names of Americans submitted to NSA for the watch lists ranged from members of radical political groups, to celebrities, to

---

[50] MINARET Charter, 7/1/69. Hearings, Vol. 5, Exhibit No. 3, pp. 149–150.
[51] Buffham, 9/12/75, pp. 50, 49; senior NSA official No. 1, 9/16/75, p. 68.
[52] Senior NSA official No. 9/16/75, p. 78.
[53] NSA Response, 8/22/75, p. 12.
In this written response, NSA confirmed reports the Committee had received from other agencies that prior to 1969 watch list requests were occasionally communicated to NSA by telephone or in person. See Mastrovito (staff summary), 10/17/75; Wannall, 10/3/75, p. 32; Smith and Strickler (staff summary), 10/7/75.
[54] Senior NSA official No. 2, 9/18/75, p. 19.
[55] Senior NSA official No. 1, 9/16/75, p. 69.

ordinary citizens involved in protests against their Government. Names of organizations were also included; some were communist-front groups, others were nonviolent and peaceful in nature.

The use of names, particularly those of groups and organizations, to select international communications results in NSA unnecessarily reviewing many messages. There is a multiplier effect: if an organization is targeted, all its member's communications may be intercepted; if an individual is on the watch list, all communications to, from, or mentioning that individual may be intercepted. These communications may also contain the names of other "innocent" parties. For example, a communication mentioning the wife of a U.S. Senator was intercepted by NSA, as were communications discussing a peace concert, a correspondent's report from Southeast Asia to his magazine in New York, and a pro-Vietnam war activist's invitations to speakers for a rally. According to testimony before the Committee, the material that resulted from the watch lists was not very valuable; most communications were of a private and personal nature, or involved rallies and demonstrations that were public knowledge.[56]

D. Overlapping Nature of Intelligence Community Requests

As noted above, the primary purpose of the watch lists on Americans from 1967–1973 was to collect intelligence on civil disturbances. NSA also responded to a requirement from BNDD to monitor for illegal drug trafficking from 1970–1973. In addition, NSA supplied information to Federal agencies (FBI, CIA, Secret Service, and Department of Defense) on possible terrorist activity, and disseminated reports to the Secret Service which related to the protection of the President. The demarcations between these categories, however, was not always clear.

Secret Service officials, for example, have told the Committee that presidential and executive protection includes "providing a secure environment" for the White House for foreign embassies within the United States and in areas where high Government officials travel. According to the Secret Service, this requires "information regarding civil disturbances and anti-American or anti-U.S. Government demonstrations in the U.S. or overseas, as these demonstrations may affect the Secret Service's mission of protecting U.S. and foreign officials." [57] After the October 20, 1967, Yarborough cable, the Secret Service began submitting names of individuals and organizations active in the anti-war and civil rights movements to NSA. Although these individuals and groups were not considered a direct threat to protectees, it was believed they might participate in demonstrations against United States policy which would endanger the physical well-being of Government officials.[58] Intercepted communications to, from, or mentioning these individuals and groups were always disseminated by NSA to the Secret Service and the CIA, and often to the FBI.

---

[56] Wannall, 10/3/75, p. 13. He stated: "the feeling is that there was very little in the way of good product as a result of our having supplied names to NSA."

General Allen, however, told the Committee in public session: "we are aware that a major terrorist act in the U.S. was prevented. In addition, some large drug shipments were prevented from entering the U.S. because of our efforts on international narcotics trafficking." Allen, 10/29/75, Hearings, Vol. 5, pp. 12–13.

[57] NSA response, 8/22/75.

[57] Secret Service response to Senate Select Committee. 10/12/75.

There was considerable overlap among various agencies in submissions for watch list coverage and requests for material. For example, the CIA was interested in:

> *The activities of U.S. individuals involved in either civil disorders, radical student or youth activities, racial militant activities, radical antiwar activities, draft evasion/deserter support activities, or in radical related media activities, where such individuals have some foreign connection* by virtue of: foreign residence, foreign travel, attendance at international conferences or meetings and/or involvement or contact with foreign governments, organizations, political parties or individuals; or with Communist front organizations. [Emphasis added.][59]

The FBI was interested in similar kinds of information, as illustrated by excerpts of two memoranda from J. Edgar Hoover to the Director, NSA:

> This is to advise you that this Bureau has a continuing interest in receiving intelligence information obtained under MINARET regarding the targets previously furnished you. . . . Information derived from this coverage has been helpful in determining the extent of international cooperation among New Leftists and has been used for lead purposes.[60]
>
> The purpose of this communication is to advise of general areas of interest to this Bureau in connection with racial extremist matters and to request your assistance in such matters.
>
> *There are both white and black racial extremists in the United States advocating and participating in illegal and violent activities for the purpose of destroying our present form of government. Because of this goal, such racial extremists are natural allies of foreign enemies of the United States.* Both material and propaganda support is being given to United States racial extremists by foreign elements. The Bureau is most interested in all information showing ties between United States racial extremists and such foreign elements. [Emphasis added.] [61]

These requests reflect an underlying similarity of interests among agencies, despite the differing needs which are expressed in their requirements. To some extent the DIA, FBI, CIA, and the Secret Service received information on Black activists and groups, and on the antiwar movement. All were concerned with how civil disturbances and antiwar demonstration were affecting the internal security of the United States. Although their general area of concern was the same, each agency used the information for its own particular purposes. The DIA was interested in travel to North Vietnam; the CIA kept files on alleged antiwar radicals for its Project CHAOS;

---

[59] NSA Response, 8/22/75, p. 17.
[60] Memorandum from J. Edgar Hoover to Director, NSA 6/3/70.
[61] Memorandum from J. Edgar Hoover to Director, NSA, 11/6/70.

the FBI used the information to develop "leads" on new left activists, at the same time it was conducting COINTELPRO efforts against alleged radicals;[62] and the Secret Service was concerned with protecting the President. Despite slight variations in focus, the different agencies' requests reflected the overriding fear that the nation was being undermined internally and externally. It was this perception which produced the watch list program directed against Americans.

E. Drug Watch Lists: United States—South American Intercepts

1. Initial Monitoring: 1970

An unofficial requirement to collect and disseminate international communications concerning drug trafficking was levied on NSA by the Bureau of Narcotics and Dangerous Drugs on April 10, 1970. BNDD Director John Ingersoll sent a memorandum to NSA Director Noel Gayler requesting "any and all COMINT information which reflects illicit traffic in narcotics and dangerous drugs." NSA initiated its monitoring in June 1970, but a general requirement to obtain foreign intelligence on drug trafficking was not validated by the United States Intelligence Board until August 1971.

The Ingersoll memorandum specified that BNDD was interested in individuals and organizations involved in illegal drug activities, information on production centers, and all violations of United States laws pertaining to narcotics and dangerous drugs. In order to assist NSA in fulfilling the requirement, BNDD stated that they would provide NSA lists of individuals and organizations which had a history of involvement with illegal drug activities. According to the Ingersoll memorandum, "this watch list will be updated on a monthly basis and and additions/deletions will be forwarded to NSA."[63]

NSA implemented this request by monitoring international communications traffic. The first intercepts began in June 1970.[64] Telephone traffic carried on circuits between the United States and certain South American cities was first monitored in September 1970. Unlike other watch list monitoring, the United States—South American effort required NSA to devote additional resources to intercepting communications over this specifically targeted link.[65]

This link included the telephone circuits between New York City and a South American city. BNDD was initially concerned about drug deals that were being arranged in calls from public telephone booths

[62] For a detailed discussion of the Bureau's program against the New Left, see the Committee's report on COINTELPRO.

[63] Memorandum from John Ingersoll to Noel Gaylor, 4/10/70, Hearings, Vol. 5, Exhibit No. 4, pp. 153, 154.

[64] NSA was covering links for international traffic prior to and during the drug watch list activity. However, the monitoring of certain United States-South American circuits for telephone traffic was initiated in September *solely* to cover drug traffickers. Senior NSA official No. 2, 9/18/75, pp. 107, 108.

Although NSA collected intelligence from communications intercepted in other areas of the world to support the drug watch list, the Committee's investigation centered on the United States—South American monitoring due to the specific targeting of American citizens.

[65] Senior NSA official No. 2, 9/18/75, p. 99.

in New York City to South America. According to a senior NSA official:

> BNDD had some information that led them to believe that arrangements were being made by telephone from New York City, a Grand Central Station telephone booth, to some individuals in [a South American city].[66]

BNDD felt that it could not legally tap the public telephones and thus enlisted NSA's help to cover the international link that carried these telephone calls. At BNDD's request, NSA began to intercept telephone conversations carried over this link in September 1970. Additional United States—South American links were soon added. BNDD also supplied NSA with code names for drugs and names of individuals, including American citizens.

The telephone monitoring was conducted from one NSA site until December 1970, when that intercept station was closed. An NSA East Coast facility, operated by the military, began monitoring United States—South American links in March 1971. According to NSA, 19 United States—South American links were monitored for voice traffic at the two sites between 1970 and 1973.[67] Six South American cities were of primary interest, in addition to New York and Miami.[68]

During this period, BNDD submitted 450 American names to NSA for inclusion on the drug watch list. At the high point, in early 1973, 250 Americans were on the active list.

Of the calls intercepted at the East Coast site, less than 10 percent were sent to NSA headquarters, and less than 10 percent of these were disseminated.[69] Yet it is clear that many personal and business calls of Americans were reviewed during this operation. This results from the lack of an effective method for avoiding the incidental interception of calls involving American citizens when a link with one terminal in the United States in monitored.

2. CIA/NSA Drug Activity

In October 1972, NSA requested CIA assistance in monitoring United States—South American communication links to collect intelligence on illicit drug traffic. According to Buffham, NSA made this request

> because we felt that this was a sensitive matter, and that *greater security would be achieved by utilizing the career intercept operators of the CIA to perform the activity*, and,

---

[66] *Ibid.*

[67] Senior NSA official No. 2, 9/18/75, p. 106.

[68] According to ITT, many of these cities are transit points—calls are routed through them to other cities. For example, by monitoring one New York—South American city link, NSA could pick up calls originating in other South American cities to other cities in the United States. The call would simply be routed through New York and the South American city. Senior NSA official No. 2, 9/18/75, pp. 108–109.

Most telephone calls from the United States to South America are, in fact, routed through New York City.

[69] Senior NSA official No. 2, 9/18/75, p. 113; senior NSA official No. 1, 9/16/75, p. 33.

in addition, they could be more selective in providing items because *we would be able to give the CIA operators the specific names on the watch list, and we did not feel that we could or should provide those names to the* [East Coast military station]. [Emphasis added.] [70]

NSA's concern about the security of American names being provided to the East Coast station stemmed from the fact that the operators were young military personnel on short tours of duty. They were not professional intelligence officers, and NSA felt that monitoring American citizens was too sensitive a task for them. The use of CIA career operators satisfied NSA that targeting of American citizens would not be disclosed.

The Rockefeller Commission also investigated this activity, but found no evidence that the CIA directly targeted American citizens. The Rockefeller Commission report stated:

> For a period of approximately six months, commencing in the fall of 1973 [*sic*], the Directorate monitored telephone conversations between the United States and Latin America in an effort to identify foreign drug traffickers. . . .
>
> A CIA intercept crew stationed at an East Coast site monitored calls to and from certain Latin American telephone numbers contained on a "watch list" provided by NSA. While the intercept was focused on foreign nationals, it is clear that American citizens were parties to many of the monitored calls. . . .
>
> *The Commission's investigation disclosed that, from the outset of the Agency's involvement in the narcotics control program, the Director and other CIA officials instructed involved personnel to collect only foreign intelligence and to make no attempt—either within the United States or abroad—to gather information on American citizens allegedly trafficking in narcotics.* [Emphasis added.] [71]

The evidence examined by the Select Committee directly contradicts this finding. An internal CIA memorandum of November 17, 1972, to the Director of Communications from the Chief, Special Programs Division, reveals that the CIA *was* receiving the names of U.S. citizens.

> NSA had tasked [the East Coast site] with this requirement [to monitor for drug traffic] but were *unwilling to provide the site with the specific names and U.S. telephone numbers of interest on security/sensitivity grounds* . . . to get around the problems mentioned above NSA requested the Agency undertake intercept of the long lines circuits of interest. *They have provided us with all information available (including the "sensitive") and the [CIA] facility is working on the requirement.* [Emphasis added.] [72]

---

[70] Buffham, 9/12/75, p. 20.

[71] Report to the President by the Commission on CIA Activities Within the United States (Rockefeller Commission Report), June 1975, pp. 222–223.

[72] Memorandum from Chief, Special Programs Divisions (CIA) to the Director of Communications, 11/17/72.

This memorandum and subsequent testimony by NSA officials revealed that the CIA was monitoring these circuits to intercept the calls of American citizens suspected of illegal drug trafficking. During this period, NSA continued to monitor the same circuits at its East Coast site, but that site did not have the specific BNDD "sensitive" watch lists of American names which were supplied to the CIA. Thus, the conclusion reached by the Rockefeller Commission—that CIA intercepts were not undertaken for the purpose of gathering intelligence on American citizens—is not supported by the evidence.

3. Termination of Drug Activity

Three months after the CIA monitoring was initiated, CIA General Counsel Lawrence Houston issued an opinion which stated that the intercepts may violate Section 605 of the Communications Act of 1934.[73] This law, as amended in 1968, prohibits the unauthorized disclosure of any private communication of an American citizen to another party, unless undertaken pursuant to the President's constitutional authority to collect foreign intelligence which is crucial to the security of the United States.[74] Since intercepted messages were provided to BNDD, Houston concluded that the activity was for law enforcement purposes, which is also outside the CIA's charter. As a result of this memorandum, the CIA suspended its collection. NSA, which has no charter, continued to monitor these links for drug information.

NSA officials have testified that they were told in early 1973 that the CIA was terminating collection because it was concerned about operating an intercept station *within* the United States. This concern is completely different from the one expressed in Houston's memorandum. NSA officials have told the Committee that questions concerning the legality of the activity were either not mentioned by the CIA,[75] or else mentioned secondarily.[76]

NSA Deputy Director Buffham testified that after the CIA decided to stop the United States—South American drug monitoring, NSA began to review the legality and appropriateness of its efforts in support of BNDD. Although NSA is not prohibited by statute or executive directive from disseminating information that may pertain to law enforcement, it has always viewed its sole mission as the collection and dissemination of foreign intelligence. A senior NSA official testi-

---

[73] Memorandum from Houston to Acting Chief, Division D, 1/29/73.

[74] 18 U.S.C. 2511 (Omnibus Act, 1968) states: "nothing contained in . . . Section 605 . . . shall limit the constitutional power of the President to take such measures as he deems necessary to protect the nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States. . . ."

However, the *Keith* case (407 U.S. 297 (1972)) held that the Omnibus Act was simply a congressional recognition of the President's constitutional powers to protect the nation's security and did not grant the Executive additional powers. The Act did not further define the 1934 statute or provide the Executive with any additional authority to conduct foreign intelligence.

[75] Senior NSA official No. 2, 9/18/75, p. 117.

[76] Buffham, 9/12/75, pp. 23, 71.

See also former NSA Deputy Director Louis Tordella's testimony of 9/21/75, p. 77: "It was in their General Counsel's opinion beyond CIA's charter to monitor radio communications on U.S. soil and I was told that if they could move a group of Cubans up to Canada it would be quite all right, but they would not do it in the United States."

fied: "We do not understand our mission to be one of supporting an agency with a law enforcement responsibility." [77]

Although BNDD clearly was a law enforcement agency, NSA initially held that the intelligence it was supplying BNDD was a part of a legitimate USIB-approved effort to prevent drugs from entering the United States.[78] This international aspect of the requirement was interpreted by NSA as sufficient justification for classifying the activity as part of its "foreign intelligence" mission.

After discussions with the General Counsel's office at NSA and within the Office of the Secretary of Defense, the Director of NSA terminated the activity in June 1973.[79] All of NSA's drug materials—product, internal memoranda, and administrative documents—were destroyed in late August or early September 1973. Ordinarily, NSA keeps material for five years or more. According to a senior NSA official: "it wasn't thought we would get back into the narcotics effort anytime soon. There didn't seem to be any point in keeping them." [80]

4. Continuation of NSA's United States-South American Monitoring

In June 1975 the Committee received information that NSA continued to monitor United States—South American telephone calls after the June 1973 termination of the drug watch list activity. NSA officials confirmed that the same links targeted for the purpose of curbing illegal drug traffic were monitored by NSA for foreign intelligence after June 1973. Certain of these links were monitored until July 9, 1975.[81]

According to NSA, this activity was terminated when "it did not prove productive." [82] While this effort was underway, NSA states that it did not collect or disseminate any information on narcotics traffic from the United States—South American links. A senior NSA official stated: "Nothing ever came. No by-product. The problem was dead." [83]

5. Current Internal Policy Concerning Telephone Monitoring

No statute or executive directive prohibits NSA's monitoring a telephone circuit with one terminal in the United States.[84] An internal NSA instruction was issued on August 7, 1975, that requires the personal approval of the chief of a major element within the Agency before monitoring of voice communications with a terminal in the United States is initiated. According to Deputy Director Buffham, "It is obvious that no such collection will be undertaken unless it is extremely important and is properly reviewed within the Agency." [85]

F. Termination of the Civil Disturbance Watch List Activity

The watch list activity involving civil disturbances was officially terminated in the fall of 1973. This was due to a combination of fac-

[77] Senior NSA official No. 1, 9/16/75, p. 10.
[78] Senior NSA official No. 1, 9/16/75, p. 10; Banner, 9/15/75, pp. 49–50.
[79] Allen, 10/29/75, Hearings, Vol. 5, pp. 14–15.
[80] Senior NSA official No. 2, 9/18/75, p. 91.
[81] *Ibid.*, p. 125.
[82] *Ibid.;* Buffham, 9/12/75. p. 26.
[83] Senior NSA official No. 2, 9/18/75, p. 126.
[84] *Ibid.*, pp. 127–128.
[85] Buffham, 9/12/75, p. 30.

tors: growing concern within NSA regarding the program's vulnerability and propriety; the fact that courts were beginning to require the Government to reveal electronic surveillance conducted against particular criminal defendants; and the questions, raised by the drug watch list activity, about NSA's authority to engage in monitoring for law enforcement purposes. What follows is a description of events leading to the termination of the watch lists.

The only Supreme Court case addressing the issue of electronic surveillance purportedly undertaken for national security purposes is *United States* v. *United States District Court*, commonly referred to as the *Keith* case.[85a] The Supreme Court's decision was handed down on June 19, 1972, over a year before the watch list activity was terminated.

The case involved warrantless wiretaps on three U.S. citizens who were subsequently indicted for conspiracy to destroy Government property. There was no evidence of *foreign* participation in the alleged conspiracy.

After examining logs of the wiretaps *in camera*, the District Court judge had held that the surveillance on the defendants was unlawful and required that the overheard conversations be disclosed.[85b] The Supreme Court affirmed the District Court's ruling.

While recognizing the President's constitutional duty to "protect our Government against those who would subvert or overthrow it by unlawful means," [85c] the Court held that the power inherent in such a duty does not extend to the authorization of warrantless electronic surveillance deemed necessary to protect the nation from subversion by *domestic* organizations. The Court declared that the Fourth Amendment warrant requirement for electronic surveillance developed in two 1967 cases [86] applied, and that the electronic surveillances employed in the instant case were found to be unlawful. The Court did not reach the issue of whether the Executive has the constitutional power to authorize electronic surveillance without a warrant in cases involving the activities of *foreign* powers or agents.

Although the *Keith* ruling involved wiretaps and did not apply specifically to NSA, it did have a bearing on NSA's activities. Operation MINARET did entail warrantless electronic surveillance against certain domestic organizations. If there was no evidence to show that these domestic organizations were acting in concert with a foreign power, the *Keith* case would seem to cast doubts upon the legality of intercepting their messages without a warrant.

The watch list activity was never disclosed in a court proceeding; thus its legality has never been judicially determined. A 1973 criminal case did result in the Government's disclosure that some of a defendant's communications had been subject to a "foreign intelligence intercept." Some of the defendants in this 1973 case were members of a group which had been included on an NSA watch list by the Secret

---

[85a] 407 U.S. 297 (1972).

[85b] 444 F. 2d 651 (1971).

[85c] 407 U.S. at 310.

[86] *Katz* v. *United States*, 389 U.S. 347 (1967) and *Berger* v. *New York*, 388 U.S. 347 (1967). These two decisions deal with wiretaps, *not* with activities involving NSA. For further discussion, see the Committee's report on Warrantless Electronic Surveillance.

Service and FBI in mid-1971, and NSA had distributed some of their international communications to these agencies.[87] The propriety of these actions was never considered by the court, because the Government moved to dismiss the case rather than reveal the specifics of the watch list activity.

General Lew Allen, Jr. became the Director of NSA on August 15, 1973. In the course of familiarizing himself with his new responsibilities, he was fully briefed on the watch list activity.

According to Allen, the BNDD watch list activity had been terminated just prior to his arrival at NSA because the Agency feared "that it might not be possible to make a clear separation between requests for information submitted by BNDD as it pertained to legitimate foreign intelligence requirements and the law enforcement responsibility of BNDD." He also stated that the activity in support of the FBI, CIA, and Secret Service was suspended when NSA "stopped the distribution of information in the summer [August] of 1973." [88] Deputy Director Buffham told the Committee this dissemination was terminated due to three concerns: (1) NSA could not be certain as to what uses were being made of the information it was providing other agencies; (2) it feared that broad judicial discovery procedures might lead to the disclosure of sensitive intelligence sources and methods; and (3) NSA wanted to be "absolutely certain that we are providing information only for lawful purposes and in accordance with our foreign intelligence charter." [89]

During July and August 1973, meetings were held between NSA and Justice Department representatives. According to NSA, these discussions influenced the Agency's decision to suspend the dissemination of watch list material.[90] As Buffham testified:

> I believe although I am not positive, that Dr. Tordella, the Deputy Director, had discussions with people at Justice regarding the legality of our activities, and that these could have influenced then the determination in NSA to cease the activities in August, even though we had not yet received any formal statements from Justice.[91]

At a meeting on August 28, 1973, NSA officials informed Assistant Attorney General Henry Petersen that communications involving the defendants in the 1973 criminal case had been intercepted and that NSA opposed "any disclosure of this technique and program." [92] Petersen apprised Attorney General Richardson of these events in a memorandum of September 4, 1973. On September 7, 1973, Petersen sent a memorandum to FBI Director Clarence Kelley, requesting to be advised by September 10 of:

> the extent of the FBI's practice of requesting information intercepted by the NSA concerning domestic organizations

---

[87] Memorandum from Henry Petersen to Elliot Richardson, 9/4/73, p. 6.
[88] Allen, 10/29/75, Hearings, Vol. 5, p. 15.
[89] Buffham, 9/12/75, p. 67.
[90] Lew Allen, Jr., testimony, 9/15/75, p. 55.
[91] Buffham, 9/12/75, p. 67.
[92] Petersen to Richardson memorandum, 9/4/73, p. 6.

> or persons for intelligence, prosecutorial, or any other purposes . . . [and] any comments which you may desire to make concerning the impact of the *Keith* case upon such interceptions. . . .[93]

Kelley responded three days later that the FBI had requested intelligence from NSA "concerning organizations and individuals who are known to be involved in illegal and violent activities aimed at the destruction and overthrow of the United States Government." [94] He continued that the FBI did not view the materials supplied it by NSA, or the watch list activity in general, as inconsistent with the *Keith* decision: the information "cannot possibly be used for any prosecutive purpose" and "we do not consider the NSA information as electronic surveillance information in the sense that was the heart of the *Keith* decision." The FBI's position was that the information supplied by NSA did not result from specific targeting of an individual's communications in the same sense as a wiretap; therefore, it was not "electronic surveillance." Kelley maintained:

> We do not believe that the NSA actually participated in any electronic surveillance, per se of the defendants for any other agency of the government, since under the procedures used by that agency *they are unaware of the identity of any group or individual* which might be included in the recovery of national security intelligence information.[95] [Emphasis added.]

This position is difficult to defend since intelligence agencies, including the FBI, submitted specific American names for watch lists which resulted in the interception of Americans' international communications.

On September 17, Allen wrote FBI Director Kelley and the heads of other agencies receiving information from NSA regarding continuation of the watch list activity. Noting that "the need for proper handling of the list and related information has intensified, along with ever-increasing pressures for disclosure of sources by the Congress, the courts, and the press," Allen requested, "at the earliest possible date," that Kelley and the other agency heads "review the current list your agency has filed with us in order to satisfy yourself regarding the appropriateness of its contents. . . ." [96]

After receiving Kelley's September 10 memorandum, Petersen advised the Attorney General that the current number of individuals

---

[93] Memorandum from Henry Petersen to Clarence Kelley, 9/7/73, p. 1.

[94] Memorandum from Clarence Kelley to Henry Petersen, 9/10/73, p. 2.

Kelley is clearly overstating his case when he says Americans are "known" to be involved in illegal activities. Many of the individuals were protesters speaking out against the Government's policies, not urging the overthrow of the Government.

J. Edgar Hoover discusses the necessity of obtaining information "determining the extent of international cooperation among New Leftists" in a memorandum to NSA of June 5, 1970, which is much broader than targeting individuals who are attempting the violent overthrow of the Government.

[95] Kelley memorandum, 9/10/73, pp. 3–5.

[96] Letter from Lew Allen, Jr. to Clarence Kelley, 9/17/73, Hearings, Vol. 5, Exhibit No. 6, pp. 158–159.

and organizations on NSA watch lists submitted by the FBI was "in excess of 600." [97] Petersen pointed out many legal problems arising from this program and recommended that

> the FBI and Secret Service be immediately advised to cease and desist requesting NSA to disseminate to them information concerning individuals and organizations obtained through NSA electronic coverage and that NSA should be informed not to disclose voluntarily such information to Secret Service or the FBI unless NSA has picked up the information on its own initiative in pursuit of its foreign intelligence mission.[98]

He also recommended that the standards and procedures which applied to "cases where the FBI seeks to acquire foreign intelligence or counterespionage information by means of its own listening devices" be extended to apply to the watch list activity.[98a] These procedures included obtaining prior written approval by the Attorney General.

On October 1, Richardson sent memoranda to FBI Director Kelley and the Director of the Secret Service, instructing them to cease requesting information obtained by NSA "by means of electronic surveillance." [99] The Attorney General also requested that his approval be sought prior to either agency's renewing requests to NSA for foreign intelligence or counterespionage information.

On the same day, Richardson sent a letter to Allen, stating that he found the watch list activity to be of questionable legality in view of the *Keith* decision, and requesting that NSA "immediately curtail the further dissemination" of watch list information to the FBI and Secret Service. Although Richardson specified that NSA was not to respond to "a request from another agency to monitor in connection with a matter that can only be considered one of domestic intelligence," he stated that "relevant information acquired by you in the routine pursuit of the collection of foreign intelligence information may continue to be furnished to appropriate Government agenices." [100]

Kelley responded to Richardson's memorandum on October 3 and agreed to comply with the Attorney General's "instructions to discontinue requests to NSA for electronic surveillance information and to obtain approval prior to any future inquires to NSA for such information." [101] There was apparently some confusion at this point whether Richardson's instructions meant that NSA was prohibited from disseminating *any* information to FBI. After further consultations, it was determined that the caveats Richardson placed on dissemination applied only to information on American citizens and organizations, and not to foreign intelligence and counterespionage matters.

Allen replied to Richardson's letter on October 4, stating that he had "directed that no further information be disseminated to the

---

[97] Memorandum from Henry Petersen to Elliot Richarson, 9/21/73, p. 1.
[98] Petersen to Richardson memorandum, 9/21/73, p. 3.
[98a] *Ibid.*
[99] Memorandum from Elliot Richardson to Clarence Kelley, 10/1/73.
[100] Letter from Elliot Richardson to Lew Allen, Jr., 10/1/73, Hearings, Vol. 5, Exhibit No. 7, pp. 160, 161.
[101] Memorandum from Clarence Kelley to Elliot Richardson, 10/3/73.

FBI and Secret Service, pending advice on legal issues." [102] Although Allen had agreed to suspend dissemination, NSA's position remained that these communications had always been collected "as an incidental and unintended act in the conduct of the interception of foreign communications." Allen thus asserted that NSA's "current practice conforms with your [Richardson's] guidance that, 'relevant information acquired [by NSA] in the routine pursuit of the collection of foreign intelligence information may continue to be furnished to appropriate government agencies.' " [103]

As a result of these and other exchanges between officials at NSA and Justice, the Agency officially terminated its watch list activity involving American citizens and organizations in the fall of 1973. It would no longer accept such names from other agencies for the purpose of monitoring their international communications.

To a substantial degree, this decision was prompted by the legal implications of the Keith case and by NSA's fear that criminal prosecutions of persons on the watch lists would inevitably lead to disclosure of its intelligence sources and methods. Indeed, the 1973 criminal case referred to above posed the threat that the watch list activity might have to be disclosed for the first time in a public forum.

It is important to note that the decision to terminate the watch list was ultimately the administrative decision of an executive agency. There is no statute which expressly forbids such activity, and no court case where it has been squarely at issue. Without legislative controls, NSA could resume the watch list activity at any time upon order of the Executive.

G. Authorization

Authorization of the watch list activity must be viewed in the context of how NSA operates. It is a service agency which provides foreign intelligence information at the request of consumer agencies. Specific requirements are levied on USA, although the Agency also engages in collection activities that are not responsive to specific tasking. For example, many USIB requirements—such as those aimed at terrorist activities, gathering economic intelligence, or discovering foreign links to civil disturbances—were so broad that NSA was given wide discretion for selecting not only the communications channels to be monitored, but also what information was disseminated.[104] While this is often appropriate because only NSA has the knowledge and expertise to make these decisions, it also allows NSA considerable flexibility in carrying out its mission.

NSA also responds to specific requests from other Federal agencies. Indeed, it is no exaggeration to state that NSA's operations are undertaken almost entirely to satisfy the intelligence needs of other agencies. The watch list activity was no exception.

---

[102] Letter from Lew Allen, Jr. to Elliot Richardson, October 4, 1973, Hearings, Vol. 5, Exhibit No. 8, p. 163.

[103] Allen letter, October 4, 1973, Hearings, Vol. 5, Exhibit No. 8, pp. 162, 163.

[104] Wannall (FBI), October 3, 1975, p. 12: "I would say that by far the majority of the product that I saw would have been information that would have been disseminated to us by NSA, based upon the knowledge of that Agency of our responsibilities, as opposed to a specific request for any information that might come to NSA's attention, that we ourselves initiated."

1. Knowledge and Authorization Outside NSA

In the case of the 1967–1973 watch list activity, NSA clearly received instructions from the Army in 1967 to look for possible foreign influence on, or control of, American peace and Black power activists. NSA subsequently received the names of American and foreign citizens and groups from other intelligence agencies.

This activity was not formally approved by USIB. Although NSA notified USIB members that it was responding to the Army's request, the inclusion of American names on an NSA watch list was never discussed at subsequent USIB meetings. Although there were official USIB requirements for information concerning international drug activity, presidential protection, and terrorism, there was no approval or discussion of targeting American citizens. NSA officials contend that the submission of American names by USIB members constituted approval.[105]

The desire for tight security over the watch list program resulted in limiting participation to those "with a need to know." Therefore, it was not in NSAs best interests to have formal USIB approval of a requirement since knowledge would have been more widely spread.

According to documents supplied to the Committee and testimony of NSA officials, Defense Secretaries Melvin Laird and James Schlesinger, as well as Attorneys General John Mitchell and Richard Kleindienst, were informed that NSA was monitoring Americans. Former NSA Director, Admiral Noel Gayler sent a Top Secret "Eyes Only" memorandum to Laird and Mitchell on January 26, 1971, which outlined ground rules for "NSA's Contribution to Domestic Intelligence." In this memorandum, Gayler refers to a discussion he had earlier that day with both men on how NSA could assist them with "intelligence bearing on domestic problems." The memorandum mentioned the monitoring for drug trafficking and foreign support of subversive activities, but did not discuss "watch lists" specifically.[106]

NSA Deputy Director Buffham supplied the Committee with a Memorandum for Record which indicated that he had personally shown the Gayler memorandum to Mitchell and had been told by the Military Assistant to Secretary of Defense Laird that the Secretary had read and agreed to the memorandum.[107] In a handwritten note

---

[105] Allen, 10/29/75, Hearings, Vol. 5, p. 28.

[106] Memorandum from NSA Director Noel Gayler to the Secretary of Defense and the Attorney General, "NSA Contribution to Domestic Intelligence," 1/26/71, Hearings, Vol. 5, Exhibit No. 5, pp. 156–157.

This memorandum responded to the interests of the Intelligence Evaluation Committee (IEC), a Justice Department working group set up to carry out domestic intelligence-gathering activities. The IEC was an outgrowth of the Huston Plan and is detailed in the Committee's report on the Huston Plan. Suffice it to say that NSA sent a representative to that group and Gayler was providing them with a statement of NSA's capabilities and procedures for supplying intelligence.

[107] Memorandum for the Record, Benson K. Buffham, 2/3/71.

When questioned by the Committee, neither Mitchell, Laird, nor Kleindienst recalled the watch list activity. Mitchell does not recall NSA's involvement in monitoring the communications of American citizens or the meeting with Buffham. He stated, however, that "he may have" had such a meeting, but cannot recall. John Mitchell testimony, 10/2/75, pp. 47–48.

made available to the Committee, Gayler recalls that he personally showed the January 26, 1971, memorandum to Kleindienst on July 1, 1972.

Finally, former NSA Deputy Director Tordella testified that he accompanied General Samuel C. Phillips, Gayler's successor as Director of NSA, to brief Secretary of Defense Schlesinger on the watch list in the summer of 1973.[108]

In summary, a number of Federal agencies were aware of NSA's watch lists and used them. It is clear that the United States Intelligence Board, which ordinarily set the intelligence requirements to which NSA responded, never gave its formal approval for the watch list activity. It also appears that at least two Attorneys General and two Secretaries of Defense were generally aware that NSA was monitoring the international communications of American citizens, but none took measures to halt the practice.

2. Knowledge and Approval Within NSA

There is a discrepancy in the testimony of knowledgeable NSA staff members and a former NSA Director with regard to his knowledge of the watch list activity. When asked whether NSA had included the names of American citizens or organizations on its watch lists, Admiral Noel Gayler (who was Director of NSA during the height of the activity) responded:

> I don't know that I even knew that in that specific way. I knew that communications of one foreign terminal sometimes concerned doings of interest of people, including American citizens, yes. And when I became aware of that, I can't tell you, I guess it was a year or so after I got there.[109]

Gayler became NSA Director in August 1969. He maintains that he first became aware of the watch list activity about the time of the June 1970 Huston plan for domestic surveillance, ten months after his arrival and eleven months after the MINARET Charter was issued.

Gayler was one of the original participants in the Huston plan deliberations and in the Intelligence Evaluation Committee (early 1971). Both of these efforts were designed to use the resources of NSA and other intelligence agencies to gather information on internal security matters. In fact, part of the Huston plan called for the expansion of the watch list activity. Buffham told the Committee that if the plan had been implemented he assumed "other intelligence agencies would then increase the numbers of names on their lists" and NSA would possibly target specific communications channels to obtain the international traffic of American citizens.[110] NSA was par-

[108] Tordella, 9/21/75, p. 74.
[109] Noel Gayler testimony, 6/19/75, p. 64.
[110] Buffham, 10/29/75, Hearings, Vol. 5, p. 45.
In addition, the Huston Plan report sent to the participants was classified "Top Secret, Handle Via COMINT Channels Only," the classification placed on NSA intercept information. This caveat was designed to limit the distribution of the report and prevent disclosure of the illegal activities suggested by Tom Charles Huston. For a further explanation, see the Committee's report, "National Security, Civil Liberties, and the Collection of Intelligence: A Report on the Huston Plan."

ticularly concerned that the executive branch directives would have had to be changed to permit such an expansion. The alternatives outlined in the Huston plan included the recommendation that the controling NSCID and the relevant DCID be changed to allow NSA to target international communications links carrying the messages of American citizens.

NSA was already engaged in watch list activity which although it did not involve targeting of specific communications links, did involve targeting Americans by name. The Huston Plan states:

> NSA is currently doing so on a restricted basis, and the information it has provided has been most helpful. Much of this information is particularly useful to the White House. . . .[111]

As discussed earlier, the July 1, 1969, MINARET charter was designed to restrict knowledge of the watch list activity. It was released about a month before Gayler arrived at NSA and, according to a senior NSA official, Gayler "knew everything that was in it, what was going on, and endorsed it." [112] Gayler recalls that his first knowledge of the watch list came during the Huston Plan deliberations, almost a year later. Another senior NSA official testified that Gayler "*review every piece of MINARET product*" and maintained that "the Director kept a close eye on this activity and reviewed the requirements." [Emphasis added.] [113] This employee also testified that Gayler was shown the product of the watch list activity and was kept fully informed.

H. Conclusions

NSA's monitoring of international communications comprises only a portion of its total mission, but the examination of this capability to intrude on the telephone calls and telegrams of Americans represents a major part of the Committee's work on NSA. The watch list activities and the sophisticated technological capabilities that they highlight present some of the most crucial privacy issues facing this nation. Space age technology has outpaced 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.

The analysis presented here of the deliberate targeting of American citizens and the associated incidental interception of their communications demonstrates the need for a legislative charter that will define, limit, and control the signals intelligence activities of the National Security Agency. This should be accomplished both to preserve and protect the Government's legitimate foreign intelligence operations, and to ensure that the constitutional rights of Americans are safeguarded.

---

[111] Memorandum from Tom Charles Huston to H. R. Haldeman, 7/7 "Operational Restraints on Intelligence Collection," p. 1, Hearings, Vol. 2, Exhibit No. 2, p. 193.

[112] Senior NSA official No. 2, 9/18/75, pp. 43–44.

[113] Senior NSA official No. 1, 9/16/75, pp. 63, 62.

The next section describes a recently terminated NSA collection program which also involved United States citizens—Operation SHAMROCK. This program did not require any special technology; international telegrams were simply turned over to NSA at the offices of three cable companies.

III. A SPECIAL NSA COLLECTION PROGRAM: SHAMROCK

SHAMROCK is the codename for a special program in which NSA received copies of most international telegrams leaving the United States between August 1945 and May 1975. Two of the participating international telegraph companies—RCA Global and ITT World Communications—provided virtually all their international message traffic to NSA. The third, Western Union International, only provided copies of certain foreign traffic from 1945 until 1972. SHAMROCK was probably the largest governmental interception program affecting Americans ever undertaken. Although the total number of telegrams read during its course is not available, NSA estimates that in the last two or three years of SHAMROCK's existence, about 150,000 telegrams per month were reviewed by NSA analysts.[115]

Initially, NSA received copies of international telegrams in the form of microfilm or paper tapes. These were sorted manually to obtain foreign messages. When RCA Global and ITT World Communications switched to magnetic tapes in the 1960s, NSA made copies of these tapes and subjected them to an electronic sorting process. This means that the international telegrams of American citizens on the "watch lists" could be selected out and disseminated.

A. Legal Restrictions

1. The Fourth Amendment to the Constitution of the United States

Obtaining the international telegrams of American citizens by NSA at the offices of the telegraph companies appears to violate the privacy of these citizens, as protected by the Fourth Amendment. That Amendment guarantees to the people the right to be "secure . . . in their papers . . . against unreasonable searches and seizures." It also provides that "no Warrants shall issue, but upon probable cause." In no case did NSA obtain a search warrant prior to obtaining a telegram.

2. Section 605 of the Communications Act of 1934 (47 U.S.C. 605)

As enacted in 1934, eleven years before SHAMROCK began, section 605 of the Communications Act provided:

> No person receiving, assisting in receiving, transmitting, or assisting in transmitting, any interstate or foreign communication by wire or radio shall divulge or publish the existence, contents, substance, purport, effect, or meaning thereof. . . .

Section 605 was amended in 1968 by the addition of the phrase: "Except as authorized by chapter 119, Title 18, no person . . . ."

[115] Staff summary of interview with senior NSA official No. 3, 9/17/75, p. 3.

The import of this 1968 addition, however, is not clear, and the Supreme Court has yet to rule on the point.[116]

The relevant provision in chapter 119, section 2511(3), provides that "nothing contained in this chapter or in section 605 of the Communications Act of 1934 . . . shall limit the constitutional power of the President . . . to obtain foreign intelligence information deemed essential to the security of the United States. . . ." [117] Yet the Supreme Court, in the *Keith* decision (1972), held that this section "confers no power" and "merely provides that the Act shall not be interpreted to limit or disturb such power as the President may have under the Constitution." [118]

It is thus uncertain what the phrase in the 1968 amendment to section 605—"except as *authorized* by chapter 119, title 18" [Emphasis added.]—means. The Supreme Court has held that the relevant section of chapter 119 does not *authorize* any activity. The applicability of section 605 to the interception of international telegrams for foreign intelligence purposes is therefore unclear. It would appear that where such telegrams are intercepted for other than foreign intelligence purposes (e.g., the watch list activity), section 605 would be violated.

3. The Controlling National Security Council Intelligence Directive

Since 1958, this executive directive has authorized NSA to conduct communications intelligence activities.[119] These have been defined as *excluding* "the intercept and processing of unencrypted written communications." It would appear that if copies of international telegrams are "written communications," NSA has exceeded its authority under the executive's own internal directives.

B. The Committee's Investigation

The SHAMROCK operation was alluded to in documents furnished to the Committee by the Rockefeller Commission in May 1975. They indicated that CIA had provided "cover" for an NSA operation in New York where international telegrams had been copied.[120]

In early June 1975, an oral inquiry regarding the operation was made to NSA officials, but no confirmation of the project was forthcoming. In July, the Committee sent written interrogatories to NSA, and was told that this subject was so sensitive that it would be disclosed only to Senators Church and Tower. No such briefing was immediately arranged, however.

In July and August, news stories were published which appeared to reveal small parts of the SHAMROCK operation.[121]

The Committee continued to press the matter with NSA, and in early September the agency gave the Committee its first detailed

---

[116] The U.S. Court of Appeals for the Third Circuit did rule, in *U.S.* v. *Butenko*, 494 F.2d 593 (3d Cir. 1974), *cert. denied sub nom. Ivanov* v. *United States*, 419 U.S. 881 (1974), that section 605 did not render unlawful electronic surveillance conducted solely for foreign intelligence purposes.

[117] 18 U.S.C. 2511(3).

[118] *United States v. United States District Court for the Eastern District of Michigan, et al.*, 407 U.S. 297 (1972). See pp. 757, 759–760.

[119] See pp. 737–738.

[120] Commission on CIA Activities Within the United States, interview with senior CIA officials, 3/11/75, pp. 14–16, in Select Committee files.

[121] See Frank Van Riper, "Find U.S. Agents Spy on Embassies' Cables," *New York Daily News*, 7/22/75; *idem.*, "FCC Terms Cable-Tapping Illegal, Will Investigate FBI," *New York Daily News*, 7/23/75; Nicholas Horrock. "National Security Agency Reported Eavesdropping on Most Private Cables," *New York Times*, 8/1/75, p. 1.

information. This briefing was followed by interviews with present and former NSA employees who had been responsible for the program and by examinations of documents at NSA and the Department of Defense. NSA assured the Committee at the time that it had examined all NSA documents which pertained to SHAMROCK. On September 23, the full Committee was briefed by an NSA official in executive session. Following this briefing, the Committee interviewed officials in the telegraph companies which had participated in the SHAMROCK program.

On the basis of this investigation, the Committee prepared a report which it submitted to NSA for review. NSA had no specific comments regarding the accuracy of the report, but expressed its general objection to public disclosure of the operation on the grounds that the report was based on classified information.[122]

On November 6, 1975, in a public session of the Committee, Chairman Frank Church read the report on SHAMROCK into the record. Due to the refusal of the executive branch of provide witnesses in public session, no other public record was made.[122a]

At this point, the Committee's active investigation ceased. The Committee presumed that it had exhausted all sources of information about SHAMROCK.

On March 25, 1976 as the Committee was about to send this report to press, it was informed by the Department of Defense that NSA had "discovered" a file containing various documents and memoranda about SHAMROCK. An NSA official explained that the file had been held by a lower-level employee at NSA until around March 1, 1976, when he brought it to the attention of his superiors. Since this occurred several months after the Committee's public report, and, in the opinion of NSA, did not substantially alter the Committee's findings, it was not immediately reported to the Committee.

After examining the documents, the Committee decided that the final NSA report should incorporate this new information. Although it does not alter the basic findings reported in November 1975, it does change some of the details.[123]

C. The Origins of SHAMROCK

During World War II, under the wartime censorship laws,[124] all international message traffic was made available to military censors.[125] Copies of pertinent foreign traffic were turned over to military intelligence. With the cessation of the War in 1945, this practice was to end.

In August 1945, the Army sought to continue that part of the wartime arrangement which had allowed military intelligence access to certain foreign traffic.[126] At that time, most of this traffic was still conveyed via the facilities of three carriers.[127]

On August 18, 1945, two representatives of the Army Signal Security Agency were sent to New York

> to make the necessary contacts with the heads of the Commercial Communications Companies in New York, secure their

---

[122] Letter from NSA to the Select Committee, 10/29/75, Hearings, Vol. 5, p. 51.
[122a] Hearings, Vol. 5, pp. 57–60.
[123] *Ibid.*
[124] 47 U.S.C. 606.
[125] See the testimonies of: Senior NSA official No. 4, 9/23/75, pp. 45–46; Tordella, 99/21/75, pp. 6–7; senior officer, ITT World Communications, Inc., 10/15/75, p. 4.
[126] Letter from an Army intelligence officer to the Commanding General, Signals Security Agency, Army Service Forces, "Report on New York Trip," 8/24/45.
[127] Staff summary of an interview with Senior NSA official No. 3, 9/17/75, p. 3.

> approval of the interception of all Governmental traffic entering the United States, leaving the United States, or transiting the United States, and make the necessary arrangements for this photographic intercept work.[128]

They first approached an official at ITT, who "very definitely and finally refused" to agree to any of the Army proposals. The Army representatives then approached a vice president of Western Union Telegraph Company, who agreed to cooperate unless the Attorney General of the United States ruled that such intercepts were illegal.[129]

Having succeeded with Western Union, the Army representatives returned to ITT on August 21, 1945, and suggested to an ITT vice president that "his company would not desire to be the only non-cooperative company on this project." The vice president decided to reconsider and broached the matter the same day with the president of the company. The ITT president agreed to cooperate with the Army, provided that the Attorney General decided that the program was not illegal.[130]

These Army representatives also met with the president of RCA on August 21, 1945. The RCA president indicated his willingness to cooperate, but withheld final approval until he, too, had heard from the Attorney General.[131]

After their trip, the Army representatives reported to their superiors that the companies were worried about the illegality of their participation in the program:

> Two very evident fears existed in the minds of the heads of each of these communications companies. One was the fear of the illegality of the procedure according to present FCC regulations. In spite of the fact that favorable opinions have been received from the Judge Advocate General of the Navy and the Judge Advocate General of the Army, it was feared that these opinions would not hold in civil court and, as a consequence, the companies would not be protected. If a favorable opinion is handed down by the Attorney General, this fear will be completely allayed, and cooperation may be expected for the complete intercept coverage of this material. The second fear uppermost in the minds of these executives is the fear of the ACA which is the communications union. This union has reported on many occasions minor infractions of FCC regulations and it is feared that a major infraction, such as the proposed intercept coverage, if disclosed by the Union, might cause severe repercussions.[133]

Later memoranda by another Army representative who was present indicate that the companies had consulted their corporate attorneys during these three days of discussions, and that their attorneys uniformly advised against participation in the proposed intercept program.[134] The company executives were apparently willing to ignore this advice if they received assurances from the Attorney General that he would protect them from any consequences.[135]

---

[128] Army intelligence officer letter to Commanding General, 8/24/45.
[129] *Ibid.*
[130] *Ibid.*
[131] *Ibid.*
[133] *Ibid.*
[134] Memorandum from Record, Armed Forces Security Agency, "SHAMROCK Operations," 8/25/50.
[135] *Ibid.*

The new documentary evidence made available to the Committee did not reveal that the Attorney General at that time, Tom C. Clark, actually made the assurances that the companies desired. It is clear, however, that the program began shortly after the August meetings: ITT and Western Union began their participation by September 1,[136] and RCA by October 9, 1945.[137]

In a letter from the Army Signals Security Agency to the Army Chief of Staff on March 19, 1946, the writer indicates that SHAMROCK was well underway, but that concerns about its legality had not vanished:

> It can be stated that both [Western Union and RCA] have placed themselves in precarious positions since the legality of such operations has not been established and has necessitated the utmost secrecy on their part in making these arrangements. Through their efforts, only two or three individuals in the respective companies are aware of the operation.[138]

April 26, 1976, while this report was being printed, DOD informed the Committee that nine additional documents relating to SHAMROCK had been found in the National Archives. The documents revealed that the Office of Secretary of Defense James Forrestal attempted unsuccessfully in June 1948 to have Congress pass an amendment to relax the disclosure restrictions of Section 605 of the Federal Communications Act of 1934. Agencies designated by the President would have been allowed to obtain the radio and wire communications of foreign governments. If the amendment had passed, the SHAMROCK program, as it was originally conceived, would have been authorized by law.

The proposed amendment sought to allay concerns of the companies on the legality of their participation in SHAMROCK. The companies were demanding assurances in 1947 not only from the Secretary of Defense and the Attorney General, but also from the President that their participation was essential to the national interest and that they would not be subject to prosecution in the Federal Courts. Secretary Forrestal, who stated he was speaking for the President, gave ITT and RCA representatives these assurances at a December 16, 1947, meeting in Washington, D.C.[139] Forrestal warned, however, that the assurances he was making could not bind his successors in office.[140]

Representatives of Western Union were not present at this meeting. Documents made available to the Committee indicate that the President and Operating Vice President of Western Union were briefed in January 1948 on the earlier meeting with RCA and ITT.[141]

In early June 1948, the Chairmen of the Senate and House Judiciary

---

[136] Army intelligence officer letter to Commanding General, 8/24/45. The armistice ending hostilities between the United States and Japan was signed in Japan on September 2, 1945 (September 1 in the United States).

[137] Letter from a senior official at RCA Global, Inc., to the Army Signal Security Agency, 10/9/45.

[138] Letter from Assistant Chief of Staff, Army Signals Security Agency, to the Army Chief of Staff, "Letters of Appreciation," 3/19/46. This letter transmitted letters of appreciation that were to be forwarded to two of the participating companies.

[139] Andrews, 9/23/75, p. 34 (referring to documents in his possession). These documents were examined by the Committee. Select Committee memorandum, 9/17/75, "Review of Documents at DoD Regarding LPMEDLEY."

[140] Andrews, 9/23/75, p. 40.

[141] Select Committee memorandum, 11/5/75, "Persons at 1947 and 1949 SHAMROCK Meetings" (describing a handwritten note to this effect).

Committees were informed of the Government's need for a relaxation of Section 605 and of its position with the telegraph companies. The delicacy of the problem and the top secret nature of the information were made clear to these two Chairmen. The amendment was considered in an executive session of the Senate Judiciary Committee on June 16, 1948, and approved. Since support for the bill was not unanimous, however, the Committee voted to leave it to the Chairman's discretion whether or not to release the bill to the Senate floor. The representative of the Secretary of Defense then told the Senate Judiciary Chairman that "we did not desire an airing of the whole matter on the Floor of the Senate at this late date in the session." The bill apparently was not reported out.

A Defense Department official expressed the view that the thought a great deal had already been accomplished and that the administration had sufficient ammunition to be able to effect a continuation of the present practices with the companies. Apparently no other statutory attempts were made to authorize the companies' participation in SHAMROCK.

The companies sought renewed assurances from Forrestal's successor, Louis Johnson, in 1949. Johnson told them that the President and Attorney General had been consulted and had given their approval.[144] To the knowledge of those interviewed by the Committee, this was the last instance in which the companies such assurances from the Department of Defense.[145]

Dr. Louis Tordella, who was NSA Deputy Director from 1958 until 1974 and the NSA official with chief administrative responsibility for SHAMROCK, testified that to the best of his knowledge, no President since Truman knew of the program. He "was not sure" whether any Attorney General since Tom Clark had been informed of it, or if succeeding Secretaries of Defense were aware of it. Tordella stated he briefed former Secretary of Defense Schlesinger about the SHAM ROCK operation in the summer of 1973.[146]

The Army Signals Security Agency controlled the collection program until 1949, when the Armed Forces Security Agency was formed. Responsibility for the program passed from AFSA to the National Security Agency when it was created in 1952.[147]

D. The Participation of the Companies

None of the telegraph companies could find any record of an agreement with NSA or its predecessors wherein the companies would provide copies of telegrams to the Government,[148] or which reflected anything about arrangements with NSA. No one interviewed by the Committee had any recollection or knowledge that the Government had

[144] Andrews, 9/23/75, p. 34.
[145] *Ibid.*, p. 40.
[144] *Ibid.*, p. 34.
[145] Andrews, 9/23/75, p. 40; Tordella, 9/21/75, p. 12.
[146] Tordella, 9/21/75, pp. 32–34. Tordella did state that he thought former NSA Director Noel Gayler had informed Attorney General John Mitchell about SHAMROCK in 1970 (*Ibid.*, p. 33); Mitchell, however, did not recall being informed about the operation (Mitchell, 10/2/75, pp. 47–48). Tordella stated that he was "quite sure" former Secretary of Defense Laird had known of the SHAMROCK program (Tordella, 9/21/75, pp. 33–34).
[147] Tordella, 9/21/75, p. 34; senior NSA official No. 4, 9/23/75, p. 47.
[148] Staff summaries of interviews with Counsel, RCA Global, Inc., 10/9/75, p. 3; Counsel, ITT World Communications, Inc., 10/9/75, p. 1; Counsel, Western Union International, Inc., 10/10/75, p. 1.

given the companies specific assurances to ensure their cooperation in 1945, 1947, 1949, or at any time thereafter.[149]

Apparently only a few people in each company—apart from those who physically turned over the materials—had any knowledge of the NSA arrangement.[150] These were primarily mid-level executives charged with the operational aspects of the companies' business. All assumed that the arrangement was valid when it was made and thus continued it. No witness from the telegraph companies recalled that there had ever been a review of the arrangements at the executive levels of their respective companies.

Furthermore, none of the participating companies was apparently aware that information other than foreign traffic was extracted from the messages they were providing.[151] Yet no official at any of the three companies could recall his company asking NSA what it was doing with the information it was furnished and, specifically, whether NSA was reading the telegrams of the companies' American customers.[152]

Finally, both the telegraph companies and NSA deny that the companies ever received anything for their cooperation in SHAM ROCK, whether in the form of compensation or favoritism from the Government. All claim they were motivated by purely patriotic considerations.[153]

If there were similarities as to their involvement in SHAM ROCK, the participation of each company varied in practice.

1. RCA Global

According to a memorandum prepared by Army representatives, RCA (the parent company of RCA Global) agreed in August 1945 to allow Army personnel, who were to be dressed in civilian clothes, to photograph foreign traffic passing over its facilities in New York, Washington, and San Francisco. The memorandum further provided that "only the desired traffic will be filmed." [154]

The company official at RCA Global who was charged with implementing the SHAMROCK program testified that several alternatives were discussed with Army representatives. He stated that the Army had first proposed tapping into the company's overseas lines, but the official rejected this idea as unfeasible. The Army representatives then proposed that company employees sort out pertinent traffic and turn it over to them; the official rejected this because he did not want company employees involved. The RCA official finally agreed to provide paper tapes of all international message traffic. It was understood that these messages would be sorted manually by persons from the Army Signals Security Agency on the company's premises, and that only

[149] Testimonies of former vice president, RCA Global, 10/9/75, pp. 17–18, and senior officer, ITT World Communications, Inc., 10/15/75, p. 6; and affidavit of senior officer, Western Union International, 10/19/75, p. 1.

[150] Counsel, RCA Global, 10/9/75, p. 2; counsel, ITT World Communications, 10/9/75, pp. 1–2; and counsel, Western Union International, 10/10/75, p. 3 (staff summaries).

[151] Former vice president, RCA Global, 10/17/75, p. 13; senior officer, ITT World Communications, 10/15/75, p. 12.

[152] Senior officer, ITT World Communications, 10/15/75, p. 12. See also testimony of senior officer, RCA Global, Inc., 10/19/75, p. 19. RCA Global and ITT World Communications were, by the mid-1960s, providing NSA all of their outgoing telegraph traffic on magnetic tapes.

[153] Senior officer, RCA Global, 10/19/75, p. 23; senior officer, ITT World Communications, 10/15/75, p. 14; counsel, Western Union International, 10/10/75, p. 2 (staff summary).

[154] Army intelligence officer letter to Commanding General, 8/24/45.

certain foreign traffic would be selected. There was never a written agreement to this effect, however, according to the former official.[155]

In New York, Army representatives were given office space in the area where the paper tapes of RCA Global's international message traffic were sorted manually for foreign traffic. Messages of interest were transmitted over teletype machines located in that office space.[156]

In Washington and San Francisco, Army agents were permitted to pick up copies of foreign messages, which they took to another office for microfilming.[157] By 1950, a Recordak (microfilm) machine was placed in the New York office and was used to film messages of intelligence interest.[158]

This arrangement continued without substantial disruption until 1963, when RCA Global began to store its message traffic on magnetic tapes. NSA made arrangements to obtain copies of these tapes from the RCA Global facilities in New York—they were taken "on loan," copied, and returned, the same day if possible. Gradually, magnetic tapes began to supercede paper tapes and microfilm as a means of storing messages. By 1966, the New York office was turning over only magnetic tapes to NSA.[159] The offices in Washington and San Francisco, however, continued to furnish copies of international message traffic for microfilming by NSA. RCA Global employees in Washington, D.C. were under the impression they were providing information only to the FBI.[160]

2. ITT World Communications

In August 1945, ITT agreed to allow the Army access to all incoming, outgoing, and transiting messages passing over the facilities of its subsidaries involved in international communications. It was agreed that "all traffic will be recorded on microfilm, that all Governmental traffic will be recorded on a second microfilm in addition to the original one, that these films will be developed by the SSA [Signals Security Agency], and the complete traffic will be returned to ITT." [161]

It is not clear whether these arrangements, agreed to at the outset, were actually implemented in the manner described. The ITT official with the earliest recollections of the program could recall only that by the early 1950s, ITT World Communications was providing NSA representatives with copies of the company's international message traffic, which NSA then sorted and microfilmed.[162]

When ITT World Communications began to use paper tapes to transmit its messages, these were turned over to NSA as well.[163] It is not clear whether these tapes were transmitted from the premises of

---

[155] Former vice president, RCA Global, 10/17/75, pp. 5–7.

[156] *Ibid.*, pp. 7–8, 11.

[157] Telegram from an AFSA officer to an AFSA officer, "RCA SHAMROCK," 6/24/51.

[158] Senior officer, RCA Global, 10/19/75, p. 4.

[159] *Ibid.*

[160] Van Riper, "Find U.S. Agents Spy on Embassies' Cables," *New York Daily News*, 7/22/75.

[161] Army intelligence officer letter to Commanding General, 8/24/45.

[162] Senior officer, ITT World Communications, 10/15/75, pp. 7–8.

[163] *Ibid.*, p. 8. A senior officer of ITT World Communications stated that he had no personal knowledge that paper tapes had been turned over to NSA; however, NSA confirmed that it had received paper tapes from ITT (testimony of Senior NSA official No. 4, 9/23/75, pp. 49–51). Counsel for ITT World Communications also told the Committee that his investigation had revealed that the company was providing paper tapes to NSA. (Counsel, ITT World Communications, 10/9/75, p. 1 (staff summary).)

ITT World Communications to another location (as with RCA Global) or whether they were simply transported to NSA for sorting.

When ITT World Communications began to use magnetic tapes to store its incoming and outgoing messages—the best recollection of this change places it around 1965 [164]—the magnetic tapes were turned over to NSA for duplication. They were returned to the company on the same day. By 1968, ITT World Communications was turning over only its magnetic tapes to NSA.[165]

The Washington and San Francisco offices of ITT World Communications participated in a similar fashion. In Washington, however, company officials believed that they were providing the telegrams to the FBI, rather than NSA. [166] It is clear from the information made available to the Committee that the Washington messages were sent to NSA.[167]

3. Western Union International

At the August 1945 meeting between Army representatives and the Western Union Telegraph Company (the parent company of Western Union International), the company stated that it

> desired that Western Union personnel operate the [microfilm] camera and do all the actual handling of the messages. It was agreed that [the Army Signal Security Agency] would furnish the necessary cameras and film for the complete intercept coverage of Western Union traffic outlets. The film, after exposure, will be delivered [to the office of a company vice-president], at which place an officer from the Signal Security Agency, in civilian clothes, will pick it up.[168]

The company agreed to implement this arrangement at its New York, San Francisco, Washington, and San Antonio facilities.[169]

This arrangement was apparently implemented as originally agreed. In New York, at least, company employees segregated such messages and processed them through a microfilm machine on the transmission room floor.[170] At approximately 4:00 each morning, an NSA courier would come to the floor to pick up the microfilm cartridge. In San Antonio, an Army signal officer from Ft. Sam Houston was tasked with picking up the microfilm each day.[171]

It appears that Western Union turned over to NSA only its telegraph traffic to one foreign country. Approached in 1959 by persons who identified themselves as being from Ft. Holabird, Maryland (Army intelligence), Western Union agreed to allow them to duplicate the traffic going to a particular country.[172] In 1970, the company also began to provide copies of messages going to a particular city within that country which were not being duplicated as part of the previous arrangement.[173] These messages were apparently sorted by

---

[164] Senior officer, ITT World Communications, 10/15/75, p. 8.
[165] Letter from an NSA courier to an NSA official, 1/23/68.
[166] Counsel, ITT World Communications, 10/9/75, p. 2 (staff summary).
[167] Tordella, 9/21/75, pp. 36–37.
[168] Army intelligence officer letter to Commanding General, 8/24/45.
[169] *Ibid.*
[170] Counsel, Western Union International, 10/10/75, p. 1 (staff summary).
[171] Memorandum for Record, Armed Forces Security Agency, "SHAMROCK Operations," 8/25/50.
[172] Counsel, Western Union International, 10/10/75, p. 2 (staff summary).
[173] *Ibid.*

NSA personnel in space provided by Western Union at its New York offices.[174]

Western Union International (which was formed in 1963) continued to microfilm certain foreign traffic for NSA until about 1965, when a company executive discovered the existence of the microfilm machine on the transmission room floor. After ascertaining its purpose, he demanded that NSA renew its request to have this information in writing. He recalled that instead of submitting such a request, NSA simply had the machine removed.[175] This recollection, however, was not borne out by documents furnished by NSA. The documents showed that on February 2, 1968, a company vice president (not the one referred to above) had discovered the existence of NSA's Recordak (microfilm) machine in the Western Union transmission room. The machine was reported to the company president, who directed his employees to find out to whom the machine belonged and what the basis for the arrangement was. The NSA courier, when asked these questions by a Western Union International official on February 9, 1968, replied that he was from the Department of Defense and did not know what the basis for the arrangement was or what was being done with the microfilm being furnished.[176] Yet the documents do not reflect whether the Recordak machine was removed, either in 1965 or in 1968.

It is clear that NSA continued to receive duplicates of all messages to the foreign country referred to above until 1972; when again as a result of "discovery" by company officials, this procedure was halted. Although the original request for this intercept procedure had been made by "Holabird people" (Army intelligence), when the company attempted to contact someone regarding its termination, it was ultimately referred to NSA.[177]

Finally, Western Union International, unlike its competitors, never utilized magnetic tapes to store its message traffic. Accordingly, none was ever provided NSA.[178]

In effect, Western Union International's participation in SHAM ROCK ended by 1972.[179]

E. NSA's Participation

1. Origins and Early Development

From 1952 (when NSA first inherited the SHAMROCK sources) until 1963, microfilm and paper tapes originating with the sources were brought to NSA's headquarters at Ft. Meade, Maryland several times a week.[180] As noted above, some of these had undergone initial screening, either by NSA operatives or company employees. Even with this preliminary screening, however, the volume of messages which reached NSA daily was apparently quite large.[181]

---

[174] *Ibid.*
[175] Affidavit of senior officer, Western Union International, Inc., 10/16/75, p. 1.
[176] Letter from an NSA courier to an NSA official, 2/9/68.
[177] Counsel, Western Union International, 10/10/75, p. 2 (staff summary).
[178] *Ibid.*, p. 3.
[179] Tordella, 9/21/75, p. 53.
[180] Tordella, 10/21/75, p. 17.
[181] A former NSA official testified that NSA had received "literally miles and miles and miles of punched tape." 10/23/75, p. 49.

Several witnesses have told the Committee that during this period the sheer volume of traffic would have likely prohibited the selection of messages on the basis of content.[182] Messages which were selected out were passed on to NSA analysts, who screened them further.

2. The Switch to Magnetic Tape

The character of the SHAMROCK operation changed markedly with the use of magnetic tape. RCA Global was the first company to begin using such tape in the early 1960s.[183] NSA was notified of the changeover in early 1963 and, by 1964, was able to sort electronically the information provided by RCA Global against its selection criteria. This is significant because it meant that the telegrams of citizens whose names were on NSA's "watch list" could be selected for processing by NSA analysts.

From 1964 until 1966, magnetic tapes from RCA Global were brought to Ft. Meade daily and returned to New York the same day.[184] By 1965, ITT World Communications had also begun its changeover to magnetic tapes and was beginning to provide traffic in this form to NSA messengers.[185]

3. CIA Cover Support

To alleviate the administrative burden entailed by these daily round-trips, NSA in 1966 sought to find a place in New York City where the tapes could be duplicated.[186] NSA Deputy Director Tordella requested that the CIA provide "safe" space where this operation could be conducted. The CIA agreed to rent office space in lower Manhattan, under the guise of a television tape processing company, where the tape duplication process could be carried out.[187] CIA designated this project "LPMEDLEY."

The cover support began in November 1966 and lasted until August 1973, when CIA terminated its part of the program.[188] Tordella was told that the CIA General Counsel was "concerned about any kind of operation in which the CIA was engaged in the continental United States. Regardless of whether CIA was doing anything so small as renting an office, he said 'get out of it.' " [189] NSA subsequently moved its duplicating operation to new office space in Manhattan, where it remained until SHAMROCK was terminated in 1975.[190]

4. Control of the Program

Numerous NSA employees were aware of SHAMROCK, but responsibility for its conduct rested only with the Director, Deputy Director, and one lower-level managerial employee.[191] Throughout the program's existence, only two individuals occupied this lower-level

[182] See Tordella, 10/21/75, p. 20; testimony of former NSA official, 10/23/75, pp. 49–50.
[183] Staff summary of interview with NSA official No. 5, 10/24/75, p. 1.
[184] *Ibid.*
[185] *Ibid.*
[186] Tordella, 10/21/75, pp. 23–24; Senate Select Committee memorandum, "Review of CIA Documents re LPMEDLEY," 9/17/75.
[187] *Ibid.*
[188] Letter from an NSA courier to an NSA official, 11/27/66.
[189] Tordella, 10/21/75, p. 38.
[190] *Ibid.*
[191] *Ibid.*, p. 41.

managerial position: the first between 1952–1970; the other from 1970–1975.[192]

The manager was instructed to report directly to the Deputy Director of NSA regarding any problems with the companies. As a routine matter, this individual was in charge of the NSA couriers who traveled between New York and Ft. Meade; he usually received information regarding the SHAMROCK operation from these couriers rather than from the companies. The individual who held this position between 1952–1970 told the Committee that he met with company officials on only two occasions during this time, and both meetings were perfunctory.[193]

Both of the NSA employees who acted as liaison with the companies confirmed to the Committee that the companies had never asked what NSA was extracting from the materials provided, and that NSA had never volunteered this information. Neither of the lower-level employees knew what NSA did with the materials; they stated that the messengers who worked under them also had no knowledge of what was sorted from the telegrams.[194] It seems clear, therefore, that the companies never learned that NSA sorted anything except foreign traffic from the telegrams that the companies provided NSA.

Since none of the companies (treating them as separate from their parent corporations) engage in domestic communications, they could not have provided NSA with domestic traffic. The Committee has no evidence to show that NSA has ever received domestic telegrams from any source.

5. Consideration of SHAMROCK in Connection with the Huston Plan

Former NSA Deputy Director Tordella told the Committee that in 1970, in connection with the Huston plan,[195] the principals involved in this project—Helms of CIA, Sullivan of the FBI, Bennett of DIA, and Gayler of NSA—discussed the feasibility of the FBI's taking over the SHAMROCK program in order to obtain more information on internal unrest. The FBI did not want the responsibility, according to Tordella, and NSA did not want to jeopardize its own working relationship with the companies.[196] The idea was therefore dropped.

F. Termination of SHAMROCK

Operation SHAMROCK terminated on May 15, 1975, by order of Secretary of Defense James Schlesinger.[197] NSA claims that the program was terminated because (1) it was no longer a valuable source of foreign intelligence, and (2) the risk of its exposure had increased.[198]

---

[192] Staff summaries of interviews with NSA official No. 5, 10/24/75, p. 1; and former NSA employee, 10/24/75, p. 1.

[193] Former NSA employee, 10/24/75, pp. 1–2 (staff summary).

[194] *Ibid.* See also NSA official No. 5, 10/24/75, p. 2 (staff summary).

[195] The formulation and content of the Huston Plan are described in the Committee's report: "National Security, Civil Liberties, and the Collection of Intelligence: A Report on the Huston Plan."

[196] Tordella, 10/21/75, pp. 34–35, 47–49.

[197] Staff summary of interview with senior NSA official No. 3, 9/17/75, p. 1. The Committee also reviewed a handwritten memorandum from the Director of NSA, Lt. Gen. Lew Allen, Jr., dated May 12, 1975, which stated that the Secretary of Defense had decided that SHAMROCK should be terminated, effective May 15, 1975.

[198] Senior NSA official No. 3, 9/17/75, p. 3.

IV. NSA PERSONNEL SECURITY AND RELATED MATTERS

The Committee investigated the NSA Office of Security to examine personnel security activities which may have been conducted in an overzealous and, possibly, unlawful manner. These activities are not part of NSA's two primary missions—the collection of signals intelligence and the protection of United States communications. Although this subject area is more narrow than others investigated by the Committee, there are similiarities involving the protection of both the rights of citizens and the national security.

A. Background

The NSA Office of Security is responsible for safeguarding the security of NSA facilities, operations, and personnel, and for protecting classified materials from unauthorized disclosure. This Office also administers NSA's security clearance program and investigates suspected breaches of security by NSA employees. The CIA's Office of Security performs the same functions for that Agency.

Personnel in the NSA Office of Security are quick to point out that substantial intangible differences exist between the role of the CIA and NSA Offices of Security. In recent years, the NSA Office has not enjoyed the same high status within NSA that the CIA Office has had within its own organization. At least two factors appear to contribute to this difference. First, the work of an Office of Security investigator bears no similarity to that performed by the professionals conducting signals intelligence and communications security activities, which comprise the heart of NSA. Second, during the 1950s and 1960s, personnel security programs at NSA suffered some widely publicized failures, resulting in both prosecutions for espionage and actual defections to the Soviet Union by NSA employees.

These factors have impelled the Office in conflicting directions. On the one hand, its personnel are not expected, and ordinarily do not tend, to take actions on their own initiative that would exceed the normal bounds of keeping the Agency reasonably secure. On the other hand, failures in personnel security have occasionally generated intense public pressure (especially from the House Committee on Un-American Activities) to take extraordinary measures to protect that security.

A fair analysis of the incidents listed below, all of which are of dubious legality or propriety, requires an awareness of these dynamics. Like other Government officials, personnel in the Office of Security must be held responsible for their actions. Yet, like most people in the United States, they have been greatly sensitized by the Watergate scandal and the recent congressional investigations of the intelligence community to the need to protect civil liberties against dangerous encroachments in the name of "national security." In this section we disclose certain aberrations from that sensitivity, in the confidence that this disclosure will encourage its growth.

B. Questionable Activities

1. NSA Office of Security: Access to Files on American Citizens

From NSA's inception in 1952 until October 1974, a unit of the Agency outside the Office of Security maintained a large number of files on American citizens. At the time of the destruction of these

records, approximately 75,000 United States citizens were included. Unlike CIA's Operatons CHAOS, these files were not created for the purpose of monitoring the activities of Americans, but for carrying out NSA's legitimate foreign intelligence mission.[199]

Many circumstances could contribute to the creation of such a file, perhaps the most frequent being the mere mention of an American citizen's name in a communication intercepted by NSA. The files also included reports from other intelligence agencies, such as the CIA and military intelligence units, which mentioned the name of the citizen and were routinely forwarded to NSA. Materials from open sources, such as newspapers, were also in the files.

Until the files were destroyed, the Office of Security was often supplied with information from them when it was conducting background investigations on applicants for employment at NSA or when other persons were being considered for clearances to receive intelligence gathered by NSA. In effect, this meant that the Office of Security was a beneficiary of the vast communications intelligence apparatus of the entire Agency, a resource which is on an entirely different order of sophistication than the wiretapping capability of any police or security force in the nation.

(*a*) *CIA Access to NSA Files.*—The NSA files contained entries on many prominent Americans in business, the performing arts, and politics, including members of Congress. Although the Committee has no reason to believe that any person at NSA used them improperly, it has learned that for at least 13 years, one or more employees of the CIA worked full-time in these files, retrieving information for the CIA without any supervision from NSA. One of these CIA employees recalled, with varying degrees of certainty, checking in these files for the names of various well-known civil rights, antiwar, and political leaders.

It is likely, although the Committee is not in a position to so state, that some of the information obtained from NSA found its way into Operation CHAOS.[200]

NSA did not develop these files for any sinister reason. They were useful in many ways to conducting successfully NSA's legitimate communications intelligence functions. Nevertheless, the fact that CIA personnel used the files without NSA supervision to gather information on American citizens—during a period when the CIA was engaged in unlawful domestic activities aimed against many of those same citizens—illustrates the danger of maintaining such files. The massive centralization of this information creates a temptation to use it for improper purposes, threatens to "chill" the exercise of First Amendment rights, and is inimical to the privacy of citizens.

(*b*) *Destruction of Files.*—The Committee was informed by NSA that the files on American citizens were destroyed in 1974. At that time, a centralized information storage system for foreign names was set up in the intelligence community. This reorganization provided the impetus for a re-evaluation of the files on American citizens, and a consensus was reached that their usefulness did not justify the costs in time, money, and storage space.

---

[199] For a detailed discussion see the Committee's report on Operation CHAOS.
[200] Testimony of a CIA employee, 7/25/75, pp. 17, 25.

2. Failure to Purge "Suitability Files"

Like other Federal agencies, NSA maintains "suitability files" concerning its employees. These files, which are held by the Office of Civilian Personnel, constitute an interface between that Office and the Office of Security. The latter provides information to these files and has access to them. These files contain highly personal information which might show the kind of unreliability or vulnerability of an employee which could lead to compromises of classified information. According to NSA, the purpose of these files is to aid the Agency in providing counseling and other forms of assistance to individuals with personal problems, not to threaten or damage such employees. The Committee has no reason to believe that the information in these files has been misused. During its investigation, the Committee reviewed 50 of these files, selected on a random basis, with the names of all individuals deleted.

Since the information stored in these files is so personal, it seems reasonable to expect that its retention would be kept to the minimum necessary for the purposes of these files. Unfortunately, this policy does not seem to have been observed in the past. Much of the information is either many years old or simply irrelevant to the suitability of an individual for employment.

If a systematic effort had been made periodically to review these files and purge them of inappropriate or dated information, such notations would probably have been eliminated long ago. The establishment of such a system has now been undertaken by NSA. Although persons in sensitive positions at agencies such as NSA may be expected to sacrifice some degree of privacy to the need to protect national security, that sacrifice must be kept within reasonable bounds.

A related question is the access of employees to their own files. NSA regulations provide: "In no instance will employees be given access to their own Suitability File." [201] Nevertheless, with the recent implementation of the Privacy Act, employees may ask for, and be granted, access to their files. Since the Committee found that these files sometimes contain unsolicited and unsubstantiated statements from neighbors, spouses, and others, the Privacy Act should result in much of this information being purged.

3. Files on Nonaffiliates of NSA Who Publish Writings Concerning the Agency

The Office of Security maintained files on two individuals who have published materials describing the work of the National Security Agency. In one case, the relevant writings were published in the late 1960s; in the other case, much more recently.

By the time of the second case, NSA had gained some experience in dealing with publicity. The file on this person consisted mainly of checks with other Federal agencies to determine what information they possessed concerning the author, and the results of various internal NSA inquiries as to where the author might have obtained information. Nevertheless, the Office of Security did submit the author's name for inclusion on the NSA watch list. There is no evidence that this submission resulted in the dissemination of any international messages sent or received by the author.

[201] NSA Personnel Management Manual (NSAPMM), Section 2-7(c)(2).

In the earlier case, the Agency appears to have overreacted. NSA had learned of the author's forthcoming publication and spent innumerable hours attempting to find a strategy to prevent its release, or at least lessen its impact. These discussions extended to the highest levels of the Agency, including the Director, and resulted in the matter being brought to the attention of the United States Intelligence Board.

In the course of these discussions, possible measures to be taken against the author were considered with varying degrees of seriousness. The Director suggested planting disparaging reviews of the author's work in the press, and such a review was actually drafted. Also discussed were: purchasing the copyright of the writing; hiring the author into the Government so that certain criminal statutes would apply if the work were published; undertaking "clandestine service applications" against the author, which apparently meant anything from physical surveillance to surreptitious entry; and more explicit consideration of conducting a surreptitious entry at the home of the author. To the credit of those involved, none of these measures were carried out.

Other steps, however, were taken. The author's name was placed on the NSA watch list and various approaches were made to his publisher. The publisher submitted a manuscript of the work to the Department of Defense, apparently without the author's permission. Despite requests from NSA to halt publication or to make extensive deletions, publication took place with only minor changes, to which the author had agreed.

The most remarkable aspect of this entire episode is that the conclusion reached as a result of NSA's review of this manuscript was that it had been written almost entirely on the basis of materials already in the public domain. It is therefore accurate to describe the measures considered by NSA and USIB as an "overreaction."

4. Other Files Maintained by the Office of Security

Although the Office of Security does not maintain files today on persons not affiliated with the Agency, it has done so in the past. The Agency describes these files in the following terms:

> The maintenance of these files began in the late 1950s. In early 1974, approximately 2800 files concerning nonaffiliated organizations and personnel were destroyed in accordance with DOD Directive 5200.27. The files consisted of reports from the FBI and other intelligence, security and federal agencies as well as state and municipal agencies who maintained such records. Information was also obtained from the congressional records of the House Committee on Un-American Activities, and open source, commercial publications. These files were retained primarily as a reference source for security education purposes, as an aid to our personnel security process and to provide assessment regarding the vulnerability of this Agency to foreign intelligence activities and extremists activities which posed a threat to the NSA mission, functions and property.
>
> Of the 2800 files which were accumulated, the great majority concerned foreign controlled and subversive organizations cited by the Attorney General of the United States.

> These organizations were those advocating the overthrow of the U.S. Government, and the violent disruption of the orderly process of government, etc. The small percentage of files maintained on individuals concerned suspected espionage agents, extremists, anarchists, etc. These persons were both U.S. and foreign citizens.[202]

DOD Directive 5200.27 was first issued in March 1971, and it greatly restricted the discretion of Department of Defense units to retain such files. The Directive stated, however, that it was "not applicable to the acquisition of foreign intelligence information or to activities involved in ensuring communications security." [203] NSA's General Counsel interpreted this language as exempting NSA from the coverage of the Directive, and was supported in this opinion by a Deputy General Counsel in the Department of Defense.[204] Only in 1973 was NSA informed by the Defense Investigative Review Council (DIRC) that some of its activities were subject to the Directive. Once this was established, NSA took steps to comply, which included destruction of of the 2800 files.[205]

In April 1975, the DIRC conducted an unannounced inspection of the NSA Office of Security to ascertain its compliance with DOD Directive 5200.27. Although substantial compliance was found, the DIRC did note that the Office still maintained three files with some questionable entries. These files concerned "threats" to NSA functions and property; characterizations of organizations; and unsolicited inquiries and "cranks." [206] Since the time of the DIRC report, NSA has drastically reduced the amount of materials in these files.

The Committee did obtain from NSA copies of the files as they existed at the time of the DIRC inspection. As the DIRC report noted, the first two of these files contained some questionable entries. At the time of the inspection, the "threat" file still contained extensive information on a peaceful demonstration of less than 40 persons near NSA headquarters in 1974. Similarly, the "characterizations" file reflects the fact that in the past the Office of Security would prepare a characterization of almost any organization that an NSA employee wanted information about before joining it or otherwise becoming involved. The characterizations were prepared largely on the basis of NSA's own files and from information supplied by other agencies.

It appears that DOD Directive 5200.27 and its enforcement through the DIRC mechanism are functioning effectively at this time to prevent the excessive accumulation of files on American citizens.

5. Office of Security Participation in Watch List Activity.

In his testimony before the Committee, NSA Director, General Lew Allen, Jr., detailed the efforts made by the Agency to intercept communications to and from certain American citizens from the late 1960s until 1973.[207] Not all of the names "watch listed" under this program

---

[202] NSA Response, 8/25/75, p. 4.
[203] DOD Directive 5200.27, 3/1/71, section II.B. See the Committee's report: "Improper Surveillance of Private Citizens by the Military," for a detailed discussion of this directive.
[204] *Ibid.*
[205] NSA Response, 8/25/75, p. 1.
[206] *Ibid.*, Tab 3, p. 6.
[207] Hearings, Vol. 5, pp. 1–46.

were submitted to NSA from the outside. The Office of Security also submitted approximately 13 names for monitoring.

Of these names, 11 had some present or past affiliation with NSA. Each of these 11 individuals had either defected to the Soviet Union, been convicted of espionage, were suspected of some other connection to an unfriendly power, or had made threats against NSA or its Director. Two of the names were of American citizens not affiliated with NSA. As described earlier, these two persons had published writings in this country about the Agency's activities, causing the Office of Security concern about the possible compromise of classified information.

The Government does have a continuing legitimate interest in the communications of defectors and suspected enemy agents, and should be permitted to intercept such communications if the proper procedures (e.g., a warrant or approval of the Attorney General) are established. The danger in allowing the Office of Security to place names on a watch list is that the decision as to whether the activities of a particular individual are sufficiently suspicious to justify intrusion into the privacy of his communications is left in the hands of an interested party: the Office of Security itself. The inclusion of the names of two persons not affiliated with the Agency—neither of whom was seriously suspected of any intent to aid a foreign power and each of whom was directly exercising First Amendment freedoms—illustrates the tendency of limited infringements of privacy to be extended to an ever-widening scope. Only the involvement of a neutral third party can help safeguard against such extensions.

6. Conventional Electronic Surveillance and Surreptitious Entries

For many years, the Office of Security has scrupulously avoided the use of conventional electronic surveillance off NSA premises. It has neither tapped any telephones nor engaged in any bugging of rooms outside the Agency since 1958.

In the late 1950s, four instances of electronic surveillance without a court order did take place. Three of these incidents transpired at the residences of present or former NSA employees. The fourth occurred in a New York City hotel room occupied by one of those same persons. The subjects of surveillance ranged from persons convicted of espionage activities to persons friendly with diplomatic personnel of unfriendly foreign powers and/or homosexuals. The duration of the coverage varied from a few days to three months.

The technology of the bugging devices used by the Office of Security in the late 1950s was such that they could only be installed by trespassory means. Each of the above instances thus involved a surreptitious entry at the place being bugged. Moreover, the devices were battery operated; in the case of a surveillance lasting three months, periodic re-entries were necessary to charge the batteries powering the device.[208]

In addition, the Office of Security conducted four surreptitious entries in the early 1960s which were unrelated to electronic surveillance and which did not involve warrants. The entries involved two defectors to the Soviet Union (Martin and Mitchell), an employee suspected

[208] Staff summary of an interview with NSA Office of Security official, 8/8/75.

of taking classified documents out of NSA, and an employee who had contact with an embassy of an unfriendly foreign power.

With the passage of many years since these relatively isolated incidents, it is difficult to ascertain the levels at which they were approved. Both past and present Directors of Security at NSA have stated that they would not have taken place without the approval of the person holding that position, and that at the time of these incidents the Director of Security enjoyed such a close working relationship with the Director of NSA that the surveillance would not likely have occurred without the Director's knowledge.[209]

7. "External Collection Program"

In 1963, after a review of the Office of Security's counterintelligence program by the Office and the Director of NSA, several steps were taken to strengthen the program. Among these was the establishment in October 1963 of an "External Collection Program." [210] It appears that this "program" was, from its beginning, highly informal. Office of Security personnel had only vague and conflicting recollections as to what it had consisted of or how long it had lasted.

Most did recall that the program included brief periodic visits to bars, restaurants, and other establishments in the vicinity of NSA headquarters by Office of Security personnel. These visits were made to determine where NSA employees gathered after hours, whether they discussed classified information, and whether agents of hostile intelligence services also frequented these locations. The program also involved an effort to encourage persons working in these establishments to report any suspicious incident to NSA and to make the local police aware of the sensitivity of NSA's mission.

Since the revelant documents were destroyed in 1973, the Committee has been unable to establish whether the External Collection Program was used to gather information on persons other than NSA employees and foreign agents. The Office of Security, in fact, soon discovered that it lacked the personnel to carry on such a program, and it died quietly "in approximately 1966–1967." [211]

---

[209] Staff summary of an interview with NSA Office of Security official, 8/22/75.
[210] NSA response of 9/30/75 to Senate Select Committee letter of 9/3/75.
[211] *Ibid.*