DRAFT

WRITTEN

INTERCEPTION OF INTERNATIONAL TELECOMMUNICATIONS BY THE NATIONAL SECURITY AGENCY

STET

Report by The
Committee on Government Operations

Introduction:

The federal intelligence agency which is subject of this report is the National Security Agency (NSA). Official published estimates of its size in dollars expended or manpower employed, by either the Legislative or Executive branches, do not exist.[1] Unofficial estimates are that the NSA annually spends as much as $15 billion and employs up to 120,000 persons, when military agencies under the NSA's direction are included.[2] Whatever its actual budget and personnel levels, it has, through a network of over 2,000 specialized intercept positions around the world, the technological capability to intercept a significant portion of worldwide telecommunications. This capability can be brought to bear against any country. If used against the American people, Senator Frank Church has noted, "no American would have any privacy left ... there would be no place to hide."[3]

The NSA was created by a seven-page Top Secret memorandum from President Harry S. Truman to Secretary of State Dean G. Acheson and Secretary of Defense Robert A. Lovett, on October 24, 1952. Under this directive, which even today remains classified, the NSA assumed the responsibilities of the Armed Forces Security Agency, which in turn had largely inherited the intelligence responsibilities of the Army Security Agency (which remains a functioning Army entity).[4]

The NSA's two basic functions, derived from Top Secret National Security Council and Director of Central Intelligence directives, are: (1) to protect the "Communications Security" (COMSEC) of U.S. telecommunications that are national security related; and (2) to obtain foreign intelligence related telecommunications through the interception of "Signals Intelligence" (SIGINT).

SIGINT interception is the NSA's dominant activity. It consists of "Communications Intelligence" (COMINT), or intelligence obtained through the interception of electronic message communications (such as telegrams and telephones),[5] and "Electronic Intelligence" (ELINT), intelligence obtained through the interception of electronic signals (such as radar and missile emissions), which were not

intended by the sender to communicate messages.

This report is primarily concerned with ~~one type of~~ the USA's COMINT activity ~~under-taken in the past by NSA~~ ~~the interception of international telegrams~~ areas of written telecommunications 5a/ -- and how this activity affects the constitutionally guaranteed right of privacy of American citizens. This report also notes, to a lesser extent, one COMSEC activity that extends beyond the "protection" of communications related to national security, that may likewise encroach on the privacy of American citizens.

Background:

Prompted by a press report,6/ the Subcommittee on Government Information and Individual Rights initiated in August 1975, an investigation into the interception and monitoring by federal intelligence agencies, of telegrams and other forms of data transmissions entering and leaving the United States. The investigation was undertaken pursuant to the subcommittee's oversight responsibility for matters concerning the rights of privacy of American citizens and for the operations of the Federal Communications Commission. Public hearings were held on October 23, 1975, and February 25, March 3, 10, and 11, 1976. (Hereafter cited as Subcommittee Hearings.) These hearings were conducted in the face of intense Executive branch efforts to have them curtailed or postponed.7/

Similar pressure was exerted on the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities. (Hereafter referred to as the Church Committee and cited as the Church Committee Hearings and Church Committee Final Report.) On October 7, 1975, Attorney General Edward Levi personally asked Senator Church on behalf of the President to postpone committee hearings on selected National Security Agency activities, scheduled for October 8 and 9, at which NSA Director Lew Allen, Jr. was to testify. The Church Committee agreed to delay Gen. Allen's appearance indefinitely.

Whereas the Church Committee had conducted its NSA investigation by going directly to that Agency, the subcommittee approached no government agency, going instead to the international telegraph companies who allegedly had participated in such activities. These companies were initially responsive. It was apparently not until October 21, 1975 -- two days prior to the subcommittee's initial hearing -- that the Administration became aware of the subcommittee's investigation, at which time it reacted strongly. On that day, the subcommittee received a letter from FBI Director Clarence Kelley, advising that a former FBI special agent, whom the subcommittee staff had interviewed, would not be allowed to testify.8/ On the

same day, as a result of government pressure, the two largest international common carriers involved -- RCA Global Communications and ITT World Communications -- suddenly withdrew their offers to appear voluntarily and demanded that they be issued subpenas as a condition to their testifying. (A representative of ~~the author~~ communications carrier ~~involved in international~~ subsequently informed the subcommittee that highly placed Justice Department officials, immediately prior to the subcommittee's October 23 hearing, had urged the company to demand subpenas. The company did not accede to the Executive branch request~~s~~.) ~~however.~~

On October 22, 1975, the subcommittee Chairwoman, Representative Bella S. Abzug, was visited by ~~a delegation of Executive officials consisting of~~ Deputy Attorney General Harold Tyler, NSA Director Allen, Assistant Secretary of Defense for Intelligence Albert Hall, Special Counsel to the President Jonathan Marsh, and White House Congressional Liaison Charles Leppert, who requested the hearings not be held on grounds of either jeopardizing an ongoing Justice Department criminal investigation or ~~or~~ jeopardizing national security.

On October 23, moments before the subcommittee's hearing was to begin, Attorney General Levi unexpectedly arrived at the hearing room, bearing the same message. Like the previous visitors, Mr. Levi could not say which "national security" interests were being jeopardized, nor suggest to the subcommittee any course of action beyond postponement or cancellation. The subcommittee's hearing proceeded as scheduled, but former FBI special agent Joe R. Craig, and representatives of RCA Global Communications and ITT World Communications refused to testify unless subpenaed. Testimony was taken from representatives of American Telephone and Telegraph Company and one of its operating subsidiaries, the Chesapeake & Potomac Telephone Company.

Within two hours of the close of the subcommittee's October 23 hearing, the Church Committee reversed its earlier decision and voted to hold public hearings on the NSA.

On October 29, NSA Director Allen, accompanied by NSA Deputy Director Benson Buffham and NSA General Counsel Roy Banner, appeared before the Church Committee in public session, essentially confining their testimony to the Agency's "watch-list" activity (see p.). A second matter raised at the hearing, identified as Operations SHAMROCK (see p.), was temporarily put off.

On November 6, in public session, Senator Church read the committee's SHADOCK report, a summary of the Church Committee's investigation to date, into the record.[9] No testimony, however, was elicited in public session.

The Church report primarily dealt with contacts between U.S. telegraph companies and government representatives between 1947[10] and 1975, and procedures by which private communications entrusted to the carriers were turned over to the NSA and, to a lesser extent, the FBI. The report did not discuss how the information made available to the intelligence agencies was utilized by its collectors, or to whom it was disseminated, or the uses made of it by those entities -- subjects of vital interest to this Committee.

On February 4, 1976, this Committee issued subpenas ad testificandum and subpenas duces tecum to three FBI special agents, one former FBI special agent, one NSA employee, and executives of ITT World Communications, RCA Global Communications, and Western Union International. On February 17, President Ford instructed Secretary of Defense Rumsfeld and Attorney General Levi "to decline to comply with the subpenas" directed to the government and government witnesses, stating that disclosure of the records sought by the Committee were not in the public interest.[11] Immediately, Secretary Rumsfeld instructed the NSA employee, and Attorney General Levi instructed the FBI employees, that the Committee's subpenas duces tecum were not to be complied with, inasmuch as "President Ford has asserted executive privilege."[12] On February 17, Attorney General Levi also requested "that Western Union International honor [President Ford's] invocation of executive privilege, and that it not produce and deliver documents described by the said subpenas."[13] These applications of "executive privilege" to private corporations and to former government employees, were unprecedented expansions of that concept.

On February 25, the aforementioned former FBI employee, three current FBI agents, and one NSA employee appeared before the subcommittee, but refused to testify. Both the present and former FBI agents refused to testify on instructions from the Attorney General, while the NSA employee refused on orders from the Deputy Secretary of Defense, William P. Clements, Jr. Because of their failure to give testimony, the subcommittee recommended that all five be cited, pursuant to 2 U.S.C. 192, for contempt of Congress. Four of the witnesses were also recommended for contempt citations for their failure to produce documents pursuant to subpenas.

On March 3, the Executive Vice President of Western Union International testified before the subcommittee, and turned over an eight year old list of NSA targets, the production of which President Ford had attempted to block by asking the corporation to honor his claim of "executive privilege."

Attorney General Levi also asked RCA Global Communications that its representatives neither testify before the subcommittee, nor produce documents, "until procedures can be agreed upon to assure that the President's invocation of executive privilege is not effectively undone."[14/]

Without procedures being "agreed upon", representatives of RCA Global Communications did testify on March 3, as well as on March 10, and subsequently turned over to the subcommittee additional records that the company had previously considered as not covered by the subcommittee's subpena duces tecum.[15/] Also on March 10, the subcommittee received the testimony of the Chairman of the Federal Communications Commission, Richard E. Wiley.

On March 11, representatives of ITT World Communication, which did not receive an "executive privilege" request from Attorney General Levi, testified before the subcommittee.

PART I

CHRONOLOGY OF U.S. TELEGRAPH COMPANIES' COOPERATION WITH FEDERAL INTELLIGENCE AGENCIES

Pre-World War II

I. History

During World War I, U.S. government intelligence agents censored telegraphic telecommunications by working in the offices of private telegraph companies. All telegrams entering or leaving the United States were placed at the disposal of a military intelligence unit of the War Department known as MI-8 [Military Intelligence - Section 8].[16/] This practice ceased soon after the conclusion of the war.[17/]

MI-8, from its inception in 1917, had been directed by Herbert Osborne Yardley, considered by some cryptologists to be the most famous in history. At war's end, faced with the phasing out of his organization, and envisioning its having a peacetime role, Yardley, in May 1919, convinced the State and War Departments to approve a plan for a "permanent organization for code and cipher investigation and attack."[18/] Forty thousand dollars of the organization's $100,000 annual budget was to come from State Department special funds, with

the balance to come from military intelligence budgets after selected Congressional leaders had been briefed on the project.19/

Although supported by government funds, the resulting organization had no visible government connection. Known as "The Black Chamber" by the few persons familiar with its existence, it operated, from 1919 until 1929, under Yardley's leadership in New York City -- under the cover name "Code Compilation Company."20/ The operation was initially situated in townhouses in the East Thirties, but following a 1925 break-in in which desks were rifled, it was moved to a large Manhattan office building.

In 1929, President Hoover's newly appointed Secretary of State, Henry L. Stimson was shocked to learn of the Black Chamber's existence and abruptly terminated the operation 21/ in the belief its activities were shameful in a "world [that] was striving with good will for lasting peace."22/

Suddenly without a job and in need of funds, and apparently believing that since the Black Chamber had been destroyed there was no longer any valid reason for withholding its secrets, Yardley wrote a book, The American Black Chamber, published in 1931, which soon became an international best-seller. In it Yardley boasted:

> We solved over forty-five thousand cryptograms from 1919 to 1929, and at one time or another, we broke the codes of Argentine, Brazil, Chile, China, Costa Rica, Cuba, England, France, Germany, Japan, Liberia, Mexico, Nicaragua, Panama, Peru, Russia [sic], San Salvador, Santo Domingo, Soviet Union and Spain.23/

The Black Chamber, he stated,

> also made preliminary analyses of the codes of many other governments. This we did because we never knew at what moment a crisis would arise which would require quick solution of a particular government's diplomatic telegrams. Our personnel was limited and we could not hope to read the telegrams of all nations.24/

Despite his proclivity towards sensational disclosure, Yardley coyly avoided stating how, in the ten years of MI-8's peacetime existence, from 1919 to 1929, the Black Chamber had obtained telegrams it had analyzed:

> We employed guards, replaced all the locks and were ready to begin [in 1919] our secret activities. But there were now no code and cipher telegrams to work on! The cable censorship had been lifted and the supervision of messages restored to the private cable companies. Our problem was to obtain copies of messages. How?
>
> I shall not answer this question directly. Instead I shall tell you something of the Soviet Government's type of espionage as revealed by documents that passed through my hands. After you read these, you can draw your own conclusions as to how the United States Government obtained the code and cipher diplomatic messages of foreign governments.25/

However, this question was answered in a letter Yardley sent to his publisher on March 18, 1931.[26/] There he wrote that none of the messages alluded to in the manuscript of The American Black Chamber,

> other than certain wireless messages exchanged between Germany and Mexico, were sent by radio. They came by cable. With respect to every cablegram referred to in such book, the copies thereof to which I refer therein were obtained by the consent and authority of the respective presidents of the Western Union Telegraph Company and of the Postal Telegraph Company over the wires of one or the other of such companies such messages were transmitted. [Emphasis added.]

In the 1920's, these two companies carried almost all the telegraphic communications in and out of this country.[27/]

According to Yardley's book, only coded messages were turned over to MI-8; plain text (i.e. uncoded) messages were never made available.[28/]

The Army Security Agency's 323 page Historical Background of the Signal Security Agency 1919-1939, which the subcommittee requested and received in sanitized form, omits any mention of the arrangement described by Yardley, whereby MI-8 received telegraph messages from the Western Union and Postal Telegraph companies, or any other company. It suggests only that the Army Signal Corps did not continue to support the MI-8 activities:

> Plans for establishing MI-8 on a peace-time basis in 1919 included no provision for the development of facilities for obtaining the necessary intercepted messages. A detailed account of the situation will be given shortly but at this point it will suffice to indicate that it was doubtless assumed that the cable companies would continue to supply copies of all messages passing through their offices and that the Signal Corps would continue its war-time intercept facilities which would be at the call of MI-8. These assumptions proved to be unwarranted. That no satisfactory solution for this problem was ever reached was one of the prime causes for the decline of activity of MI-8 in New York. It was also one of the factors which led to the absorption of the Bureau by the Signal Corps, an organization which could more easily develop intercept facilities.[29/]

The "detailed account" of the cable companies' cooperation, suggested in this passage, was deleted from the manuscript provided the subcommittee. If Yardley's account is accurate, however, MI-8 did remain operational for ten years after World War I with the cooperation of the telegraph companies heretofore identified. Furthermore, it was Secretary Stimson's philosophical objections, and not the reluctance of the telegraph companies, which apparently brought the activities of MI-8 to a halt in 1929.

II. Legality[30/]

When World War I ended, the Radio Communications Act of August 13, 1912, which provided that the Government would guarantee the secrecy of communications, was still in effect. That Act provided, in pertinent part:

> No person or persons engaged in or having knowledge of the operation of any station or stations shall divulge or publish the contents of any messages transmitted or received by such station, except to the person or persons to whom the same may be directed, or their authorized agent, or to another station employed to forward such message to its destination, unless legally required so to do by the court of competent jurisdiction or other competent authority.31/

This law did not prohibit the interception of radio traffic per se, but merely prohibited the employees of common carriers covered by the Act from divulging or publishing the contents of messages to unauthorized persons. Although no court had occasion to so rule, the prohibition contained in the statute would seem to have been violated by those employees of the cable companies who divulged the contents of telegrams to MI-8, unless MI-8 could have been considered as "other competent authority". This point has never been the subject of a judicial determination.

The 1912 statute remained in effect until the enactment of the Radio Act of 1927, which considerably broadened the prohibition against unauthorized disclosures:

> No person receiving or assisting in receiving any radio communication shall divulge or publish the contents, substance, purport, effect, or meaning thereof except through authorized channels of transmission or reception to any person other than the addressee, his agent or attorney, or to a telephone, telegraph, cable or radio station employed or authorized to forward such radio communication to its destination, or to proper accounting or distributing officers of the various communicating centers over which the radio communication may be passed, or to the master of a ship under whom he is serving, or in response to a subpoena issued by a court of competent jurisdiction, or on demand of other lawful authority; and no person not being authorized by the sender shall intercept any message and divulge or publish the contents, substance, purport, effect or meaning of such intercepted message to any person; and no person not being entitled thereto shall receive or assist in receiving any radio communication and use the same or any information therein contained and no person having received such intercepted radio communication or having become acquainted with the contents, substance, purport, effect, or meaning of the same or any part thereof, knowing that such information was so obtained, shall divulge or publish the contents, substance, purport, effect, or meaning of the same or any part thereof, or use the same or any information therein contained for his own benefit or for the benefit of another not entitled thereto . . . . [Emphasis added.]32/

Whereas the 1912 Act had applied only to employees of common carriers, the 1927 Act applied to all persons not authorized by the sender to receive such communications. This would bring MI-8, as well as the employees of the cable companies, under the Act's prohibition. The Army Security Agency's historical record states that the law's "or on demand of other lawful authority" provision had never been used by MI-8 to justify its interception of foreign diplomatic traffic. Apparently, there was never a need for MI-8 to assert such authority.

Hence, subsequent to 1927 at least, the Black Chamber apparently operated in violation of the law.

The Army Security Agency's historical record suggests, on the other hand, that the activities of military intelligence gathering - including MI 8's -- were not intended to be covered by the 1927 Act's prohibitions:

> The purpose behind the legislation was of course, the security of communications from the danger of interception by unauthorized persons who might have made use of intelligence contained therein for personal profit. That the laws would also hamper Governmental agencies engaged in the production of intelligence upon which the safety of the United States might be based was probably far from the minds of the legislators. Indeed, prior to World War I, no such agency existed, and until 1931, the fact that one had existed during the war period was unknown either to the general public or to most officers in the Army itself.
>
> On the other hand, inclusion in these acts of specific exemptions permitting the interception of radio communications for the purposes of military intelligence would have given notice to the world in general, and therefore to a possible enemy in particular, that cryptanalytic units were indeed operating. Such a course would have been highly undesirable. What solution this thorny problem could have had is not clear: the fact that no solution was ever reached constituted one of the greatest obstacles to the proper functioning of MI-8.[33]

Yardley infers that the 1929 Act presented no obstacle at all. It was simply ignored.

III. Government Reaction to Yardley Disclosures

The publication of Yardley's book, in 1931, prompted the War Department to state that the American Black Chamber had not existed for four years (a date which coincided with the passage of the Radio Act in 1927).[34] General Douglas MacArthur, then Army Chief of Staff, said he did not know anything about it, while high officers in the intelligence divisions said no such bureau then existed and they professed to have no knowledge of it in former years.[35] State Department officials similarly said they were sure there had been no such practice and one official, speaking on behalf of Secretary Stimson, said he had never heard of any such organization as the so-called "black chamber."[36]

Yardley, a man who had been revered as a cryptanalytic genius, and who, in 1922, had been awarded the Distinguished Service Medal by the Secretary of War,[37] was portrayed in official commentaries as an opportunist and braggart whose actions bordered on treason.

The Army Security Agency history, written in 1946, described Yardley as a man who "had demonstrated a certain amount of cryptanalytic ability and had achieved within the War Department a reputation as a cryptanalyst." He was, the report stated, a poor administrator who had "neither the initiative nor foresight to build MI-8 on a firm foundation." He ignored his duties, the report continued, "while he profited from real estate activities; his enthusiasm for cryptanalysis lagged as he became a consultant in more profitable code production activities for commercial firms. Then, when his own position was abolished, he divulged information of the highest secrecy and made himself notorious in the annals of cryptology."[38/]

In 1932, Yardley wrote a new book entitled "Japanese Diplomatic Secrets" that was never published. On February 20, 1933, U.S. marshals in New York seized the manuscript in the publishing offices of The Macmillan Company, on the grounds Yardley, as an agent of the U.S. government, had appropriated secret documents.[39/] Yardley was never prosecuted, but his case prompted Congress to enact the "Protection of Government Records" bill in 1933. Now codified as 18 U.S.C. 952, the law makes disclosure of diplomatic codes or correspondence a felony.

IV. Assessment of MI-8 by the Army Security Agency.[40/]

According to the Army Security Agency's historical chronology, MI-8 primarily failed because "its principal support was derived from a department of the government which reflected political changes and the temper of the times more directly than does the War Department." In other words, such a sensitive activity as MI-8 was not to be entrusted to the political whims of the country's civilian leadership. The Army Security Agency, in hindsight, also saw other reasons for MI-8's demise:

(1) Its leader was not sufficiently concerned with its secrecy (though there is no evidence Yardley compromised the secrecy of the "Black Chamber" in any way, during its twelve year existence).

(2) Its isolation from direct supervision as a result of its transfer to New York produced neither the desired secrecy nor the attention it should have had from the War Department (though there was every evidence, from Yardley's narration, its existence was well known at the highest State and War Department levels).

(3) The separation of cryptanalysis (breaking the codes and ciphers of foreign governments) and cryptography (making codes and ciphers for one's own government) was a mistake. (MI-8 was not involved in cryptography).

Even before MI-8 formally terminated its operations on October 31, 1929, the War Department had formed the Signal Intelligence Service within the Agency to carry out most cryptological work on a continuing basis. By State Department defaults, most cryptological work was shifted to the Army in a single organization [illegible] — a precursor to the Armed Forces Security Service and its successor, the National Security Agency.

Post World War II

I. History

During World War II, U.S. government agents pursuant to the wartime powers of the President, again censored written telecommunications by working in the offices of the telegraph companies. Three companies -- ITT Communications, RCA Communications, and Western Union -- transmitted almost all international cablegrams and radiograms entering or leaving the United States. All such messages were placed at the disposal of military intelligence.41/

However, the War Department's post-World War II actions to convince the cable companies to make international telegrams available to federal intelligence agents were markedly different than those taken after World War I. The post World War I period was marked by inaction: six months after the Armistice, Herbert Yardley had to single-handedly persuade the government to enter into such an arrangement and his scheme provided that only coded messages would be handed over. But in August 1945, immediately after the end of the war, the Army Signal Security Agency (the same as the Signal Intelligence Service and Army Security Agency) implemented a plan that led ultimately to making most telegrams entering and leaving the United States -- including those in plain text -- available to that agency.42/ On August 18, 1945, four days after Japan surrendered, "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 approval of the interception of all [foreign] 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.'"43/ ITT and Western Union began their participation by September 1, 1945, and RCA by October 9, 1945.44/

While the Army Signal Security Agency was ostensibly only interested in the interception of foreign government traffic, in practice it was given access to all traffic. This was necessary, former RCA Executive Vice President Sidney Sparks testified, because the procedures initially proposed by the government -- that special electrical connections be put on certain tielines, or that tapes originating and terminating with certain tielines be turned over -- would result in a situation where "everybody and his brother would know just exactly what we were doing and why."[45/] To avoid that revelation, the government was given, according to Mr. Sparks, "all of the perforated tapes," i.e., access to all messages.[46/47/]

ITT also agreed to allow the Army access to all incoming, outgoing, and transiting messages -- private as well as governmental -- passing over the facilities of its subsidiaries involved in international communications. ITT agreed to record all such messages on microfilm, which the Army Signals Security Agency then developed.[48/]

For the next thirty years, between 1945 and 1975, RCA and ITT -- which together handled approximately 70 percent of all international non-verbal telecommunications in and out of this country -- continued to make all their customers' communications available to the NSA.[49/] Only the form in which these messages were turned over changed during this thirty-year period.

Western Union's procedure was far more selective. It insisted from the time it entered into the program in 1945, that its own personnel do the actual handling of all messages delivered. Moreover only messages to one foreign country initially were made available to NSA.[50/] At an undetermined later date, all foreign government telegrams were made available to NSA.[51/]

Western Union's participation was also of shorter duration. In 1963, Western Union divested itself of its international operations, which were taken over by Western Union International, an independent company formed for that purpose. Sometime between 1965 and 1972, an NSA Recordak machine located in the company's New York operations room which company employees used to copy foreign government messages, was removed at the company's request.[52/53/]

The subcommittee has no evidence that, after World War II, the Army Security Agency -- or, in 1952, its successor agency, the NSA -- made any attempts to limit its "take" to coded messages from the telegraph companies, as was done by Herbert Yardley's MI-8 organization after World War I. Both coded and uncoded messages were received and analyzed, seemingly in violation of the 1958 National Security Council Intelligence Directive (NSCID number 6, dated September 15, 1958) setting out the functions of the NSA:

> For the purpose of this directive, the terms "Communications Intelligence" or "COMINT" shall be construed to mean technical and intelligence information derived from foreign communications by other than the intended recipients.
>
> COMINT activities shall be construed to mean those activities which produce COMINT by the interception and processing of foreign communications passed by radio, wire, or other electromagnetic means, with specific exception stated below, and by the processing of foreign encrypted communications, however transmitted. Interception comprises search, intercept, and direction finding. Processing comprises range estimation, transmitter operator identification, signal analysis, traffic analysis, cryptanalysis, decryption, study of plain text, the fusion of these processes, and the reporting of results.
>
> COMINT and COMINT activities as defined herein shall not include (a) any intercept and processing of unencrypted written communications, press and propaganda broadcasts, or (b) censorship. [Emphasis added.]

The NSA contends that the specific exclusion of unencrypted written communications, which would appear to prohibit its interception of telegrams, "is and always has been limited to mail and communications other than those sent electronically."[54/] Hence, the NSA appears to have interpreted this directive as a carte blanche to intercept and process all foreign communications, i.e., all those in which at least one terminal is foreign, even though such communications were unencrypted. SU-A/

Footnote 54-A (p. 13)

> Former CIA Director Allen Dulles has defined communications intelligence as "information which has been gained through successful cryptanalysis of other people's traffic." He has defined cryptanalysis as certain codes and ciphers that can be the mathematical analysis of intercepted traffic. (Allen Dulles, The Craft of Intelligence, Harper & Row, 1963; p. 73). Dulles' characterization of COMINT excludes the utilization of plain-text messages.

Operation SHAMROCK, the code name under which the cable companies made most of their international telecommunications traffic available to the NSA, and to a lesser extent to the FBI, was terminated by the Secretary of Defense in May 1975 -- a date coinciding with the Church Committee's first demonstration of interest in the program. The "take" from Operation SHAMROCK -- plus from other NSA operations -- was used by the NSA in the 1960s and early 1970s to compile files on American citizens. NSA maintained a "watch-list" of names of individuals and organizations against which the "take" was sorted.

MINARET was the code name applied to the NSA's efforts to protect its watch-list activities on American citizens from disclosure. The watch-list had actually begun in the early sixties but the MINARET restrictions on disclosure were not applied until 1969.[55/] The MINARET charter described the watch-list program as involving "communications concerning individuals or organizations involved in civil disturbances, anti-war movements/demonstrations and military deserters involved in anti-war movements."[56/] MINARET was considered so sensitive that information being disseminated was classified TOP SECRET and labeled "Background Use Only," and while handled as SIGINT and distributed to SIGINT recipients,[57/] it was specifically not identified as having any NSA connection.[58/59/] On May 12, 1976, material collected under the NSA watch-list program was transferred to the office of the Principal Deputy Assistant Secretary of Defense for Intelligence, Thomas K. Latimer, for safekeeping.[60/] The MINARET files remain, as of March 1, 1977, in a safe in Mr. Latimer's office, retained pending a request for their production in a civil litigation.[61/]

Also utilizing the telecommunications intercepted under Operation SHAMROCK, the NSA's Office of Security maintained approximately 75,000 files on American citizens between 1952 and 1974.[62/] These files were apparently created from information obtained through SHAMROCK and NSA's other intercept programs. Persons included in these files included civil rights leaders, antiwar activists, and Members of Congress. For at least 13 years, CIA employees were given unrestricted access to these files, and one or more worked full time retrieving information that presumably was contributed to the CIA's Operation CHAOS, which existed from 1967 to 1974. The Committee does not know to which component of the CIA the NSA's Office of Security files on American civilians were transferred prior to 1967, nor by what authority these transfers were made. The Committee is disturbed by the CIA's apparently receiving information on American citizens on an established and regular basis, several years prior to the heretofore believed commencement date of that Agency's domestic surveillance activities. According to the NSA, its Office of Security files on American citizens were destroyed in 1974.[63/]

While the Committee has no reason to believe SHAMROCK continues today, i.e., that the NSA, or its representatives, is involved in hand-to-hand acquisition of international telecommunications, the Committee cannot report that the NSA no longer intercepts such messages by electronic means. Indeed, one can argue that if it were not, it would not be doing its job of intercepting foreign government telecommunications.[64/] The NSA has -- and has had for several years -- the technical capability and resources to accomplish this task without the knowledge or complicity of the cable companies;[64a/] thus, from the NSA's point of view, a program such as SHAMROCK is no longer an operational necessity.

[II. Legality - Britt insert]

64a/ See, for example, testimony of William Colby, "Central Intelligence Agency Exemption in the Privacy Act of 1974" hearings, House Subcommittee on Government Information and Individual Rights, June 25, 1975 (pp. 223-24).

II. The Legality of SHAMROCK

The Fourth Amendment to the Constitution guarantees to the people the right to be secure...in their papers...against unreasonable searches and seizures." It further provides that "no Warrants shall issue, but upon probable cause."

The fact that NSA, and its predecessors, indiscriminately obtained without a warrant copies of virtually every international telegram leaving the United States for a period of thirty years would appear to violate this constitutional guarantee of privacy. The Supreme Court has held consistently that official searches may violate the Fourth Amendment if they are not reasonably limited to the accomplishment of some legitimate governmental purpose.[65] Even assuming the collection of foreign intelligence to be a legitimate governmental purpose, the fact the NSA did not limit its interceptions to the telegrams of foreign governments, or even to those which were relevant to foreign intelligence requirements, but rather intercepted all international telegrams regardless of their source or subject matter, suggests this constitutional standard was violated.

The interception of international telegrams also appears to have violated section 605 of the Communications Act, enacted eleven years prior to the commencement of SHAMROCK, although this point has never been the subject of a judicial determination. As set forth at page , supra, that section prohibited employees of common carriers, as well as any other person "not being authorized by the sender", from intercepting and divulging the contents of telegrams, except in certain specified situations. The exception most relevant here allowed for publication "on demand of other lawful authority." However, no court decision prior to the start of SHAMROCK had interpreted this phrase to mean anything other than some form of official process.[66] In particular, no federal intelligence agency had ever been designated by any court as "other lawful authority" under this section,[67] nor did the legislative history of the Act indicate that such an interpretation was intended.[68]

It is, furthermore, important to note that the international telegraph companies which participated in SHAMROCK did not themselves interpret the "other lawful authority" exception to section 605 as legal justification for their participation.[69] To the contrary, they informally sought to have section 605 amended to permit, as a matter of law, the actions which they were being asked to undertake by the government.[70] They agreed to participate in SHAMROCK, nonetheless, upon the assurances of the Attorney General and the President that they would not be prosecuted under the provisions of section 605.[71] Whether these high-level assurances would satisfy the legal requirement of section 605, i.e., would constitute "demands of other lawful authority", has never been the subject of a judicial determination.

Section 605 essentially remained in its original form until 1968, when it was amended to read in pertinent part:

> "Except as authorized by chapter 119, title 18, 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, except through authorized channels of transmission or reception...on demand of other lawful authority. No person not being authorized by the sender shall intercept any radio communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person...(emphasis added)"

Chapter 119 of title 18, cited in this section, provided in pertinent part: "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 for the security of the United States."[72]

Ostensibly, this language seems intended to remove any doubts that communications companies, or NSA, might have with respect to whether a program such as SHAMROCK might constitute a violation of section 605. But if this was the apparent purpose of the 1968 amendments, it remained unclear whether they had this legal effect. In the well-known Keith case, for example, decided in 1972, the Supreme Court considered the language in chapter 119, quoted above, and found that it "confers no power", but instead "merely provides that the Act shall not be interpreted to limit or disturb such power as the President may have under the Constitution."[73] So if chapter 119 of title 18

did not authorize the President to do anything, as the Court suggests, one is left to ponder the meaning of the language found in the amended version of section 605 which says "except as authorized by chapter 119, title [illegible] telegraph companies shall not disclose telegrams in their possession (emphasis added).[a]

This apparent incongruity between the dicta in the Keith case and the statutory language in the amended section 605 has not been resolved by the Supreme Court. In United States v. Butenko, a 1974 case, however, the Court of Appeals for the Third Circuit, without attempting to reconcile the two, appeared to resolve the issue of 605's applicability in favor of the intelligence community by holding: "Section 605 of the Communications Act neither prohibits the President from gathering foreign intelligence information nor limits the use to which material so obtained may be put."[74] The Supreme Court denied certiorari.[75]

While the Butenko case involved intercepts of telephone conversations in the course of a wiretap which was exclusively and undisputedly undertaken for foreign intelligence purposes, the court's conclusions with respect to the legal effects of section 605 appear broad enough to insulate foreign intelligence-gathering procedures of all types from prosecutions under section 605.[76]

But as far-reaching as the Butenko language seems to be, even that decision indicates that section 605 may have continued vitality vis-a-vis the activities of intelligence agencies to the extent that such activities are undertaken for other than foreign intelligence purposes. The Butenko court stated its conclusion in the following manner: "The surveillances at issue here were conducted solely for the purpose of gathering foreign intelligence. Therefore, section 605 does not render them, in and of themselves,...unlawful."[77]

It would appear, then, that the amended version of section 605, even when read in light of the broad holding in Butenko, would prohibit the sort of activity which took place under SHAMROCK. By NSA's own account, it used information gleaned from the SHAMROCK "take"--from the early 1960's until 1973--for law enforcement and internal security purposes, and not solely for foreign intelligence purposes.[78] Virtually all overseas cables of Americans were read during this period, not simply those which had obvious foreign intelligence value.[79] Two of the telegraph companies, for their part, turned over everything to NSA, making no effort to select messages which could reasonably be expected to contain information of foreign intelligence value.[80] Thus, even under the Butenko standard, it is apparent that section 605 would have still presented a serious legal difficulty to SHAMROCK, had the program continued to operate as it had until 1973.

PART II

CURRENT NSA OPERATIONS

NSA has never fully explained to the public how it operates, ~~and, given the nature of its work, perhaps it cannot do so~~. Enough has appeared on the public record, however, and been conveyed to this Committee, to indicate what its functions are and how it carries them out. Such disclosures have also indicated the potential which NSA possesses to violate the privacy of individuals on an immense scale. The following discussion focusses upon several such apparent problem areas.

The "Vacuum Cleaner" Method

NSA's work necessarily brings it in possession of the private communications of Americans. This is so because in order for NSA to monitor international lines of communications for foreign intelligence, NSA must intercept all communications transmitted over such links. Former NSA Director Lew Allen, Jr., explained the problem which this presents to NSA to the Church Committee:

> "[I]t necessarily occurs that some circuits which are known to carry foreign communications necessary for foreign intelligence will also carry personal communications between U.S. citizens, one of whom is at a foreign location. The interception of communications, however it may occur, is conducted in such a manner as to minimize the unwanted messages. Nevertheless, many unwanted communications are potentially available for selection. Subsequent processing, sorting and selecting for analysis, is conducted in accordance with strict procedures to insure immediate and, where possible, automatic rejection of inappropriate messages. The analysis and reporting is accomplished only for those messages which meet specified conditions and requirements for foreign intelligence."[1]

General Allen's statement, apparently made to assure the Church Committee and the public, indicates the enormous potential for violation of personal privacy which NSA possesses.[1-A] [redacted]

First, it suggests that NSA is able to monitor virtually every international communication entering or leaving the United States. At present, some 24 million telegrams and 50 million telex (teletype) messages enter, leave, and transit the United States annually,[2] and most of these are sent or received by private citizens.[3] Computer data transmissions add billions of words each year electronically entering and leaving the country. Millions of additional messages are transmitted over leased lines, and international telephone calls are ~~considered as~~ yet another potential source of intelligence. ~~NSA's surveillance capabilities roar overseas.~~

Secondly, it is apparent from General Allen's statement that NSA, in the course of its intelligence-gathering, obtains access to virtually all types of information. NSA's "ear" is attuned not simply to messages with political and

military significance, but to messages concerned with financial and economic affairs, agricultural matters, cultural and social affairs, as well as purely personal affairs. The information which NSA makes use of, therefore, is not limited by the nature of the information it acquires.

Finally, General Allen's statement describes in general terms NSA's capability to select those messages which it decides meet its foreign intelligence criteria. Elaborating further on this capability, Allen noted: "[t]he use of lists of words, including individual names, subjects, locations, etc., has long been one of the methods used to sort out information of foreign intelligence value from that which is not of interest."[84] Presumably, therefore, NSA's selection process might be applied to sort out the communications of a particular government, a particular company, or a particular individual. NSA could presumably select a message going to or from such target or one which simply mentioned it. NSA could also presumably select communications about a particular subject, such as plutonium or oil.

In short, NSA possesses an extraordinary capability to intercept and make intelligible electronic signals which carry communications. No other agency of the federal government undertakes such activity on such an immense scale.[84-A]

Targeting for "Foreign Intelligence" Requirements

General Allen's statement to the Church Committee alluded to the fact that NSA selects messages on the basis of "foreign intelligence" requirements supplied by its consumers in the U.S. intelligence community.[85] What may constitute "foreign intelligence", however, is far from clear. As the Church Committee points out:

> "'Foreign intelligence' is an ambiguous term. Its meaning changes, depending upon the prevailing needs and views of policymakers, and the current world situation. The internal politics of a nation can 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."[86]

Indeed, NSA's monitoring the international communications of U.S. citizens involved in antiwar activities in the late 1960s was considered to have been part of the agency's "foreign intelligence" mission.[87] NSA claims that it no longer targets U.S. citizens by name for any purpose,[88] but it concedes that this limitation is a matter of self-restraint, rather than one of law[89] or practicality.[90]

Apart from even this sort of blatantly improper intrusion, however, it is not difficult to see how a broad range of activity carried out with foreign entities by American citizens, especially activities of an economic and financial nature, could be of "foreign intelligence" interest, and, thus, be "fair game" for NSA.

It may be of "foreign intelligence" interest, for example, to know what is being said between U.S. banks and their large Middle Eastern depositors, whose actions could have a substantial impact on the U.S. economy.[90-A] It may be of "foreign intelligence" interest to know the details of oil transactions between U.S. importers and their foreign suppliers, of commodities sales with foreign governments, of negotiations regarding the purchase of equipment or services from American concerns, of the location and quantity of various raw materials, or the location of influential U.S. businessmen traveling in foreign countries, or of what is being said about or to members or employees of the U.S. government.[90-B]

Thus, while an American citizen or company might not be targeted by name, by virtue of his international activities, his communications might be selected by NSA on the basis of its "foreign intelligence" criteria. NSA has not denied that it, in fact, "selects" U.S. messages of this nature; and, indeed, several uncorroborated reports have reached this Committee indicating that such monitoring is presently underway.[91]

Communications Security (COMSEC)

In addition to its foreign intelligence mission, NSA is charged with the protection and security of U.S. government communications.[92] NSA carries out this function primarily by developing codes and encryption devices to ensure that governmental communications cannot be read by foreign intelligence-gathering agencies.

Recently, however, press reports have stated that NSA has carried out its communications security function by monitoring purely domestic communications links to determine what information, if any, is being gleaned from American communications by Soviet intercepts within the United States.[93]

NSA has not publicly denied these reports, nor has it sought to explain them.[94] When asked about such reports, the current NSA Director, Vice Admiral Bobby R. Inman, only repeated NSA's claim that "no U.S. citizen is now targeted by the NSA in the United States or abroad".[95] As heretofore noted, however, the fact that NSA does not target U.S. citizens by name, does not necessarily mean that NSA does not intercept and select the communications of U.S. citizens to carry out its work. If

INSERT - PAGE 22

NSA representatives have repeatedly given the Committee informal oral assurances that internal NSA directives exist to prevent the misuse of intercepted telecommunications that are not "foreign-intelligence" related. And Gen. Allen has publicly declared: "The executive directives applying to these efforts state: (a) The purpose of the signals intelligence activities of the National Security Agency is to obtain foreign intelligence from foreign communications or foreign electronic signals. (b) Foreign communications exclude communications between or among citizens or entities." 91-A/

Unfortunately, these statements shed little light on what the NSA actually does with communications of American citizens which it might acquire. [redacted] any related internal NSA guidelines, no matter how tightly drawn they may be to prevent potential abuses, are so closely held that any violations will likely be [redacted] undetected by Congress or any other authority outside the NSA, since the only persons having access to these guidelines outside the NSA are a selected group within the Executive Branch and a handful of "need-to-know" Members and staff within the Congress, all of whose access to information is based on the condition they will not disclose it. Furthermore, [redacted] briefings on high-priority or potentially embarrassing intelligence matters by federal intelligence matters given to these "need-to-know" individuals in Congress, are often vague and incomplete. 91-B/ Moreover [redacted] it is virtually impossible for any person or Agency outside/selected members of the intelligence community to ascertain if the guidelines are, in practice, actually followed. The guidelines, therefore, being kept very secret, offer little assurance tothe American people. Not only are they unknown, but no public evaluation of their effectiveness is presently permitted. In practice, the "system" is ultimately based on the rule of very few men and not on the rule of law.

domestic communications are being perused by NSA with the idea of discovering what the Soviets are able to obtain from U.S. communications, NSA's communications dragnet could conceivably be of mammoth proportions.

"A"

Uncommon Secrecy

To understand NSA's reluctance to provide greater public explanation of the manner in which it intercepts and handles U.S. communications, one must understand the uncommon secrecy which has traditionally enshrouded its existence and functions. The Agency was created by classified Executive order in 1952, and its functions were assigned by classified Executive directives thereafter. Prior to 1962, its existence was not acknowledged in the U.S. Government Manual. It was not until 1975, twenty-three years after its creation, that any Director of the agency ever appeared before a congressional committee in public session.

NSA has furthermore refused to provide evidence in judicial proceedings on the grounds that such public disclosures could lead to a compromise of its "sources and methods". The Church Committee reported that at least one criminal prosecution was dropped by the Justice Department because of NSA's refusal to discuss such intercepts in a public forum.[16] Attorney General Levi admitted to the Church Committee that even he was not privileged to NSA's secrets:

> "Attorney General Levi: ... [A]t this time I would have to say that I do not know what [NSA's] procedures are. I do not know what the possibilities are. I do not know enough about the minimization procedures [for the interception and use of U.S. communications] ...
>
> "Senator Church: Until you have that information, you really do not have the foggiest idea of whether what they [NSA] are doing is legal or illegal, constitutional or unconstitutional?
>
> "Attorney General Levi: I would be glad to accept the protective shape of that proposed answer. I suppose I have a foggy idea."[17]

It has ~~finally~~ been this Committee's experience during its independent investigation of the SHAMROCK program, that even after the Church Committee had released its public report exposing in great detail the nature of the program, NSA steadfastly refused to declassify any of the documents regarding the program for requested purposes of this Committee's work.

"B"

RESTRICTIONS UPON NSA'S CURRENT OPERATIONS

NSA contends that, since it is concerned solely with gathering "foreign intelligence", neither the restrictions contained in the wiretap statute (18 U.S.C. 2510, et seq.) or in section 605 of the Communications Act of 1934 affect its operations.[18]

INSERT - p. 23 "A"

COMSEC is also involved in another area of written telecommunications of U.S. citizens that are not national security related, through the recently adopted Data Encryption Standard. Data telecommunications, like telephone communications, can be intercepted and read. To protect the integrity of these communications, the Secretary of Commerce, on November 23, 1976, approved [redacted] the Data Encryption Standard established by the National Bureau of Standards, which had been largely developed through [redacted] with the assistance of the [redacted] NSA. In this standard, messages to be transmitted can be encrypted into 56 binary digits ("bits"), and decrypted by the recipient. However, many critics of this standard maintain that the 56 bit level allows the NSA to penetrate it, and circumstantial evidence suggests that prior to the NSA's involvement, the standard being developed [redacted] by IBM was set at a much higher level.[95-A]

95-A. See, for example, a November 18, 1976 Bell Laboratories memorandum (copy in subcommittee files), which characterizes the Data Encryption Standard as having "little safety margin" and urges that it be strengthened to 64 or 128 bits. This memorandum also notes that a 1971 IBM publication describes the Data Encryption Standard's planned, but never implemented, predecessar as utilizing 128 bits.

The senior official of a giant U.S. multinational financial institution, cited in footnote 90-A, opined that his company is only concerned with interception by private entities, and it protects itself from this threat by encrypting its telecommunications at a level which makes it inaccessible to non-governmental third parties, but not inaccessible to the NSA. [redacted], he added, has not made a higher encryption operational because it would "run into a political morass with the Office of Munitions Control" in Washington [redacted]

[redacted] corporations as well as most comparable businesses,

An official of the State Department's Office of Munitions Control - which works in tandem with the Department of Defense - has advised the subcommittee that for export use, "anything above 56 bits you have to come to us," adding that one large U.S. corporation wants to use more bits in several overseas situations and in some cases we are going to grant permission." (Telephone interview [redacted] with Mr. Clyde Brant, January 5, 1977).

INSERT "2" - P. 23

The NSA has maintained this position, notwithstanding its Operation SHAMROCK represented an invasion of privacy of American citizens vastly greater than any known FBI or CIA mail intercept program, and its watch list activities vis-a-vis American citizens were deemed by former Attorney General Elliot Richardson to raise "a number of serious legal questions which have yet to be resolved."97-A (Was Fink FN 85) The NSA continues to function under a mantle of secrecy. It has not explained, and presumably does not intend to explain, itself to the American people. It simply asks the public and the Congress to "trust us."

The Committee does not believe that such trust is justified, and finds it regrettable that a shroud of secrecy, as tightly drawn as ever, continues to envelop all the activities of the NSA. The Committee further believes that even if the NSA did not pose a significant threat to the privacy of American citizens, and if it had not abused its powers in this regard, that much of the secrecy surrounding its operations is obsessive and unfounded. The fact that it does pose a significant threat to the privacy of American citizens, and has a record of violating it for more than thirty years, strengthens the Committee's belief that the NSA should explain to the public what it does with its intercepted telecommunications, and should become publicly accountable for its activities that effect Americans.

The Committee finds that much of the basis for this secrecy is historical habit, in which intelligence agencies traditionally attempt to keep everything - even, when possible, their very existence - hidden. [redacted].

The NSA has vigorously fought disclosures which, in the Committee's view, will not endanger the national security. Thought the NSA acknowledges that it monitors telecommunications of "foreign intelligence interest," and it is generally accepted in diplomatic and intelligence circles that the Agency monitors

INSERT "B" - P. 23 (cont'd)

the telecommunications of most foreign governments, the NSA, strongly reinforced by the White House and the Defense and Justice Departments, considers it unthinkable, for example, to identify even by categories, countries in which it has an intelligence interest. This attitude is maintained even though Herbert Yardley had, in 1931, listed 21 countries, including some of our closest allies, whose codes were breaking 50 years ago, in peace time. Foreign governments today can hardly believe the NSA is currently doing any less, in view of the Cold War and the ease with which modern technology allows the NSA and counterpart organizations of other governments - to acquire message traffic. 97-B

97-B Lyman B. Kirkpatrick, Jr., former Inspector General of the CIA, has written: "No mission located on foreign soil can consider immune from audio surveillance," concurrently noting that "The insatiable maw of the [illegible] intelligence community analyzed every communication of any conceivable interest...."

97-B Several knowledgeable sources have advised the Committee that the NSA, while able to collect virtually all telecommunicatios, as a practical matter is unable to read the sensitive traffic of developed nations. This results from advances in computer technology, which have enabled the codebakers to outstrip the codebreakers. This position was [illegible] publicly expressed by David KAhn, in the New York Times, [illegible] June 22, 1973:

Insofar as the interception and use of the communications of U.S. citizens are concerned, NSA is restricted only by classified guidelines established by the Attorney General in 1975. These guidelines have never been made public nor officially released in sanitized form. While they have been alluded to in various public comments of agency officials,[99] and in a report made to this Committee by the General Accounting Office,[100] these comments regarding the guidelines have been general and have not explained how NSA systematically selects and treats the communications of U.S. citizens and businesses. GAO, for example, reported to the Committee that NSA "takes great pains to remove the identity of a U.S. person from any foreign intelligence report", but in the course of sampling such reports, GAO auditors found "three instances in which the mention of equipment might identify a U.S. manufacturer to a knowledgeable person".[21] GAO suggests, on the one hand, that NSA deletes the names of U.S. citizens from communications which it uses to compile its foreign intelligence reports, but that it leaves intact certain information from which identification of such citizens could be made.

CONCLUSIONS

At the outset, this Committee realizes that the newly-created intelligence oversight committees of the Congress have primary jurisdiction over the foreign intelligence activities of NSA. The Committee is equally aware that it may not have sufficient information in its possession regarding these activities to make informed judgments regarding the controls that should be placed upon NSA. Nevertheless, in the course of this Committee's investigation of the telegram interception program, in the work of the Church Committee, and in what has appeared elsewhere on the public record, it has become apparent that the activities of the NSA have had, and probably continue to have, an adverse impact upon the rights and privacy of American citizens. This does concern the Committee.

Although NSA no longer sends its messengers to the offices of international telegraph carriers in the early hours of the morning, as it did while SHAMROCK was operational, it nevertheless intercepts international communications just as effectively and just as indiscriminately. In fact, the international communications of Americans are presumably being intercepted today in a significantly greater volume than was ever available under SHAMROCK. Moreover, the ability of NSA to sift such great volumes of material has undoubtedly improved with advances in computer technology.

NSA concedes that it must unavoidably acquire many communications of American citizens but it will not say what it does with those communications.

NSA further concedes that some of the communications of American citizens may be of "foreign intelligence" value but it will not say what it does with these communications.

NSA also says that it intercepts only communications which have one foreign terminal, but it does not explain or deny press reports that it monitors domestic long-distance calls to determine what the Soviets obtain from U.S. domestic communications.

NSA says that it operates under strict guidelines established by the Attorney General but it refuses to say what those guidelines are and refuses to make a public assessment of their effectiveness.

All of this leaves the public to wonder if their communications are being silently intercepted and used by the government without their knowledge. Apart from a fundamental concern for the privacy of one's communications, these practices unavoidably bring other possibilities to mind. Could the government be using information gleaned from such communications to influence or disrupt international business transactions? Could it provide NSA or Executive branch employees with "insider" information regarding investments or information which might otherwise give them a competitive advantage in some economic venture? Could such information be used to "blackmail" or threaten some individual or business? Could this information be turned over to a federal agency, such as the Securities and Exchange Commission or Commerce Department, in pursuit of its administrative responsibilities? Would information which suggested that a crime had taken place or was about to take place be turned over to a law enforcement agency? Would information relating to a potential civil disturbance or forthcoming political rally be turned over? Would information regarding the future of certain legislation be passed on to the appropriate federal agency? Would information which suggested some person may be a security risk be turned over to the appropriate federal agency? Could information under any circumstances be turned over to a private employer? Could such information ever be used to deny a federal benefit?

It is the opinion of the Committee that, notwithstanding the important and sensitive work undertaken by NSA, democratic government demands greater public accountability for an agency with the potential which NSA has to violate the

rights of American citizens. At the very least, NSA should make public the Attorney General's guidelines which govern its acquisition and handling of the communications of U.S. citizens, and should open such restrictions to the invigorating effects of public debate. If the guidelines as they are now written cannot be disclosed because of the intelligence methods which they might reveal, the Committee encourages that they be released in a form which does not compromise such techniques.

Over the long term, the Committee concludes that Congress should adopt statutory controls to govern the activities of NSA, at least insofar as they impact upon the communications of American citizens. At present, NSA contends that laws governing wiretapping and radio interceptions are not applicable to its operations. It has no statutory charter, nor is its director even subject to confirmation by the Senate. To this point at least, even the recently-created congressional oversight committees have provided the public with no greater insight.

In view of the Agency's considerable potential for violations of the privacy of Americans, however, and the doubts already cast upon the legitimacy of its current practices, the Committee concludes that NSA's limited accountability does not serve the public's interest. Neither the Congress nor the public can carry out their constitutional responsibilities in a vacuum. Both need information. When the activities of an Executive agency come into apparent conflict with the rights and privacy of the individual, it is essential to good government that the public be informed of the nature and extent of that conflict. We should not be left to wonder whether we are abiding the activities of NSA at the expense of the Constitution.

1/ The House Select Committee on Intelligence (hereafter cited as Pike Committee) noted that the total annual intelligence community budget was "more than $10 billion;" that the NSA "has one of the largest budgets in the intelligence community;" that "roughly 20 percent of the National Security Agency's budget is not added into the intelligence budget;" that "the costs given Congress for military intelligence [much of which would be applicable to NSA's functions] do not include expenditures for tactical military intelligence, which would approximately double intelligence budgets for the three military services." (Pike Committee Report, Village Voice, February 16, 1976, p. 72.)

This appears to conflict with a CIA briefing given to President-elect Jimmy Carter, that "the military branches of the intelligence community receive more than 80 percent of the roughly $4 billion budgeted annually for all United States intelligence efforts, principally for the photo reconnaissance and radio signals interception technology used to monitor potential adversaries." (David Binder, "U.S. Intelligence Officials Apprehensive of New Shake-Ups Under Carter," New York Times, December 13, 1976, p. 43. Emphasis added.)

2/ David Kahn, author of The Codebreakers, a definitive work on cryptology, describes the NSA as "the largest and most secretive of all American intelligence organs," and estimates that on its own it "spends about $1 billion a year." But, he adds, "the agency also disposes of about 80,000 servicemen and civilians around the world, who serve in the cryptologic agencies of the Army, Navy, and Air Force [that] stand under NSA control, and if these agencies and other collateral costs are included, the total spent could well amount to $15 billion." (Source: David Kahn, "Big Ear of Big Brother", New York Times Magazine, May 16, 1976.)

Tad Szulc describes NSA as "the largest, most important, most expensive, and secret member of America's 'intelligence community,'" which "costs over $10 billion a year and employs some 120,000 persons around the world." According to Szulc, "a vast array of specialized military agencies such as the ASA (Army Security Agency), the USAFSS (United States Air Force Security Service), and the NSG (Naval Security Group) . . . account for the vast majority of the NSA's military and civilian employees." Approximately 90 percent work abroad. (Tad Szulc, "The NSA - America's $10 Billion Frankenstein", Penthouse, November 1975.)

3/ "Meet the Press" interview, August 17, 1975.

4/ See footnote 2.

5/ For "Communications Intelligence" and "Communications Intelligence Activities" official definitions, see p. .

6/ Frank Van Riper, "Find U.S. Agents Spy on Embassies' Cables," New York Daily News, July 22, 1975, p. 2

7/ Subcommittee Hearings, pp. 2-3.

8/ Id., p. 62.

9/ Church Committee Hearings, Vol. 5, pp. 57-60.

10/ Subsequently amended to 1945 (see p.).

11/ Subcommittee Hearings, p. 56.

12/ Id., pp. 58-59.

13/ Id., p. 99.

14/ Id., pp. 125-26.

15/ Id., p. 240, et seq.

16/ Army Security Agency, Historical Background of the Signal Security Agency, Vol. III, p. 74; prepared under the Direction of the Assistant Chief of Staff, G-2, April 12, 1946.

17/ Id.

18/ David Kahn, The Codebreakers (New York, The Macmillan Company, 1967), p. 344.

19/ Herbert O. Yardley, The American Black Chamber (Indianapolis, The Bobbs-Merrill Company, 1931), p. 240.

20/ Army Security Agency, op. cit., p. 48: "In order to conceal the true nature of its activity, the office was called 'Code Compilation Company', a cover name for MI-8 but the real name of an incorporated business firm established by Yardley and Charles J. Mendelsohn, partners in this venture. This firm produced and sold in fairly large quantity, a code called the Universal Trade Code."

21/ Yardley, op cit., p. 370.

22/ Quoted in Kahn, op. cit., p. 360n. (In this regard, Secretary Stimson also made his well-known declaration, "Gentlemen do not read each other's mail.")

23/ Yardley, op. cit., p. 332. (This forty-five year old list is not dissimilar to one possessed by Western Union International which, when subpenaed by this Committee on February 4, 1976, prompted President Ford to attempt to extend the so-called "executive privilege" doctrine to a private corporation. See p. below.)

24/ Id.

25/ Yardley, op. cit., pp. 240-41.

26/ Copy in possession of subcommittee.

27/ Postal Telegraph, the holding company controlling Commercial Cable, merged with Western Union in 1943. (Of the three U.S. companies now dominating the international telegraph business in and out of this country -- ITT World Communications, RCA Global Communications, and Western Union International, an independent spin-off of Western Union -- two were only minimally in the business in the 1920's, and one did not exist.)

28/ Yardley, op. cit., p. 342.

29/ Army Security Agency, op. cit., pp. 73-74.

30/ This section is largely based on Army Security Agency, op. cit., pp. 74-77.

31/ "An act to regulate radio communication," August 13, 1912, 62nd Cong., 2d Sess., Ch. 287, Statutes at Large, Vol. 37, Part I, p. 307.

32/ "An act for the regulation of radio communication," February 23, 1927. 69th Cong., 2d Sess., Ch. 189, Statutes at Large, Vol. 44, Part II, Sec. 27, p. 1172.

33/ Army Security Agency, op. cit., p. 77.

34/ New York Times, June 2, 1931; p. 18.

35/ New York Herald Tribune, June 9, 1931; p.

36/ New York Times, June 2, 1931; op cit.

37/ Yardley described his receiving the award, as follows:

> "In awarding you the D.S.M.," the General began again, "we find it difficult to draft a citation that will describe your distinguished services, and at the same time keep the nature of your activities secret, for of course all citations are published. Have you any suggestions?"
>
> "I naturally have never given the matter any thought."

INSERT 3 -- FOOTNOTES

5-A/ "Written," as interpreted in this report, includes cablegrams, radiograms, telex transmissions, computer transmissions (such as used by banks for financial transfers), facsimile and video transmissions, telemetry, and switch and signal and other non-oral transmissions.

40-A/ The Navy also had its own cryptologic section. See Kahn, op. cit., pp. 386-88.

37/ [footnote continued]

> "Well, we'll draft something, so that your successes will not be revealed. The only regret is that the real reason for confirming the D.S.M. can not be given . . . ."
>
> I was to appear before Secretary of War Weeks at two P.M. to receive the D.S.M. On the way to his office I asked General Heintzelman if Secretary Weeks really knew why I was being awarded the D.S.M. He assured me that the Secretary was one of the most ardent supporters of the Black Chamber.
>
> I felt rather silly standing before the Secretary of War, as he read my citation that seemed to have very little to do with the breaking of codes of foreign governments, but I was relieved when he pinned the medal on my lapel, for with a twinkle in his eye he winked at me. The wink pleased me immensely. (Yardley, op. cit., pp. 322-23.)

38/ Army Security Agency, op. cit. p. 177.

39/ New York Times, February 21, 1933, p. 3.

40/ Primarily from Army Security Agency, op. cit., pp. 176-80.

41/ ITT Communications is now ITT World Communications. RCA Communications is now RCA Global Communications. In 1963, Western Union's international operations were transferred to Western Union International, which was established as an independent company. Between 1971-1974, these three companies carried 94.9 percent of all international telegraph messages in and out of the U.S. (Source: FCC letter to subcommittee, January 28, 1976).

42/ In March 1976, when representatives of the three major American telegraph companies engaged in international communications testified before the subcommittee, the subcommittee believed that the government had not commenced its post World War II interception of private messages until 1947. This belief was based on a report issued by the Church Committee on November 6, 1975, at which time Sen. Church stated:

> At meetings with Secretary of Defense James Forrestal in 1947, representatives of the three companies were assured that if they cooperated with the Government in this program, they would suffer no criminal liability and no public exposure, at least as long as the current administration was in office. They were told that such participation was in the highest interests of national security.

Shortly after the subcommittee's March 1976 hearings, a subcommittee staff inquiry led to records being uncovered in the Archives which indicated that the Army Security Agency had, in fact, taken steps to initiate the interception program as soon as the war ended. Prior to making these records available to the subcommittee, Archives sought Department of Defense permission; that permission was refused. The Department of Defense then advised the Church Committee of the existence of these documents, and allowed a staff member of that committee to inspect (but not copy) them. This transpired just prior to the issuance, in May 1976, of the Church Committee staff report on "National Security Agency Surveillance Affecting Americans," which was amended accordingly.

43/ Letter from Intelligence Officer of Army Signal Security Agency to Commanding General, August 24, 1945, quoted in Church Committee Final Report, Book III, pp. 767-68.

44/ Id., p. 769.

45/ Subcommittee Hearings, p. 212.

46/ Id.

47/ Mr. Sparks, who was the most forthright of all telegraph company witnesses, testified that within RCA he was the sole authority for making all messages available to government agents, and that this arrangement began in 1947. The Committee has no reason to doubt the accuracy of Mr. Spark's testimony insofar as he was aware of the facts. The 1947 date, as he recalled it, was presumably a result of that being the program's generally accepted date of commencement, at the time of his testimony. His belief that he was responsible for making the arrangements with the government apparently is based on initiatives made to him by Army Security Agency representatives, subsequent to arrangements unknown to him being made with his superiors. (See October 9, 1945 letter from RCA Vice-President W. H. Barsby to Brig. General W. Preston Corderman, in Subcommittee Hearings, p. 208). Mr. Sparks apparently never knew about the 1947 meeting with Secretary Forrestal; Spark's superior, Gen. Harry C. Ingles, then president of RCA Communications, represented the company.

The ITT delegation to the 1947 Forrestal meeting was led by ITT Chairman and President. Sosthenes Behn. Joseph L. Egan, Western Union president, was invited but did not attend, and his company apparently was not represented.

48/ Army Signal Security Agency letter, August 24, 1945, op. cit., p. 772.

49/ For a detailed description of these procedures see Church Committee Final Report, Book III, pp. 765-776.

50/ Id., p. 773.

51/ Subcommittee Hearings, p. 107.

52/ Western Union International's executive vice-president testified he had the machine removed in 1965. However, the Church Committee reported at Book III, p. 774: This recollection "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 . . . . 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 . . . . In effect, Western Union International's participation in SHAMROCK ended by 1972."

On June 7, 1976, Mr. Greenish advised the subcommittee, through counsel ". . . that the practices discussed by him, copying foreign government traffic on the Recordak, terminated with the removal of the one and only Recordak 'about 1965'". (Subcommittee Hearings, p. 111.)

53/ In addition, the Western Union International office in London turned over communications entrusted to its care to the government of the United Kingdom. On March 3, 1976, Executive Vice President Thomas S. Greenish testified that his company never made cables available to authorities of any country other than the United States, but he subsequently told the Subcommittee that he "misunderstood Ms. Abzug's question," and his attorney requested that his testimony be changed to show that messages had been turned over to British officials. (See Subcommittee Hearings, pp. 112-13).

Mr. Greenish's amended testimony is consistent with a February 21, 1967 report in the London Daily Express, which stated that telegrams sent out of Britain were regularly made available to that country's security authorities; the story noted that international telegrams which passed through foreign companies operating in Britain "are collected in vans or cars each morning and taken to the Post Office security department." On June 22, 1967, Prime Minister Harold Wilson told Parliament that the practice had been going on since 1927. On May 12, 1976, the British Embassy in Washington refused to state whether the practice continues, formally advising the Subcommittee that "it is not in accordance with HMG's policy to comment on such matters."

On March 11, 1976, George Knapp, president of ITT World Communications, testified that to his "personal knowledge" his company had never made communications available to any foreign government. (See Subcommittee Hearings, p. 306.) Representatives of RCA Global Communications were not asked if their company had ever made communications available to any foreign government.

53/ [footnote continued]

The Committee does not know what uses the British government makes of the messages made available to it, nor does it know if the messages are disseminated to any other governments. The British government maintains a liaison office at NSA headquarters in Ft. Meade, Maryland, and the NSA maintains a liaison office at the British government's General Communications Headquarters in Cheltenham, 75 miles northwest of London. NSA personnel are also based at several other locations in Great Britain. Under the 1947 UK-USA Agreements, the U.S. and the United Kingdom -- as well as Canada, Australia and New Zealand -- routinely exchange information gleaned from intercepted telecommunications.

54/ Church Committee Final Report, Book III, p. 737.

55/ Id., p. 739.

56/ "Establishment of Sensitive SIGINT Operation Project Minaret," dated July 1, 1969, in Church Committee Hearings, Vol. 5, pp. 149-50.

57/ SIGINT recipients include, but are not limited to, the President's Foreign Intelligence Advisory Board (PFIAB), the Central Intelligence Agency (CIA), the Federal Bureau of Investigation (FBI), the Defense Intelligence Agency (DIA), the (Army) Assistant Chief of Staff for Intelligence (ACSI), the Office of Naval Intelligence (ONI), the Air Force Office of Special Investigations (AFOSI), the Energy Research and Development Agency (ERDA) and the Department of State's Office of Current Intelligence.

58/ Church Committee Hearings, Vol. 5, p. 150.

59/ For a detailed discussion of NSA watch-list activities, see Church Committee Hearings, Vol. 5, pp. 1-55 and 145-163; also Church Committee Final Report, Book III, pp. 737-65.

60/ Letter from Comptroller General of the United States Elmer G. Staats to Chairwoman Bella S. Abzug, November 12, 1976, p. 2.

61/ Subcommittee staff telephone interview with Col. Stephen A. Harrick, Office of Assistant Secretary of Defense for Legislative Affairs, March 1, 1977. (The civil litigation is Halkin v. Helms, 75-1773, U.S. District Court, District of Columbia Circuit).

62/ For a detailed discussion of NSA Office of Security files on American citizens, see Church Committee Final Report, Book III, pp. 777-78.

63/ Church Committee Final Report, Book III, p. 778.

64/ This is not to argue for the continuation of SHAMROCK, or any SHAMROCK surrogate

65/ Not even a single blanket "vacuum cleaner approach" satisfied the appetite of government monitors, for FBI and NSA "cable drop" operations in Washington partially duplicated and triplicated the New York SHAMROCK coverage. In these operations, the FBI physically ~~accessed~~ entered the Washington offices of RCA Global Communications and ITT World Communications during daylight hours, to examine cable messages, and NSA repeated the operation between 3 and 5 a.m. (See Subcommittee Hearings, p. 241; the Committee has also been informally informed that the same persons who made nocturnal visits to RCA similarly visited the Washington offices of ITT).

For sorting messages, the FBI paid RCA employees from 1960 to 1973; starting in 1966 the FBI began withholding 20 percent of these payments for income tax purposes. (Ibid, pp. 242-43; the Committee does not know if ITT employees received comparable message-sorting compensation from the FBI).

66/ Pike Committee Hearings, p. 241.

67/ Mr. Colby's semantic qualifier, "on some occasions," is not unlike his testimony before the subcommittee and others, that the CIA's 20 year mail intercept program (which opened over 190,000 letters), was among "the few" individual instances of the Agency's domestic illegalities. Cf., for example, "Central Intelligence Agency Exemption in the Privacy Act of 1974" hearings, House Subcommittee on Government Information and Individual Rights, March 5, 1975 (p. 5) and June 25, 1975 (pp. 139-40).

68/ The legal conflict between this general search procedure and the fourth amendment is discussed on p. .

69/ Letter from R. Michael Senkowski, Legal Assistant to the Chairman, Federal Communications Commission, to Robert Fink, Professional Staff Member, Subcommittee on Government Information and Individual Rights, January 28, 1976.

70/ U.S. persons are U.S. citizens, resident aliens in the U.S., and corporations with their principal place of business in the U.S.

71/ These are headquarters procedures. Apparently, at overseas bases, many messages are also intercepted by human analysts prior to trigger word screening. Chet Flippo, an associate editor of Rolling Stone, reported that he was, in 1967, in the Naval Security Group (the NSA's naval wing), assigned to intercept telecommunications from a desert base in Sidi Yahia, Morocco. In addition to intercepting diplomatic cables, military messages, telegrams, transcripts of transatlantic phone calls, Flippo wrote, "I also screened reams and reams of transatlantic cables to and from the U.S., regardless of whether they contained any key words or names. Telegrams or phone calls involving American congressmen and journalists, 'dissidents,' multinational corporations -- were all targets." (Chet Flippo, "Can the CIA Turn Students Into Spies?", Rolling Stone, March 11, 1976).

72/ Church Committee Hearings, Vol. 5, p. 60.

73/ See p. , for a partial list of SIGINT recipients.

74/ Letter from Lt. Gen. Lew Allen, Jr. to Chairman Otis Pike, House Select Committee on Intelligence, August 25, 1975; quoted in Committee's final report as published in Village Voice, February 16, 1976, p. 90.

75/ Ibid, p. 88 [emphasis added].

76/ Attachment to letter from Federal Reserve Chairman Arthur F. Burns to Sen. Frank Church, Chairman of the Subcommittee on Multinational Corporations of the Committee on Foreign Relations, March 9, 1976. (Copy in subcommittee files). The Federal Reserve refused to supply the multinational subcommittee with deposit totals of individual Middle East oil-producing nations, but the Washington Post noted that, in 1975, the government of Kuwait had $1.7 billion on deposit with the Citibank of New York, and in the same year foreign deposits accounted for nearly two-thirds of all monies deposited in both the Citibank and Chase Manhattan Bank, the nation's second and third largest banks. (Ronald Kessler, "Banks Hold Huge Foreign Deposits: U.S. Examiners Worried About Pressure From Governments," Washington Post, January 14, 1976, p. A-1). By June 30, 1976, the deposits of the Middle East oil-exporting countries in U.S. banks reportedly totaled around $19 billion. (Dan Morgan, "Senators, Banks Block Probe of Arab Deposits," Washington Post, October 10, 1976, p. A-1.

77/ Telephone interview, December 14, 1976.

78/ The Mutual Security Act of 1954, as amended, establishes controls on "the export and import of arms, ammunition, and implements of war, including technical data relating thereto, other than by a United States government agency." Category XIII, "Auxiliary-Military Equipment;" subsection (b) includes:

> Speech scramblers, privacy devices, cryptographic devices (encoding and decoding), and specifically designed components therefor, ancillary equipment, and especially devised protective apparatus for such devices, components and equipment. (Source: International Traffic in Arms Regulations, Department of State; February 1976, p. 5).

The Act is administered by the State Department's Office of Munitions Control, assisted by the Department of Defense, which grants (and withholds) export licenses. On November 23, 1976, the Secretary of Commerce signed a Data Encryption Standard developed by the National Bureau of Standards, assisted by the National Security Agency. Many critics of this standard maintain it is set at a level (56 binary digits, or "bits") which allows the NSA and, in time, very large corporations, to penetrate it. A November 18, 1976 Bell Laboratories memorandum (copy in Subcommittee files) characterizes the standard as having "little safety margin," and urges that it be strengthened to 64 or 128 bits. An official of the Office of Munitions Control has advised the subcommittee that for export use, "anything above 56 bits you have to come to us," adding that one large U.S. corporation wants to use higher bits in several overseas situations and in some cases we are going to grant permission." (Telephone interview with Mr. Clyde Bryant, January 5, 1977).

INSERT

74A/ Until the formation of the Church Committee, these individuals were limited to selected staff members of the Armed Services committees in the Senate and the House, and the Defense subcommittees of the Appropriations committees in the Senate and the House. This Committee has asked several of these staff members if, in the course of exercising their Committee's oversight functions, the NSA had ever briefed them on Operation SHAMROCK. Some of these individuals replied they were generally aware that the Agency from time to time inadvertently intercepted private sector communications; others said the first they knew of such activity was when they read it in the newspaper. This Committee has received no indication that any of these individuals had a detailed knowledge of Operation SHAMROCK.

79/ Letter from Comptroller General of the United States Elmer G. Staats to Chairwoman Bella S. Abzug, November 12, 1976, p. 5.

80/ Ibid, p. 5.

81/ See p. .

82/ Bob Woodward, "CIA Bugging Micronesian Negotiations," Washington Post, December 12, 1976, p. A-1.

83/ In 1970, when President Nixon endorsed the so-called Huston Plan, under which the NSA would intercept the private communications of American citizens, he was unaware that the NSA had for years been conducting a watch-list program similar to what he was proposing; there is no indication the NSA ever informed him of its watch-list activity.

84/ See, for example, letter from Lt. Gen. Lew Allen, Jr., to Attorney General Elliot Richardson, October 4, 1973, in Church Committee Hearings, Vol. 5, pp. 162-63.

85/ Letter from Attorney General Elliot Richardson to Lt. Gen. Lew Allen, Jr., October 1, 1973, in Church Committee Hearings, Vol. 5, pp. 160-61.

86/ The Washington Post has described the NRO as spending "an estimated $1.5 billion a year acquiring and managing the most sophisticated, elusive and expensive force of spies that has ever been recruited into the government's service." (Laurence Stern, "1.5 Billion Secret in Sky: U.S. Spy Unit Surfaces by Accident," Washington Post, December 9, 1973, p. A-1). Two years later, the New York Times described the NRO as a semi-autonomous unit "under the Air Force that runs the satellite photography program, set to spend under $2 billion." (Leslie Gelb, "U.S. Intelligence Cost is Put at $4 Billion," The New York Times, November 19, 1975, p. 40).

87/ So unthinkable is such disclosure that President Ford invoked "executive privilege" to apply to a private corporation, in an attempt to prevent the turnover of an old NSA list of countries whose telecommunications the Agency had expressed an interest in intercepting (see p.). The contents of this list had long been known to both the company's outside counsel and selected company employees. On October 22, 1975, NSA Director Allen was informally asked by a subcommittee staff member, "What security clearance does a private attorney for a telegraph company have?" "What security clearance does a company employee who transmits messages have?" Gen. Allen replied, "None." Apparently, in the view of the NSA, these individuals are entitled to information that the Congress is not.

88/ Winslow Peck, "U.S. Electronic Espionage: A Memoir," Ramparts, August 1972. (Reporting on Peck's allegations, the New York Times stated: "Extensive independent checking in Washington with sources in and out of the Government who were familiar with intelligence matters has resulted in the corroboration of many of his revelations But experts strongly deny that the United States has broken the sophisticated codes of the Soviet Union or other foreign powers." Benjamin Welles, "Ability to Break Soviet Codes Reported," New York Times, July 16, 1972, p. 1).

89/ 5 U.S.C. 552a, effective September 27, 1975.

90/ Federal Register, Vol. 40, No. 168, August 28, 1975, pp. 39777-801.

91/ Federal Register, Vol. 40, No. 166, August 26, 1975, pp. 37579-582; Federal Register, Vol. 40, No. 187, September 25, 1975, pp. 44294-297.

92/ Federal Register, Vol. 41, No. 13, January 20, 1976, pp. 3025-033.

93/ See, for example, House Subcommittee on Government Information and Individual Rights Hearings, "Central Intelligence Agency Exemption in the Privacy Act of 1974, 1975, p. 164; also, Church Committee Final Report, Book II, p. 101.

[65]Adams v. William 407 U. S. 143 (1972); Wyman v. James 500 U. S. 309 (1971); Terry v. Ohio 392 U. S. 1 (1968); Camara v. Municipal Court 387 U. S. 523 (1967).

[66]In Newfield v. Ryan 91 F.2d 700(3rd Cir. 1937), cert. den. 302 U. S. 729 (1937), the court held that SEC subpoenas to telegraph companies to produce telegrams relating to matters under investigation constituted "other lawful authority" for purposes of section 605.

[67]Indeed, in Nardone v. United States 302 U. S. 379 (1937), the Supreme Court expressly decided that the second clause of section 605 "comprehends federal agents" within its prohibition. 302 U. S. at page 381.

[68]See Sen. Rep. No. 781, 73rd Cong., 2d Sess. 1 (1934); H. Rep. No. 1850, 73rd Cong., 2d Sess/ 3 (1934).

[69]See Memorandum of Richard W. Cutler, "Possible Liabilities Arising from surrender of RCA-Transmitted Messages to Government Officials", November 11, 1948, reprinted in Abzug Committee Hearings, at p. 255 ff.

[70]See letter from Thomas K. Latimer, Department of Defense, to Robert Fink, Staff Member of the House Government Operations Committee, May 10, 1976, reprinted in Abzug Committee Hearings, at p. 324

[71]See Church Committee Final Report, Vol. III, p. 769.

[72]United States v. United States District Court for the Eastern District of Michigan, 407 U. S. 297 (1972).

[73]18 U. S. C. 2511(3).

[74]United States v. Butenko 494 F.2d 593 (3rd Cir. 1974), cert den. sub nom United States v. Ivanov 419 U. S. 881 (1974).

[75]Ibid.

[76]Presumably, this would apply to purely domestic intercepts as well as international intercepts.

[77]The Butenko court also suggest that Fourth Amendment issues, as identified by the Supreme Court in Keith, supra, footnote 72, would be raised by surveillance conducted for other than foreign intelligence purposes. 494 F.2d at page 603.

[78]See Church Committee Hearings, pp. 20-23.

[79]See Church Committee Final Report, Vol. III., pp. 770-776.

[80]Ibid.

1/ Church Committee Hearings, ~~Hearings before the Select Committee to Study Governmental Operations with Respect to Intelligence Activities, "The National Security Agency and Fourth Amendment Rights", U.S. Senate, 94th Congress, 1st Session,~~ Vol. 5, p. 19. ~~(Hereinafter cited as Church Committee Hearings.)~~

2/ See Fink footnote 69

3/ See Fink footnote 70

4/ Church Committee Hearings, Vol. 5, p. 20.

5/ See Fink footnote 73

6/ Church Committee Final Report, ~~Final report of the Select Committee to Study Government Operations with Respect to Intelligence Activities, "Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans", U.S. Senate, 94th Cong. 2d Sess.,~~ Book III, pp. 736-37. ~~(Hereinafter cited as Church Committee Report.)~~

7/ General Allen stated that when the watch-list activity began, it was viewed as "an appropriate part of the foreign intelligence mission". See Church Committee Hearings, Vol. 5, p. 23.

8/ Testimony of General Lew Allen, Jr., Church Committee Hearings, Vol. 5, p. 16. See also the statement of NSA Director Bobby R. Inman before the Senate Subcommittee on Intelligence and Human Rights, as reported in the Washington Post, July 22, 1977. Inman ~~reportedly~~ stated: "Let there be no doubt, no U.S. citizen is now targeted by the NSA in the United States or abroad." for reasons indicated on p. 22 above, this statement is misleading.

9/ Senator Schweiker, at the Church Committee hearings asked former NSA Director Lew Allen, Jr.: "Is there any law that you feel prohibits you from intercepting messages between American citizens if one is at a foreign terminal and the other is at a domestic terminal, or do you feel there is no law that covers this situation?

"General Allen: No, I do not believe there is a law that specifically does that." (Church Committee Hearings, Vol. 5, p. 31.) See also discussion between Senator Mondale and NSA General Counsel Roy Banner at pp. 45-46.

10/ Senator Schweiker at the Church Committee hearings, asked ~~former~~ then NSA Director Lew Allen, Jr.: "Would it be possible--granted this is not your policy, and you state that you have not done so--would it be possible to use this ... apparatus that you have to monitor domestic conversations within the United States if some person with mal-intent desired to do it?...

"General Allen: I don't think I really know how to answer the question. I suppose that such a thing is technically feasible." (Church Committee hearings, Vol. 5, p. 31.)

11/ ~~Three such cases have been reported to the subcommittee.~~ In ~~the first~~ one, a U.S. businessman engaged in selling commercial building products to a Middle East oil sheikdom, reported that soon after his first international communication regarding such sale, he and his wife were visited by federal intelligence agents who were knowledgeable about the proposed sale. He further suspected that he was kept under surveillance thereafter until the sale was completed. He reported that every aspect of the transaction had been conducted using international communications.

In another ~~a second~~ case, a ~~senior partner of a~~ Washington law firm, which represented a client involved in international trade, reported that in litigation with the Justice Department, the government presented evidence which could only have been obtained through the interception of its clients international communications. The law firm did not feel it was in their client's best interest to pursue the matter, ~~however~~.

In the third case, a senior official of a large multinational U.S. corporation told the committee that he knew that NSA was intercepting its international communications. He stated that the company encrypted such communications but government regulations prevented the level of encryption from being so sophisticated that NSA would be prevented from reading it. He further stated, however, that the company felt such monitoring by the government to be "legitimate".

92/ Church Committee Hearings, Vol. 5, pp. 16-17.

93/ See New York Times, "Administration Maps Secret Plan to Fight Telephone Intrusion", July 10, 1977, p. 1; Washington Post, "Carter Seeking Ways to Block Interception of Classified Calls", July 11, 1977, p. A 3.

94/ Theoretically, NSA could determine what the Soviets were obtaining from U.S. domestic communications by monitoring Soviet transmissions leaving this country. ~~There has been doubt expressed by some authorities, notably David Kahn, author of The Codebreakers, however, that~~ NSA is able to break Soviet coded transmissions. ~~See David Kahn, "Embassy Burglaries? Old Hat.", New York Times, June 22, 1973.~~ If this is true, then it would seem that NSA may be forced to monitor domestic communications itself, if it hopes to determine what the Soviets are gaining from these intercepts. (See footnote 97-6)

95/ See footnote 8.

96/ Church Committee Report, Book III, p. 758. Recently, however, the Justice Department, for the first time, used evidence in a criminal prosecution specifically attributed to NSA interceptions. See Washington Post, "NSA Tapped Six Overseas Messages by Attorney for Sirhan, FBI Reveals", August 3, 1977.

97/ Church Committee Hearings, Vol. 5, p. 111.

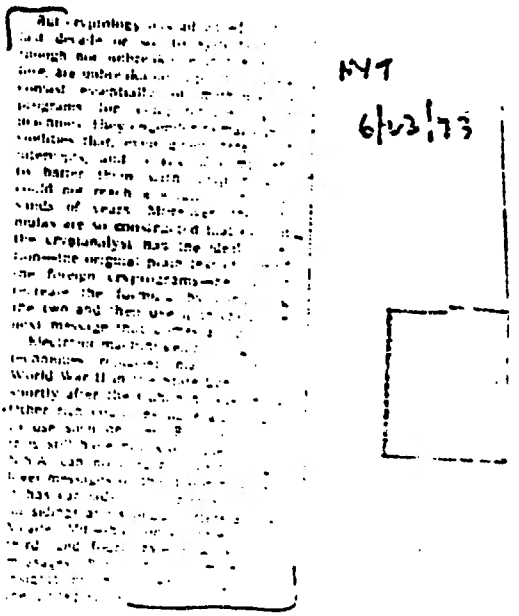
98/ Church Committee Hearings, Vol. 5, p. 18.

99/ Ibid., p. 16. Also, see footnote 8.

100/ Letter from Comptroller General of the United States, Elmer G. Staats to Chairwoman Bella S. Abzug, November 12, 1976.

101/ Ibid., p. 5.

FOOTNOTE 97-B Cont'd



NYT
6/23/75

If Kahn's assessment (along with others of a similar nature informally received)is accurate, and the Committee has little reason to doubt its validity, the NSA is largely "out-of-business" vis-a-vis the understanding of intercepted written foreign intelligence telecommunications traveling on circuits most often shared with U.S. citizens, into and out of the U.S. On these circuits it appears then, that the comprehensible COMINT "take" consists of: (a) relatively low-level encrypted messages of developed countries; (b) telecommunications of relatively unsophisticated countries; and (c) plain-text telecommunications.

ADDENDUM TO FOOTNOTE 30.

It should be noted that ~~xxxxxx~~ whereas almost all the message the telegraph companies turned over to MI-8 were transmitted by cable rather than radio (see p. above), this section is based upon statutes applicable to the interception of radio communications. During MI-8's operational lifetime, legal restrictions applicable to the interception and use of wire communications were non-existent, but the Army Security Agency apparently interpreted the statutes applicable to radio to also include cable (wire) transmissions.

N.B.

BRITT

Please verify accuracy of above - ~~xxxxx~~ change if necessary.

Add on to existing footnote):

81. Former CIA Director William E. Colby gave similar testimony on August 6, 1975, stating, "On some occasions, [the interception of U.S. citizens' telecommunications] cannot be separated from the traffic that is being monitored. It is technologically impossible to separate them." (Pike Committee Hearings, p. 241).

In fact, Mr. Colby's use of the expression "on some occasions" is misleading, inasmuch as the NSA constantly faces this problem in its search of international telecommunication links entering and leaving this country. Mr. Colby's semantic qualifier, "on some occasions," is not unlike his testimony before this subcommittee, and others, that the CIA's 20 year mail intercept program - which opened over 190,000 letters - was among "the few" individual instances of the Agency's domestic illegalities. (Cf., for example, "Central Intelligence Agency Exemption in the Privacy Act of 1974" hearings, House Subcommittee on Government Information and Individual Rights, March 5, 1975 (p. 5) and June 25, 1975 (pp. 139-40)).

81-A. Pink footnote 65.

Add on to existing footnote):

84. [redacted] In this procedure, written messages of potential interest are isolated from the mass of those transmitted by the use of computers programmed to selected "trigger" words or symbols. The [redacted] extracted messages are then studied by human analysts. [redacted] However, at overseas bases, many messages are apparently intercepted by human analysts prior to trigger word screening. Chet Flippo, an associate editor of Rolling Stone, reported that he was, in 1967, in the Naval Security Group (the NSA's naval wing), assigned to intercept telecommunications from a desert base in Sidi Yahia, Morocco. In addition to intercepting diplomatic cables, military messages, telegrams, transcripts of transatlantic phone calls, Flippo wrote, "I also screened reams and reams of transatlantic cables to and from the U.S., regardless of whether they contained any key words or names. Telegrams or phone calls involving American congressmen and journalists, 'dissidents,' multinational corporations -- were all targets." (Chet Flippo, "Can the CIA Turn Students Into Spies?", Rolling Stone, March 11, 1976).

84-A The Church Committee's report on the SHAMROCK program stated, "Of all the messages made available to NSA each year, it is estimated that NSA in recent years selected about 150,000 messages a month for NSA analysts to review. Thousands of these messages in one form or another were distributed to other agencies in response to 'foreign intelligence requirements.'" (Church Committee Hearings, Vol. 5, p. 60).

90-B The Pike Committee's final report noted that "preliminary investigation reveals at least one new area of non-political and non-military emphasis in international intercept - economic intelligence. Communications interception in this area has rapidly developed since 1972, partly in reaction to the Arab oil embargo and the failure to obtain good information on Russian grain production and negotiations for the purchase with American corporations." (Final Report as published in Village Voice, February 16, 1976, p. 88).

91-A. Letter from Lt. Gen. Lew Allen, Jr. to Chairman Otis Pike, House Select Committee on Intelligence, August 25, 1975; [redacted] op. cit., Village Voice, p. 90.

91-B. Until the formation of the Church Committee, these individuals were limited to selected staff members of the Armed Services committees in the Senate and the House, and the Defense subcommittees of the Appropriations committees in the Senate and the House. This Committee has asked several of these staff members if, in the course of exercising their Committee's oversight functions, the NSA had ever briefed them on Operation SHAMROCK. Some of these individuals replied they were generally aware that the Agency from time to time inadvertently intercepted private sector communications; others said the first they knew of such activity was when they read it in the newspaper. This Committee has received no indication that any of these individuals had a detailed knowledge of Operation SHAMROCK.

90-A [redacted] An attachment to a March 9, 1976 letter from Federal Reserve Chairman Arthur F. Burns to Sen. Frank Church, Chairman of the Subcommittee on Multinational Corporations of the Committee on Foreign Relations, indicates that Arab oil countries had over $11 billion on deposit with the six largest U.S. banks -- plus additional billions in other U.S. banks -- as of December 31, 1975.

The Federal Reserve refused to supply the multinational subcommittee with deposit totals of individual Middle East oil-producing nations, but the Washington Post noted that, in 1975, the government of Kuwait had $1.7 billion on deposit with the Citibank of New York, and in the same year foreign deposits accounted for nearly two-thirds of all monies deposited in both the Citibank and Chase Manhattan Bank, the nation's second and third largest banks. (Ronald Kessler, "Banks Hold Huge Foreign Deposits: U.S. Examiners Worried About Pressure From Governments," Washington Post, January 14, 1976, p. A-1). By June 30, 1976, the deposits of the Middle East oil-exporting countries in U.S. banks reportedly totaled around $19 billion. (Dan Morgan, "Senators, Banks Block Probe of Arab Deposits," Washington Post, October 10, 1976, p. A-1).

See staff report, [redacted] "International Debt, the Banks, and U.S. Foreign Policy," prepared for use of Senate Subcommittee on Foreign Economic Policy, of the Committee on Foreign Relations, August, 1977.

A senior official of a giant U.S. multinational financial institution, which has well over $1 billion on deposit from a single Middle Eastern oil producing nation -- as well as substantial deposits from others -- has advised the subcommittee that he has little doubt the NSA is intercepting and analyzing his company's telecommunications. But this official, knowledge about the company's telecommunications "risk safeguard management," stresses that the company is not concerned about NSA intercepts, which it feels are legitimate. (Telephone [redacted] interview, December 14, 1976).