OPTIONAL FORM NO. 10
JULY 1973 EDITION
GSA FPMR (41 CFR) 101-11.6

~~TOP SECRET~~ - COMINT MATERIAL ATTACHED

UNITED STATES GOVERNMENT

Memorandum

TO : Robert L. Keuch
Deputy Assistant Attorney General
Criminal Division

DATE: March 4, 1977

FROM : George W. Calhoun
Chief, Special Litigation

SUBJECT: Prosecutive Summary

Attached hereto is a copy of a draft of the prosecutive summary. (Corrections are being made).

As you will see, it contains some detailed information which might otherwise be unnecessary, but because Mr. Civiletti does not have a background in this area, the report has been expanded to fill him in and give him a perspective.

It goes without saying you should make any changes you wish, and if it is not acceptable at all, let me know. Also, if you need the underlying report let me know.

~~TOP SECRET~~

CLASSIFIED MATERIAL ATTACHED

SUMMARY OF TASK FORCE REPORT ON INQUIRY INTO CIA-RELATED ELECTRONIC SURVEILLANCE ACTIVITIES DISCLOSED IN ROCKEFELLER COMMISSION REPORT

Preface

As a result of information received from sources indicating that the Central Intelligence Agency (CIA) may have violated the laws regulating electronic surveillance, President Ford asked the Vice-President to head a Commission to investigate the Agency's activities and to prepare a report on the results of the investigation. The final report 1/ confirmed the existence of a number of questionable surveillances, and that prompted the Attorney General to establish a task force to investigate the Commission's findings and to determine whether there were any other questionable electronic surveillances which might have been conducted.

The investigation (including the Commission's discoveries) uncovered 23 different categories of questionable activities: however, of that group, only eight merit futher discussion, for five are barred from prosecution by the statute of limitations, and seven clearly possess no prosecutive potential.

1/ "The Report to the President by the Commission on CIA Activities Within the United States."

The following is a summary of the task force's report, a copy of which is attached hereto. This summary is divided into four parts: (1) a review of the applicable Presidential power and other purported sources of authority; (2) a brief review of Federal laws in this area; (3) a description of the eight operations, including a discussion of the primary defenses that would probably be asserted;[1] and (4) the task force's prosecutive conclusions.[2]

---

[1] The fifteen that were barred either by the statute of limitations or by a lack of any meaningful prosecutive merit will also be discussed briefly.

[2] A word of explanation at the outset concerning the approach of this summary is also in order.

While a summary usually recounts in a brief form the original, underlying document, the nature and breadth of this investigation made the use of that method impossible here. There were 23 different activities investigated, some of which spanned decades. In addition, there are many statutes, directives, orders, and policies - - as well as legal principles -- which had to be considered. A discussion of all of these would have required that the summary be rather lengthy. On the other hand, any effort to summarize all of these matters in a brief fashion would have done an injustice to the thoroughness of the investigation as well as an injury to the integrity of the report. For these reasons, the format of the following summary is somewhat different.

Starting with the main goal, which was to capture and recount the essence of the investigation and underlying report and to convey an understanding of the main reasons why the task force reached the basic conclusion it did - - that no prosecutions are warranted - - it was decided that a review-by-analogy approach would be the best method to employ. Thus, a couple of the more prominent authorities and pervasive activities were selected as being representative, and they were discussed in greater detail. Then, the principles and problems they presented were analogized to the remainder of the activities.

In adopting this approach, we realize that the method chosen is subject to the criticism that the wrong examples were used or something important was either not stressed or (worse yet) left out. Still, brevity, necessity, and our main goal mandated the choice made.

I

The Rockefeller Commission Report and the task force investigation revealed that at least three agencies[1] had conducted a variety of electronic surveillances over the past thirty some odd years in the name of national security. To whatever extent they claimed the power to do so, the agencies pointed to the Office of the President as the main repository of their power, and they asserted by way of a general defense that various directives and pronouncements from that Office gave them the power to do what they did.

This position required the task force to investigate not only the agencies' activities but the authority they relied upon -- the Presidential power to authorize a NSES[2] program and any directives, orders, or pronouncements that may have issued from that Office delegating that power. In addition, the task force had to review the two wiretap statutes 18 U.S.C. 2511 and 47 U.S.C. §605.

In order to understand the interplay among these elements, and particularly how they impact on the activity involved in this investigation, it might be helpful to review the evolution

---

[1] The Central Intelligence Agency, the National Security Agency, and the Federal Bureau of Investigation. Because the FBI halted its participation in most, if not all, of these activities prior to the running of the statute of limitations, it was not an object of this investigation.

[2] A national security electronic surveillance.

of the primary penumbra which covers whatever power exists in the area --- the Presidential power -- and then look at origin and the scope of the two wiretap statutes, especially as they relate to the exercise of the Presidential power.

A

Development of the Presidential National Security Power

As Commander-in-Chief and as the Chief Executive responsible for coordinating the Nation's defense efforts, the President has, quite expectedly, a number of so-called national security powers. One of those is the power to authorize a NSES. Unfortunately, this power did not spring full grown from one source, such as the Constitution; rather, it started with an idea and grew steadily over the better part of four decades. As we shall see, from the day of its inception, the power was never clearly described and, more importantly, its breadth seemed at times virtually open-ended. As a result, it quite naturally spawned in the minds of some the idea that the rubric of national security ensured the legality of their actions.

* * *

The entire wiretap problem started quite by accident when a little over a century ago (1875) the Nation's first telephone

call was made.[1] Interestingly, it may have been monitored, albeit consensually, and since then, surveillance of other telephone conversations has become a considerable problem.

Today, there are three ways under Federal law that one can legally wiretap a communication: (1) by obtaining the consent of one of the parties; (2) by obtaining court authorization; and (3) by having the Attorney General, acting for the President, authorize it as a national security surveillance. This is the type of tap involved here. Thus, the development of this national security power is helpful in understanding why the agencies did what they did, and what they would assert as a defense if their employees were prosecuted.

* * *

Partly in response to the concerns of civil libertarians that too many phone calls were being monitored, Attorney General Sargeant issued an order in 1928 prohibiting what was then known as the Bureau of Investigation from engaging in any wiretapping for any reason. Soon thereafter a new component, the Prohibition Unit, was transferred to the Department and became a new Bureau. Because the nature of its work required that the Bureau engaged in

---

[1] "Mr. Watson, come here; I want you."

wiretapping, then Attorney General Mitchell found himself facing the potential inconsistency of one Bureau being permitted to tap while the other was not. After reviewing the matter fully, Attorney General Mitchell took the first of six significant steps toward our present policy when he decided for the first time to permit the Federal government to conduct wiretapping, albeit on a very limited scale: only the telephones of syndicated bootleggers could be tapped. 7/

Within a year, General Mitchell found it necessary to expand the scope of permissible wiretapping to include "exceptional cases where the crimes are substantial and serious, the necessity is great, and [the Assistant Attorney General is] satisfied that the persons whose wires are to be tapped are of the criminal type." 8/

For nine years thereafter, the Department's policy remained relatively unchanged. Then, on March 15, 1940, in response to a temporary public outcry against the practice, Attorney General Jackson reinstated the original, total prohibition against all wiretapping. His order was short-lived for two months later

---

7/ Thus, Attorney General Mitchell was the first to "authorize" wiretapping of American citizens; unfortunately, his namesake many years later, John N. Mitchell, is usually (and quite mistakenly) given that dubious honor.

8/Whenever quotations are set forth, they represent the totality of the pronouncement touching on the point, so any concern in the mind of the reader with the unusual breadth and vagueness (by today's standards) is well founded.

President Roosevelt took the second (and unquestionably the most important) step when, in a memorandum to the Attorney General, he expressed his opinion that electronic surveillance would be proper where "grave matters involving the defense of the Nation" were involved. Now, the Department's wiretapping policy included, although rather cryptically, surveillance for national security purposes./

By now, the clouds of war began to appear on the horizon, and late in 1941 the Department's policy underwent another significant change: We began to recognize "Presidential authorization[s] for the intercepting of foreign messages and matters dealing with espionage, sabotage and subversive activities." (Emphasis supplied.)" The significance of this change was doubly important: First, the source of the power was, for the first time, specifically declared to repose in the Office of the President, and second, the basis of the power -- national security -- began to sharpen in focus. Because of the significance of these changes, we should pause and review in a little more detail the recorded basis for these changes.

/ Along with announcing the newly discovered power, the President also implied that it reposed in his Office by transferring it to the Attorney General and saying he was authorized to approve "listening devices [directed at] persons suspected of subversive activities . . . including suspected spies."

The new description of the President's power was contained in a memorandum from Director Hoover to the Attorney General, in addition to which he said: "The President indicated [to the Director] that as Commander in Chief of the army and navy, under the National Emergency, he believed that he had the authority to authorize such [surveillances]." Then, curiously, the Director questioned the President's decision by suggesting that it would be "highly desirable that some definite decisions be made by the Department of Justice relative to the legality of the [wiretapping activity]."[1]

As a result of that request, Solicitor General Fahy was directed to look into the matter, after doing so he concluded that surveillance could be conducted where the matter "affected the national security." Based in part on this recommendation, Attorney General Biddle concluded that certain surveillances he had previously authorized the Bureau to conduct would be permitted to continue if "they have developed evidence of

---

[1] Perhaps the suggestion was not really unusual in light of Director Hoover's strong dislike for wiretapping.

solely for intelligence gathering purposes, rather than for gathering evidence for a trial.

Although it is not entirely clear why, it seems this intelligence gathering rationale was developed during this period in an effort to reconcile the Department's wiretapping policy with a troublesome proscription in what was then the only wiretap statute.[1]

Under §605, , it was illegal to intercept and divulge the contents of a wire or radio communication. Thus, the results could not be used at trial. But there was a problem. The past descriptions of the national security power said it could be exercised to gather information about espionage, sabotage and the like, all of which are crimes. If the evidence could not be used at trial, what was the reason for gathering it? The only answer was, of course, the one Director Hoover mentioned -- intelligence purposes.

The first time Director Hoover mentioned the idea, he said: "the first consideration in any intelligence operation is that of acquiring information to enable the Executive branch of the government [1] to take preventive measures against outbreaks

---

[1] 47 U.S.C. §605, discussed infra.

of violence or [2] to control espionage on the part of subversives."[1]

Two years later, the Director said: "The FBI has an intelligence function in connection with internal security matters equally as important as the duty of developing evidence . . . . [F]or the FBI to fulfil its important intelligence function, considerations of internal security and the national safety are paramount and, therefore, may compel the unrestricted use[2] [of such surveillances]. (Emphasis supplied.)

During this period in which Director Hoover was claiming "unrestricted use," NSA was created. Its "enabling statute" which was really not a statute but a Presidential Directive (called NSCID #9),[3] contained the following provisions:

---

[1]/Later, as we shall discuss, these two bases were to be expanded, included in a new wiretap statute (18 U.S.C. §2511(3)) and become known generally as domestic and foreign intelligence surveillance.

[2]/There is no recorded disclaimer of this idea in the Department's records.

[3]/These will be discussed in more detail later.

> The special nature of [NSES] activities requires that they be treated in all respects as being outside the framework of other or general intelligence activities. Orders, directives, policies, or recommendations of any authority of the Executive branch relating to the collection * * * shall not be applicable to [such] activities, unless specifically so stated and issued by competent departmental or agency authority represented on the Board. Other National Security Council Intelligence Directives to the Director of Central Intelligence and related implementing directives issued by the Director of Central Intelligence shall be construed as non-applicable to [such activities, unless the National Security Council has made its directive specifically applicable to COMINT.

Thus, NSA was born in a period of "unrestricted use" and its birth certificate (which was, by the way, top secret) said it did not have to follow the limitations in the NSES area that limited other agencies unless it was expressly directed to do so.

For the next decade, the intelligence-gathering idea simmered,[1] until President Johnson issued an Order making the next significant change in the Department's policy. On June 30, 1965, he sent a memorandum to all Executive Departments and agencies severely limiting electronic

---

[1] During this period Attorney General Kennedy directed that existing wiretapping procedures and practices "are continued in force."

surveillance by the Executive Branch in the future. However, after stating that surveillance "may sometimes be essential in protecting our national security," he expressly directed that this type of surveillance was not prohibited by the order, but rather limited its use solely to cases in which the national security is at stake."[1]

Two years later, on June 16, 1967, Attorney General Clark issued a similar memorandum, but he too expressly excluded its limitations from applying to "investigations directly related to the protection of the national security."[2]

By now, the pressure for a new wiretap statute forced Congress to act, and it precipitated the fifth major change in the Department's policy when it passed a new wiretapping law 18 U.S.C. §2510, et seq. (Title III of the Omnibus Crime Control and Safe Streets Act of 1968.)

The only existing wiretap statute prior to that time was 47 U.S.C. §605, and for a number of years after that Act was passed,[3] the Department had repeatedly sought (and invited) legislation from Congress which would both permit wiretapping and allow the use of the results or fruits of such surveillance at trial, but Congress, however, declined to act. By 1967,

---

[1] Nothing was said about NSA.

[2] Ibid.

[3] 1934.

though, a consensus was gradually reached in Congress that additional legislation was necessary; and as a result, it enacted Title III.

Although the new Act established procedures whereby a warrant could be obtained for conducting certain kinds of electronic surveillance, our concern here is limited primarily to one Section, §2511(3). Because this part of the new statute will be discussed in greater detail later, it will not be recounted verbatim here now, but it is important to point out for now that that Section expressly exempted the President's power from the coverage of the provisions of Title III.

Late in the fall of 1970, the Supreme Court forced the last major change when it held that in the Keith case that the President did not have any power to authorize a NSES for domestic purposes.[1] Of course, its decision three years earlier in Katz v. United States, 389 U.S. 347, in which it held that all wiretapping was subject to fourth amendment limitations, was a factor, both in the enactment of Title III and in its approach to later cases. Keith, however, has a more direct relationship to the Commission's investigation and this report.

---

[1] United States v. Sinclair, 321 F. Supp. 1074 (E.D. Mich. 1971), petition for mandamus denied sub. nom. United States v. United States District Court for the Eastern District of Michigan, Southern Division, the Honorable Damon J. Keith, 444 F. 2d 651 (6th Cir. 1971), aff'd, 407 U.S. 297 (1972).

This, then, is how the Presidential power to authorize an NSES came about,[1] and as we have seen, it was expressly exercised in at least one way - - by giving the Attorney General the power to permit the Bureau to engage in NSES activity.

It was also exercised in another important way - - by directives and orders, the President, gave two members of the intelligence community the power to conduct certain NSES programs. Thus, a brief(er) review of those are in order.

[1] There have been other equally significant changes in the power since Keith, especially its description and guidelines, but our concern here is limited to the scope of the power as it existed when the acts discussed herein were committed.

A

"Major Operations"

A number of the activities the task force investigated involved programs which spanned many years and which tended to ebb and flow over the period. And, more often than not, the program lacked a specific directive, order, or statutory basis; instead, its authority was a combination of elements. For our purposes here, we will select one such program (perhaps the most pervasive), trace its development, and then explain why a prosecution would be inappropriate. We believe the same principals which dictated that conclusion apply as well to the other programs which will be discussed, but much more briefly.

"SHAMROCK" was one of the most pervasive programs the task force discovered, spanning over 30 years; like so many things that grow to massive proportions, however, "SHAMROCK" started very innocently.

(footnote continued from page)

In addition to these, the task force discovered a second category of activity , which, though questionable, was non-prosecutable. For example, NSA and CIA engaged in a number of support activities which helped wiretapping programs. They obtained telephone toll records, [redacted] supplied the D.C. Police Department and the Secret Service with wiretapping equipment, supplied an office to assist in a program to review domestic telegram traffic, and recruited agents and introduced others to them (agency representatives and personnel provided to assist their communication carriers). All of these activities, while relating to other various wiretapping programs, did not themselves involve intercepting communications; thus, they clearly did not violate the wiretap statutes.

Faced with the ever-increasing threats posed by Japan and Germany, Director Hoover started working with the Department on a proposed executive order to permit the program, but before the Order could be finalized, Pearl Harbor intervened.

Congress, acting with uncharacteristic swiftness, enacted what was later to be called the Censorship law, and on December 22, 1941, the Solicitor General told the Bureau that the proposed Executive Order would no longer be necessary, for the newly created Office of Censorship would have full authority over international communications, and the FBI could obtain any that it needed from that Office in the future.

While all this was occurring, though, the Bureau was moving ahead. Very soon after December 7, the Bureau was requested by the State Department to ask the appropriate cable companies to hold up the transmissions of messages to certain countries for 24 hours, and then to make copies of the cables available for review. The requests were made and suprisingly, yet understandably, the companies readily agreed. The Attorney General was promptly advised, thereby putting the Department on notice the program had begun.

_/cont'd
cooperate, but this time they did so expressly on the ground that they felt they were prohibited by law from doing so and would be subject to possible prosecution if they complied! As we shall see, this was a continuing concern of the companies and, unfortunately, their initial instincts would, many years later, prove to be correct.

Once again, as in 1940, the cable companies' survival instincts were aroused, but this time they were in a different position: they were already supplying the cable copies. Nevertheless, their concern soon mounted, prompting them to seek assurances that the "federal government [could] guarantee to (sic) commercial communication companies against criminal liabilities resulting from these companies furnishing to the Army certain documents and traffic."[1]

Twice -- in 1947 and again in 1949 — the companies were given the assurances they sought. Of more than passing interest, though, was something else than Secretary Forrestal said to a group of executives of IT&T and RCA:[2]

> . . . while it was always difficult for any member of the Government to attempt to commit his successor, he could assure the gentlemen present that if the present practices were continued the Government would take whatever steps were possible to see to it that the companies involved would be protected.

---

[1] For some unexplained reason, no mention was made of the companies' practice of supplying copies to the Bureau.

[2] Initially, Secretary of Defense Forrestal told the group he was speaking for President Truman in commending them for their cooperation and requesting their continued assistance because the intelligence constituted a matter of great importance to the national security. Two years later, on May 18, 1949, Secretary of Defense Johnson met with officials of the same companies and stated that President Truman, Attorney General Tom Clark, and he endorsed the Forrestal statement and would provide them with a guarantee against any criminal action which might arise from their assistance. Former Secretary of Defense Laird, as late as 1973 when the program was halted, said "SHAMROCK" was also tacitly endorsed by him.

He also said that, so long as the present Attorney General was in office, he could give assurances that the Department of Justice would also do all in its power to give the companies full protection. In an effort to clarify this latter point, a company official inquired if Mr. Forrestal was speaking not only for the Office of the Secretary of Defense, but also in the name of the President of the United States. Mr. Forrestal replied that that was correct.

Two years later, essentially the same representations were made, however, the memorandum reflecting that fact had an interesting pair of handwritten notes, one saying, "OK'd. by the President and Tom Clark," and signed by Louis Johnson, and the other initialed as approved, "T.C.C.," presumably meaning then Attorney General Tom Clark.

Though Congress repealed the Censorship law, it recognized the need of the President to get advise in certain domestic, foreign, and military areas, particularly as they relate to national security matters, so in response to that need, Congress enacted a law which established the National Security Council (NSC). Five years later, in 1952, the President signed a directive which created the National Security Agency; the functions assigned to it included responsibility for "SHAMROCK".

For the better part of the next two decades, the Bureau worked closely with the newly-created Agency, becoming a regular courier between the Agency and the companies for the purpose of picking up cable traffic. Then, for reasons not of moment here, the Bureau withdrew its participation in the program in 1973, and in May of 1975, "SHAMROCK" was halted entirely when the Agency also stopped the practice.

When NSA first assumed responsibility for the "SHAMROCK" operation in 1952, the practice and the procedures had already been established for more than a decade. Those procedures permitted NSA employees access to all diplomatic messages handled by the RCA, ITT, and Western Union offices located in New York City and Washington, D. C., as well as the RCA and ITT offices in San Francisco. RCA provided NSA employees with duplicates (drop copies) of all international messages, thus requiring NSA employees to visually screen and select out diplomatic messages for microfilming on NSA-owned machines located on the RCA premises. Western Union and ITT (starting in 1945), went further, providing NSA agents with a daily microfilm of diplomatic messages which had already been selected out and photographed by company employees on NSA-owned [illegible] machines. The investigation also shows that NSA employees were given access to all perforated paper tape copies of international messages transmitted by RCA and possibly from ITT.

[redacted] NSA started to select out other international messages containing the names of persons on what was called the watch lists.[1] [redacted]

Statutes

Though it would seem that the companies, the FBI, and NSA violated clauses one and three of §605,[2] there are a number of problems with trying to prosecute anyone for this activity, including the following possible defenses:

(1) Prior Presidents and Attorneys General had notice of and, in at least one case, appeared to approve the operation;

(2) Two Secretaries of Defense had tried to give the companies immunity;

(3) Clause one of §605 permits companies to disclose information "upon demand of lawful authority;"[3]?

---

[1] This was a list of names maintained by NSA for other investigative agencies of persons about whom the agencies wanted investigative information, usually for domestic security reasons. This use of this list continued until 1973 when Attorney General Richardson terminated the practice.

[2] Title III does not apply for the collection method was non-aural -- copies of telegrams and magnetic tapes containing electrical impulses. Accord, Smith v. Nunker, 356 F. Supp. 44 (D.C. Ohio, 1972

[3] A few years ago, a United States attorney asked the Department what that exemption encompassed, and in reply we said the term "embraces any state or federal agency authorized by state or federal law to demand, by subpoena or otherwise, the production of books, records, papers, or other documents," (Emphasis supplied.) While the statute speaks in terms of a "demand," the requests to the companies here were, at most, patriotic pleas plus parting (footnote continued)

(4) There was no divulgence outside the Executive Branch, so there was no divulgence within the meaning of §605;

(5) A use which benefits the Government is not the type of "use" contemplated by the statute;

(6) It is not illegal to "ask" a company to give out copies of cables. If the company complies, it may be violating the statute but the recipient would not; and

(7) The putative defendants acted in good faith, and they lacked the necessary intent to prove a violation of the law.

In addition to these problems, there are a number of other reasons which militate against prosecution.

First, as is clear from a review of a evolution of the President's power from its inception, the true scope of the President's power (with which the Bureau and the Agency were familar) was unknown. And although by today's standards the power was virtually open ended, "SHAMROCK" would have fitted quite easily, then within its parameters, especially in 1941 when the program started. That, coupled with the notice to the Attorney General could lead one to believe he had accepted it under the President's NSES power.

/(footnote cont'd)
promises of protection. Still there is a question whether the agencies could be said to come within the demand part; moreover, this defense could only be advanced by the companies, not the Agencies.

Second, it would be singularly unfair to carve out for prosecution those who carried out the program the last three years it was in existence when they had no reason to question the legality of a program that had gone on for 30 years.

Third, although it is not directly controlling here, the directive which created NSA and gave it certain powers to collect information expressly provided that because of the special nature of their work, prohibitions contained in "orders, directives, policies. . . of the Executive Branch relating to the collection . . . of intelligence . . . shall not be applicable to [such] activities, unless specifically so stated. . . ." Thus, agency employees could very easily have concluded that if there was a prohibition to the program, it did not apply to them (Throughout all of this, it is also important to keep in mind that the potential defendants are all laymen and, as we have seen, the law in this area is complex.)

Fourth, Congress, by funding this program, undoubtedly had some understanding of its existence. We also know that various Presidents and cabinet officers knew of the program but did nothing to halt it, thereby permitting agency personnel to believe it had Executive approval.

Fifth assuming it could be shown that a President impliedly authorized the program, and assuming he had the power to do so, Section 2511(3) would exempt the program from either wiretap statute coverage. Finally, even if the statute (§605) applies all of these reasons indicate the potential defendants acted in good faith sufficient to negate the criminal intent.

For all of these reasons, the task force recommends against prosecution of power and agency personnel for operation "SHAMROCK"

As noted earlier, other programs will be discussed briefly. While each employed different means of surveillance, presenting different problems under §605 and/or §2511, they share many common defenses. More important, the basic question involved -- whether it is just to prosecute individuals for these activities -- remains the same.

* * *

NSA had two other programs that fall within the "Major Operation" group -- MINERET and [redacted]

MINERET was started in July of 1969, and it formalized the agency's practice of collecting information for the Secret Service and the FBI about people in whom they had an interest. (e.g., civil disturbance and national security information).

MINERET gathered intelligence from a variety of communication programs involving both aural and non-aural communications. Some

of the input for this program came from operation "SHAMROCK", but other than that, the MINERET input came from communications that had at least one terminal in a foreign country. (The interceptions occurred both from within and without the United States.)

In mid-1970, MINERET was enlarged to include checking to see if any intelligence concerning narcotic trafficking was picked up incidentally as a by-product of its work. Later, it included the use of a watch list

[redacted]

The task force recommends against prosecution for a number of reasons.

First, the Attorney General decided in 1971 that electronic surveillance to obtain intelligence concerning potential domestic violence was within the President's national security

power. Second, as late as November of 1975, the Attorney General suggested to the Senate Select Committee that it was arguable there was no reason for people to expect privacy if their communications are transmitted by radio; therefore, the Fourth Amendment would not apply. (This conclusion would include the wiretap statutes as well.) These positions would undoubtedly be asserted as a defense to any prosecution. In addition, there is the problem of the TOP SECRET order concerning NSA mentioned earlier, and which suggested they were not under the same prohibitions as other members of the community. On that point, the Senate Select Committee concluded in a recent report that there were no existing statutes which controlled, limited, or defined the intelligence activities of the NSA; that no statute or executive order prohibits NSA from monitoring a telephone circuit with one terminal in the United States; and that there is no statute which prohibits the watch list program. 1/

So, as with "SHAMROCK" an argument could be made that MINERET [redacted] violated at least one if not both of the wiretap statutes; however, any prosecution would have to overcome all of these problems, and the prospects of that seem very slim. For these reasons, the task force recommends against prosecution of any agency personnel for MINERET [redacted] activitie

1/ S. Rep. No. 94-755, 94th Cong., 2nd Sess., Book___pp. 736, 756, 761 (1976).

* * *

The final "major operation" involves a program first named NARCOG.

In October 1969 the President, deeply concerned with a number of serious problems arising from international narcotics traffic, established the White House Task Force on Heroin Suppression, and CIA was directed by the President to provide the task force with assistance. A CIA office of Narcotics Coordinator was established (and later reorganized under the name of NARCOG) to provide representation of CIA on the working group, liaison with other agencies, and intelligence reports and studies concerning the principal areas of task force concern [redacted]

In August 1971, the President up-graded the priority of the program by replacing the task force with a Cabinet Committee on International Narcotics Control (CCINC). The CIA Coordinator was named chairman of a subcommittee, and it continued to provide BNDD (also a member of the Intelligence Subcommittee) with foreign narcotics intelligence.

The information gathered by CIA was obtained primarily as the result of incidental surveillance by NSA (e.g., MINERET [redacted] and then a review to see if any by-product of the NSES activity involved drugs. In addition, CIA engaged in other overseas interceptions specifically conducted to gather international narcotics intelligence.

When overseas CIA stations inadvertently acquired information concerning the narcotics trafficking activities of U.S. citizens as the result of electronic surveillance, the local CIA official would reportedly surrender the information to his local BNDD counterpart and take steps to insure that no further collection on the U.S. citizen occurred.

The task force believes a prosecution for NARCOG would be inappropriate in light of the problems which arise because of the implied Presidential authorization which caused the activities to start. In addition, neither NSA nor CIA conducted any specific surveillance of American citizens specifically to meet its responsibility under NARCOG; the only information supplied was information gathered from intelligence collected for other purposes; in short, it was by-product information. (To whatever extent CIA wiretapped, it was (with one exception discussed next) done totally outside the country, and it did not involve this Nation's communication system, and therefore it did not violate the wiretap statutes.) For these reasons, the task force recommends against prosecution.

"Minor Operations"

[redacted]ran for a four month period during 1972-73 during which the CIA intercepted (by radio) certain radio

telephone communications between this country and Latin America (the surveillance was directed against a foreign target) for the purposes of gathering narcotics information. The interceptions occurred within this country.

There are, as we discussed earlier, a number of directives authorizing CIA to gather intelligence information and those, coupled with the President's insistence that the agency contribute to the maximum extent possible and "mobilize its full resources to fight the international drug trade." could be construed by some to be tantamount to Presidential authorization under §2511(3). In addition, it was during this time that the President considered narcotics control a matter of foreign policy. He said it was imperative to halt the flow of drugs; that drugs were a menace to the general welfare of the country, that the drug fight was one of the most important, the most urgent national priorities; and that keeping drugs out of the country was as important as keeping the enemy from entering.

Congress has also recognized the need for such intelligence and the general propriety of utilizing CIA and NSA to obtain it, at least to the extent it provided for the funding of such programs and received reports of the results, e.g., budget requests.

While these factors do not bar a prosecution as such, they do act to cloud the issue considerably so the chances of a conviction are considerably slim.

[redacted]

* * *

[redacted]

Also of importance here is the fact that the program was conducted pursuant to the agency's guidelines and approved by its general counsel. For these reasons, the agency personnel could be said to have acted in good faith which, if true, would tend to frustrate any chance of proving the requisite criminal intent.

Accordingly, the task force recommends against prosecution.

* * *

[redacted]

[redacted]

[redacted]

* * *

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

The chance of a successful prosecution are not very good for an important element, criminal intent, would be difficult to prove, and there are serious questions whether the temporary-interception-and-destruction practice would satisfy the "divulgence" or "use" elements of 605.

For all of these reasons the task force recommends against prosecution for these testing practices.

CONCLUSION

This report quite obviously did not focus on the particulars upon which affirmative prosecutive decisions may be made in specific cases. Rather, it attempted to provide the important legal and factual detail one should consider in determining whether inquiry into any specific activities should be terminated for lack of prosecutive potential or whether further investigation should be pursued, e.g., by grand jury.

The task force recommends that all further inquiry be terminated, for there appears to be little likelihood, if any, that convictions could be obtained on the basis of currently available evidence or evidence which might reasonably be developed.

B.

Sources of Authority Other Than The Presidential Power

While no specific authorization or exemption permitted some of the CIA and NSA intelligence activities involving interceptions of communications otherwise proscribed by §2511 and /or §605, a number of factors -- in addition to the Presidential national security power -- suggest that the Agencies were reasonable in believing these activities to have been lawful. Included are the historial purposes of, and subsequent directives given to, the Agencies; the interrelation between their national security function and the criminal justice function of the other federal agencies with whom they worked; the broad powers conferred upon them by statute; and the express or implied approval given by various officials.

The National Security Council and the CIA were established pursuant to the National Security Act of 1947, 50 U.S.C. §401, et seq.. Under that Act, NSC's primary function is to advise the President with respect to the integration of domestic, foreign, and military policies relating to the national security so as to enable the military services and the other departments and agencies of the government to cooperate more effectively in matters involving the national security. 50 U.S.C. §402. Its membership includes, among others, the President, the Vice President, and the Secretaries of State and Defense.

CIA also finds support for its intelligence gathering activities from NSCID 5, which, since 1958, has delegated primary responsibility to the CIA for cladestine activities abroad "in order to meet the needs of all departments and agencies concerned in connection with the national security." This authorization, along with the CIA's more general power under §403(d)(4) to "perform ... such additional services of common concern as the National Security Council determines can be more effectively accomplished centrally" explains the Agency's view that such actions were authorized.[1]

In a similar fashion, NSA draws support for its activities from NSCID 6, which has provided, at least since 1958, for NSA to provide "signal intelligence" for all intelligence agencies. "Signal intelligence" as defined therein, is intelligence produced by the study of foreign communications. To implement this NSCID, and to insure that it is involved only in "foreign" communications, NSA's long-standing policy has been to intercept a communication only if it has at least one-terminal outside the United States.

---

[1] It should also be reiterated that NSCID9 exempted CIA and NSA from restrictions publicly placed upon intelligence activities.

In addition to those direct sources of authorization, other statutes and actions reasonably suggest that CIA and NSA were not covered by the stricture of §2511 or §605.

[redacted]

Another good example is in the area of narcotics intelligence gathering. In addition to the sources of authority already discussed, the Federal Narcotics and Drug Abuse Act of 1973, 5 U.S.C. §901 et seq., acknowledges that both CIA and NSA have functions relating to the collection of information concerning trafficking in narcotics and dangerous drugs. And here, as in other areas, presidential memoranda closely linked national problems like narcotics with the national security. This too, according to the Agencies, caused them to believe their actions were within the law.

Finally, there are a number of other events from which NSA and CIA derive support - - or at least approval - - for their surveillance activities.

In July of 1973, William Colby testified before the Senate Armed Services Committee on his nomination to become DCI. In response to a question specifically addressed to whether CIA was then engaged in assisting law enforcement agencies in addition to the FBI, Colby replied in the affirmative, stating that CIA routinely disseminated its foreign intelligence reports to such agencies as the Drug Enforcement Administration, the Immigration and Naturalization Service, the Customs Service, the Secret Service, and the Armed Services. Since there was little doubt that a least some of CIA's information was governed by electronic surveillance, the Agency regards the lack of congressional objection as tacit approval of such dissemination.

More direct approval by the Executive Branch is provided by a February 3, 1971, NSA memorandum in which NSA officials described separate briefings two days earlier of Attorney General Mitchell and Secretary of Defense Laird on certain NSA activities. This memorandum reflects that both Mitchell and Laird read and approved a proposed memorandum which set forth proposed ground rules for NSA contribution to intelligence gathering for domestic problems. [redacted]

[redacted] CIA files also reflect that the same memorandum was read and approved in 1972 by Richard Kleindienst, then Attorney General.[1]

The participation of the Office of the General Counsel of NSA in the drafting of §2511(3), and the assurance of that office to the Agency that the effect of the subsection was to remove any doubt as to the legality of NSA surveillance is another factor cited by that Agency. A 1968 memo from the General Counsel to the Agency states that the language of §2511(3) "precludes an interpretation that the prohibitions against wiretapping or electronic surveillance techniques in other laws applies to [NSA activities] ... Wiretapping and electronic surveillance techniques are, therefore legally recognized as means for the Federal Government to acquire foreign intelligence information and to monitor U.S. classified communications..."

[1] Although Mr. Kleindienst has no recollection of this briefing, he did not dispute the CIA memo. Mr. Laird also did not remember seeing the memorandum or attending the briefing, but said the memo contained nothing he did not generally know of as early as 1964, when he served on the House Armed Forces Appropriations Subcommittee.

NSA also notes that NSCID 6 has provided, since 1958, that the departments and agencies being served are responsible for informing the NSA Director of the information desired. NSA interprets this language to require the implicit assurance by the agency seeking intelligence that the request is appropriate. Hence the responsibility is on the requesting agencies to frame their requests in accordance with the law. In 1973, Department of Defense General Counsel approved this interpretation, and stated that NSA was operating within the law.

Finally, NSA files reflect that since 1962 the Justice Department has sent hundreds of names of racketeers to NSA, requesting any information it might have concerning them. This too indicates that the Department did not regard this dissemination unlawful.

In reviewing these justifications, it must be remembered that some sources of authorization were after the fact, that others could not legally be relied upon, and, most important, that 50 U.S.C. 403(d)(3) expressly provides that the CIA shall have "no police, subpoena, law-enforcement powers, or internal security functions." Nonetheless, it appears from a number of authorities that no one really was clear on precisely what the Agencies could and could not do, that they were encouraged to become involved in law enforcement activities, and that no one, at least in any direct fashion,

ever seriously warned them that their actions were contrary to law. Thus, it seems harsh to charge either CIA or NSA employees with the responsibility of foreseeing the legal limits of their activites.

We will now turn to a discussion of the federal statutes which regulate the interception of communications.

C

Wiretap Statutes

Section 605 and Title III were premised on a few basic yet important principles which should be kept in mind when reviewing the statutes.

The basic purpose for enacting §605 in 1934 was to protect the integrity or the privacy of the Nation's communication's systems. In an effort to reach that goal, the statute regulated the conduct of personnel who worked for communications companies, and anyone else who might attempt to invade the integrity of such systems without proper authority.

Unfortunately the framers of the legislation fell somewhat short of their goal. They required, for example, that, before a violation could be shown, there must be both an interception and a divulgence of a communication, rather than a mere interception. This additional requirement allowed much wiretapping to slip through the crack. And, to the extent the drafters intended §605 to cover all electronic communications or electronic interceptions, they failed for Section 605 is, by its terms, limited to wire and radio communications, thereby exempting a host of esoteric communication techniques which would be developed in later years; e.g., laser and micro-wave communications.

Thirty-four years later, Congress enacted another wiretap statute; it too, however, had some important gaps.

The new statute, Title III, overlapped its predecessor by taking over the regulating of wire communications, but it also expanded the coverage to a new area: oral communications. Still, like §605, there were some noticeable gaps. First, the statute does not cover communications transmitted purely by radio; therefore, such communications require the "divulgence" element of §605. In addition, the new statute is limited to aural acquisitions (through the sense of hearing), thereby eliminating from its coverage many other surveillance techniques.[1] As mentioned earlier, though, the most important aspect of Title III is that it exempted from its coverage, as well as from §605, the President's power to authorize NSES.

With this as background, we turn first to a review of the specific statutory prohibition of §605 and Title III; then we will look at the Presidential power "exemption."

* * *

The stark contrast between the simplicity of the descriptions of the President's NSES power and the

---

[1] E.g., silent messages sent by electrical impulses, rather than by a voice which can be heard.

complex scope of §605 should, standing alone, prompt some sympathy for fledgling agencies created -- as were CIA in 1948 and NSA in 1952 -- in the midst of this development and then charged with the very serious task of gathering adequate intelligence to protect the Nation's security. An analysis of the 1934 Act quickly reveals why.

One of the earliest courts to analyze §605, Sablowsky v. United States, 101 F. 2d 183 (3rd Cir. 1938), started by noting that §605 has four major clauses. The first provides in essence that:

> No person receiving or transmitting any communication shall divulge the contents [improperly]. __/

Sablowsky held that this referred to a communications company employee and prohibited him from divulging something he had

---

__/ Each clause has many phrases and words we will ignore for our purposes here, for they are often synonyms which the drafters hoped would make sure that no unintentional gaps were left. For example, when referring to a communication, the Act refers to its "existence, contents, substance, purport, effect or meaning." We have selected one -- contents -- to represent the group. Also, for this part of the discussion, we will review §605 as it existed prior to the 1968 Act.

received lawfully.[1] (A major part of the task force's investigation involved telegraph and telephone company personnel who had helped various agencies to intercept and receive many private communications.)

The third clause, which, like the first, involves receivers, prohibits someone not entitled to receive a communication from doing so (e.g., by means of an extension phone or by having a communications company employee assigned to a "non-receiving job provide a copy of a message) if its use will be for the benefit of himself or someone else. The unique aspect of this clause, as contrasted with the first, is that it is not illegal merely to divulge it; rather it must be used for some benefit.

---

[1] By received, we mean obtained by a person and by a method in a way the sender or receiver would expect. This we contrast with the term "intercepted," which is the unexpected obtaining of a communication between a sender and receiver. See, e.g., Reitmeister v. Reitmeister, 162 F. 2d 691 (2nd Cir. 1947).

> The interception forbidden by Section 605 of the Communications Act of 1934, 47 U.S.C.A. §605, must be by some mechanical interpositions in the transmitting apparatus itself, that is the interjection of an independent receiving device between the lips of the sender and the ear of the receiver.

But, cf., United States v. Sullivan, 116 F. Supp. 480 (D.D.C. 1953) and United States v. Polakoff, 112 F. 2d 888 (2nd Cir. 1940), certiorari denied, 311 U.S. 653 (1940), holding that the means employed to accomplish the interception is irrelevant.

The second clause says that:

> . . . no person not being authorized by the sender shall intercept any communication and divulge the contents of such intercepted communication to any person; . . .

The important distinction between this clause and the first and third, is that it involves intercepting, rather than receiving. And, it refers to "any communication," rather than to "interstate or foreign communication by wire or radio." To date, no court has held that the second clause has a narrower scope than the first and third; rather, Sablowsky, supra, and Weiss v. United States, 308 U.S. 321 (1939) seem to indicate that the term "any communication" not only includes interstate and foreign communications, but also includes intrastate communications. Thus, to this extent, the second clause includes the scope of the first and third and, in addition, it seems to prohibit the interception of other communications. _/ Tracking the first-third-clause-procedure, the fourth clause covers what the second did not -- those who acquire an intercepted message:

_/ Unlike the rather extensive legislative history of Title III, the complete legislative history for §605 says:

> Section 605, prohibiting unauthorized publication of communications, is based upon section 27 of the Radio Act and extends it to wire communications.

Thus, there is no definition of the term "any communication," thereby inviting some confusion.

> . . . no person having received such intercepted communication shall divulge or publish the contents or use the same or any information therein contained for his own benefit or for the benefit of another not entitled thereto: * * *.

Some of the less-obvious "gaps" in the statute now begin to emerge. While under clauses one and two, neither the lawful receiver nor the unauthorized interceptor is expressly barred from using the message for his or another's benefit, the unauthorized receiver has an "escape" under clause three for he can divulge it so long as there is no benefit derived. The fourth clause is comparatively "tighter", for one who acquires an unauthorized interception cannot do anything with it. Finally, there is a problem as to what the term "use" means., but a discussion of that will be deferred until later, when potential defenses are discussed.

If all of this seems to give rise to some confusion, the 1968 Act added still more.

* * *

On June 19, 1968, §605 was amended in conjunction with the enactment of Title III, 18 U.S.C. §2510, et seq.

In order to understand the scope of Title III, it would be helpful to establish a few definitional "guideposts." The statute covers wire and oral communications; wire communication is defined as:

> any communication made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign communications (Emphasis supplied).

On first reading this would seem to suggest that the system the Act protects is a point-to-point wire system, i.e., a telegraph or telephone wire. The problem with this interpretatic though, is that it is much too primative in light of techniques now available and in light of the make-up of our Nation's communication system.

That system could be characterized as one which is contiguous, switched (e.g., from wire to cable to microwave), automatic, and self-routing. Its "wireless" components include a multi-channel microwave carriers system capable of carrying up to 2,000 communications on some channels. International commercial radio-telephone communications can be transmitted by high-frequency, single or multi-channel

telephony which enters the national communications network through what are known as "gateways." (This is a means to pass from one system to another). As we will discuss, high-frequency telephony is considerably more susceptible to interception by comparatively unsophisticated equipment, such as ship-to-shore radio or the ordinary Zenith transoceanic-type portable radio than other systems.

Microwave transmissions are also used, usually in a "straight line". They can cover much higher frequencies than "high frequency telephony" which follows the curvature of the earth. Thus, it has been estimated that the radio portion of a high frequency single-channel radio-telephone communication from Montevideo, Uruguary, to New York City, could be intercepted with relatively unsophisticated radio receivers over an area of perhaps 30 percent of the earth's surface, and high frequency multi-channel transmissions may also be de-channeled by "homemade" amateur equipment. (Indeed, an index of the users of international radio frequencies is reportedly published by the FCC and may be obtained from the Government Printing Office.)

Though the term "wire communication" as used in the statute would include these systems, we believe it is limited to communications passing through our Nation's communications network. (Both case law and the legislative history seem to suggest that 2510 et seq. have no extra-territorial application where a "foreign" communication system is used.)

The second definition of importance is "oral communication" which is defined as:

> any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation.

Once again, while wire communications are covered regardless of whether any expectation of privacy exists, only those oral communications uttered under circumstances justifying a reasonable expectation of privacy are protected. An example of the problem one encounters in applying these two is set forth in United States v. Hall, 488 F. 2d 193 (9th Cir. 1973). [1]

[1] Early in 1971, a Tucson housewife was listening to a high-band receiver and overheard two men talking on radio telephones in their cars. (This type of radio is not unique; it is sold on the open market to the general public to permit them to listen to police and fire broadcasts. On these same frequencies radio telephone communications are broadcast.) After listening for a period of time she became suspicious and reported the conversations to State authorities who also monitored the conversations. As a result, the defendants were arrested and convicted for possession drugs. (footnote continued on page 25)

Having specified the types of communications (wire and oral) to be protected,[/] Title III defined the term interception:

> the aural acquisition of the contents of any wire or oral communication through the use of any electronic, mechanical, or other device.

There are two important elements here (1) "aural" and (2) "through the use of a device."

Although the word "aural" is not defined in the statute, the legislative history discusses it specifically and says it excludes all other means of acquisition:

(footnote continued from page 24)

Although the appellate court held that Title III did not protect communications between two mobile radio telephones, because they were oral communications uttered with no reasonable expectation of privacy, the court went on to hold they would not reach the same result where a radio telephone called a regular telephone, because that would have been a case where the latter instrument involved a wire communication, and that is protected without qualification as to an expectation of privacy. This result was accurately described by the court when it said, "We realize that our classification of a conversation between a mobile and a land-line telephone as a wire communication produces what appears to be an absurd result." Then, the court went on to compound the problem when it said that:

> . . . any citizen who listens to a mobile telephone band does so at its own risk, and scores of mariners who listen to the ship-to-shore frequency, commonly used to call to a land-line telephone, commit criminal acts.

[/] Another "gap" problem is that Title III does not cover the "receiving" of a wire communication, as do clauses one and three of §605.

> Paragraph (4) defines "intercept" to include the aural acquisition of the contents of any wire or oral communication by any electric, mechanical, or other device. Other forms of surveillance are not within the proposed legislation. See Lee v. United States, 47 S. Ct. 746, 274 U.S. 559 (1927); Corngold v. United States, 367 F. 2d (9th 1966). An examination of telephone company records by law enforcement agents in the regular course of their duties would be lawful because it would not be an "interception". (United States v. Russo, 250 F. Supp. 55 (E.D. Pa. 1966). The proposed legislation is not designed to prevent the tracing of phone calls. The use of a "pen register", for example, would be permissible. But see United States v. Dote, 371 F. 2d 176 (7th 1966).

1968 U.S. Code and Adm. News at 2178. This is of more than passing significance, for it seems to exclude from the statute's coverage all communications transmitted mechanically, i.e., transmitted by signals independent of sound, for example, by electrical pulse.

The phrase "acquisition through the use of any . . . device" is another important limitation, for it makes it clear that the congressional concern was with the activity engaged in at the time of the communication which causes the communication to be overheard by uninvited listeners; that is, the contemporaneous surveillance (by hearing, recording, or otherwise) was at the center of congressional concern. See, e.g., United States v. Turk, 526 F. 2d 654, 658-659 (5th Cir. 1976).

With these aside, we can turn now to a brief look at the proscriptions of Title III. They are, in essence, as follows:

(1) . . . [A]ny person who

(a) willfully intercepts, endeavors to intercept, or procures any other person to intercept . . . any wire or oral communication. . . .

* * *

(b) willfully discloses, or endeavors to disclose, to any other person the contents or any wire or oral communication, knowing or having reason to know that the information was obtained through the interception or a wire or oral communication. . .

(c) willfully uses, or endeavors to use, the contents of any wire or oral communication, knowing or having reason to know that the information was obtained through the interception of a wire or oral communication. . . .

shall be fined not more than $10,000 or imprisoned not more than five years, or both.

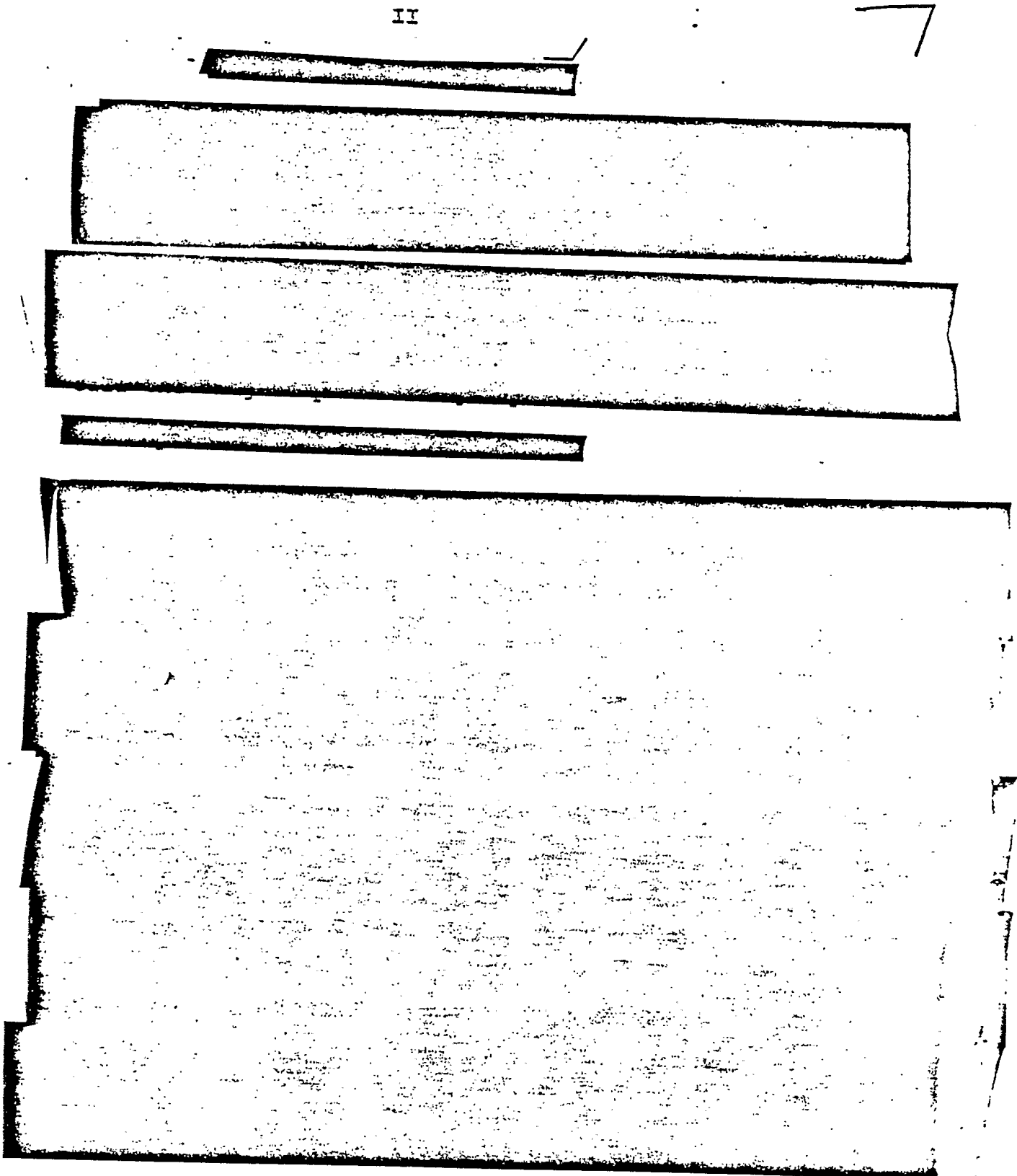
Title III is, in a phrase, an "interception-disclosure-use" statute. But, perhaps the most important aspect of the Act is the exemption to both statutes which it provides in §2511(3):

> Nothing contained in this chapter or in section 605 of the Communications Act of 1934 (48 Stat. 1143; 47 U.S.C. 605) shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign

> intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities. Nor shall anything contained in this chapter be deemed to limit the constitutional power of the President to take such measures as he deems necessary to protect the United States against the overthrow of the Government by force or other unlawful means, or against any other clear and present danger to the structure or existence of the Government.__/

We are now ready to review the activities which were investigated, and some of the central questions we will be focusing on in the rest of the summary will be (1) does the activity under investigation come within a prohibition listed in the statutes (2) and if so, is it exempted by §2511(3). And, even though the exception was not spelled out until 1968, we will also be considering such prosecutive problems and potential defenses as lack of intent or good faith reliance on prior history, the lack of any definitive guidance, and reassurances of legality by high government officials.

__/ As was indicated earlier, this was an expansion of Director Hoover's descriptions many years earlier; and, in 1970 the Supreme Court held, in Keith, that the President did not have the power described in the second (last) sentence of this section.



In addition to the difficulty one could expect trying to apply all of these principals to the following facts, there is another problem that should be kept in mind.

Today, we tend to be quite jaded about these matters, for almost everyday we read in the newspapers of a new intelligence-gathering program or technique. Up until the Keith case was decided in 1970, however, very few people even knew about national security wiretapping. For those who did, it was almost impossible to find out anything definitive about the power, for "one simply does not inquire into such matters." In addition, the state of the law was still very much undecided (as noted earlier, it was not until 1967 that the Supreme Court held in Katz that wiretapping protected people in addition to places.) Thus, up until a few years ago this entire matter was shrouded in secrecy, and the lack of any public information, coupled with what now must be considered naive acceptance of claims of national security power, quite understandably could cause some confusion. The problem then will be to try to avoid seeing -- and judging -- everything with the benefit of what might be called 1977 hindsight.

The investigation has not revealed for instance a single case in which intelligence obtained by means of electronic surveillance was gathered or used for personal or partisan political purposes. The participants in every questionable operation, however oblivious or unmindful, appear to have acted under at least some colorable semblance of authority in what they conscientiously deemed to be the best interests of the United States. While they may be regarded from our current perspective as having abused their broad discretionary power on occasion, that ill-defined power was conferred upon them and their agencies with a bevy of sweeping Presidential claims of power, Executive orders and directives, legislation and (e.g., the National Security Act) and a number of NSCIDs. If the intelligence agencies possessed too much discretionary authority with too little accountability, that would seem to be a 35-year failing of Presidents and the Congress rather than the agencies or their personnel.

In addition to all of these problems, there is the specter, in the event of any prosecution, that there is likely to be much "buck-passing" from subordinate to superior, agency to agency, agency to board or committee, board or committee to the President, and from the living to the dead.

Other practical considerations include the implications and complexities of providing discovery of national security materials (e.g., NSC, PFIAB, DOD, and White House documents and record), as well as sensitive foreign intelligence gathering methodology and technology to any potential defendant and to the public (as the result of any trial). These considerations become particularly acute when weighed against the minimal chances of sustaining the technical proof of violations and the probable lack of juror enthusiasm for convicting those whom the defense may plausibly portray as dedicated employees who only followed orders in trying to protect the national interest, i.e., keep heroin out of the United States.

Rather than to look to possible prosecutions to provide any remedial help, the better remedy might be to seek and to undertake administrative revision of policies and programs. These could include the following proposals:

1. Governmental agencies charged with the research and development of electronic equipment essential to the national security should be provided with clearly defined authority and procedures for testing such equipment against appropriate communications systems.

2. Consideration should be given to seeking specific Congressional and Presidential designation of certain international criminal activities as matters affecting the national security (e.g., international narcotics trafficking, gun-running, etc.) for purposes of foreign intelligence-gathering.

3. National security intelligence agencies should be authorized to provide appropriate U.S. law enforcement agencies with criminal intelligence incidentally obtained in the exercise of their lawful functions, including information indicating criminal activity on the part of U.S. citizens.

4. An effort should be made (consistent with the constitutional rights of criminal defendants) to secure legislation and/or rules changes to prevent the public identification of national security agencies as the source of criminal intelligence incidentally obtained in the exercise of their lawful functions, at least where such evidence is not introduced at trial.

5. The authority of the CIA, NSA and FBI to perform their respective missions in the field of electronic surveillance should be clearly delegated and delineated with specific procedures prescribed for the lawful exercise of that authority.

6. The Office of General Counsel for each intelligence agency should be staffed with one or more attorneys with expertise in electronic surveillance law and Federal criminal law and procedure.

7. Agency personnel should be required to consult their General Counsel and confirm, in advance, the legality of all electronic surveillance projects.

* * *

The recommendations of the task force set forth above are (accepted) (rejected).

BENJAMIN R. CIVILETTI
Assistant Attorney General
Criminal Division

Under NSC is the CIA and its head, the Director of Central Intelligence (DCI). In carrying out its responsibility of "coordinating the intelligence activites of the several Government departments and agencies in the interest of "national security," the Agency's duties are (1) "to advise the National Security Council in matters concerning . . intelligence activities of the Government ..."; (2) "to make recommendations to the National Security Council for the coordination of . . . intelligence activities of the department and agencies..."; (3) "to correlate and evaluate intelligence relating to the national security, and provide for the appropriate dissemination of such intelligence ..."; (4) "to perform, for the benefit of the existing intelligence agencies, such additional services of common concern as the National Security Council determines can be more efficiently accomplished centrally." and (5) "to perform such other functions and duties related to intelligence affecting the national security as the National Security Council may from time to time direct." 50 U.S.C. §403(d).

The National Security Agency was established by Presidential directive in 1952, and placed under the authority and control of the Secretary of Defense. The primary function of NSA is to engage in communications intelligence activities; i.e., the gathering of intelligence information by other than the intended recipients.

CIA also finds support for its intelligence gathering activities from NSCID 5, which, since 1958, has delegated primary responsibility to the CIA for cladestine activities abroad "in order to meet the needs of all departments and agencies concerned in connection with the national security." This authorization, along with the CIA's more general power under §403(d)(4) to "perform ... such additional services of common concern as the National Security Council determines can be more effectively accomplished centrally" explains the Agency's view that such actions were authorized.[1]

In a similar fashion, NSA draws support for its activities from NSCID 6, which has provided, at least since 1958, for NSA to provide "signal intelligence" for all intelligence agencies. "Signal intelligence" as defined therein, is intelligence produced by the study of foreign communications. To implement this NSCID, and to insure that it is involved only in "foreign" communications, NSA's long-standing policy has been to intercept a communication only if it has at least one-terminal outside the United States.

[1] It should also be reiterated that NSCID9 exempted CIA and NSA from restrictions publicly placed upon intelligence activities.

In addition to those direct sources of authorization, other statutes and actions reasonably suggest that CIA and NSA were not covered by the stricture of §2511 or §605.

[redacted]

Another good example is in the area of narcotics intelligence gathering. In addition to the sources of authority already discussed, the Federal Narcotics and Drug Abuse Act of 1973, 5 U.S.C. §901 et seq., acknowledges that both CIA and NSA have functions relating to the collection of information concerning trafficking in narcotics and dangerous drugs. And here, as in other areas, presidential memoranda closely linked national problems like narcotics with the national security. This too, according to the Agencies, caused them to believe their actions were within the law.

Finally, there are a number of other events from which NSA and CIA derive support - - or at least approval - - for their surveillance activities.

In July of 1973, William Colby testified before the Senate Armed Services Committee on his nomination to become DCI. In response to a question specifically addressed to whether CIA was then engaged in assisting law enforcement agencies in addition to the FBI, Colby replied in the affirmative, stating that CIA routinely disseminated its foreign intelligence reports to such agencies as the Drug Enforcement Administration, the Immigration and Naturalization Service, the Customs Service, the Secret Service, and the Armed Services. Since there was little doubt that a least some of CIA's information was governed by electronic surveillance, the Agency regards the lack of congressional objection as tacit approval of such dissemination.

More direct approval by the Executive Branch is provided by a February 3, 1971, NSA memorandum in which NSA officials described separate briefings two days earlier of Attorney General Mitchell and Secretary of Defense Laird on certain NSA activities. This memorandum reflects that both Mitchell and Laird read and approved a proposed memorandum which set forth proposed ground rules for NSA contribution to intelligence gathering for domestic problems. [redacted]

[redacted]

[redacted] CIA files also reflect that the same memorandum was read and approved in 1972 by Richard Kleindienst, then Attorney General.[1]

The participation of the Office of the General Counsel of NSA in the drafting of §2511(3), and the assurance of that office to the Agency that the effect of the subsection was to remove any doubt as to the legality of NSA surveillance is another factor cited by that Agency. A 1968 memo from the General Counsel to the Agency states that the language of §2511(3) "precludes an interpretation that the prohibitions against wiretapping or electronic surveillance techniques in other laws applies to [NSA activities] ... Wiretapping and electronic surveillance techniques are, therefore legally recognized as means for the Federal Government to acquire foreign intelligence information and to monitor U.S. classified communications..."

[1] Although Mr. Kleindienst has no recollection of this briefing, he did not dispute the CIA memo. Mr. Laird also did not remember seeing the memorandum or attending the briefing, but said the memo contained nothing he did not generally know of as early as 1964, when he served on the House Armed Forces Appropriations Subcommittee.

NSA also notes that NSCID 6 has provided, since 1958, that the departments and agencies being served are responsible for informing the NSA Director of the information desired. NSA interprets this language to require the implicit assurance by the agency seeking intelligence that the request is appropriate. Hence the responsibility is on the requesting agencies to frame their requests in accordance with the law. In 1973, Department of Defense General Counsel approved this interpretation, and stated that NSA was operating within the law.

Finally, NSA files reflect that since 1962 the Justice Department has sent hundreds of names of racketeers to NSA, requesting any information it might have concerning them. This too indicates that the Department did not regard this dissemination unlawful.

In reviewing these justifications, it must be remembered that some sources of authorization were after the fact, that others could not legally be relied upon, and, most important, that 50 U.S.C. 403(d)(3) expressly provides that the CIA shall have "no police, subpoena, law-enforcement powers, or internal security functions." Nonetheless, it appears from a number of authorities that no one really was clear on precisely what the Agencies could and could not do, that they were encouraged to become involved in law enforcement activities, and that no one, at least in any direct fashion,

ever seriously warned them that their actions were contrary to law. Thus, it seems harsh to charge either CIA or NSA employees with the responsibility of foreseeing the legal limits of their activites.

We will now turn to a discussion of the federal statutes which regulate the interception of communications.

C

Wiretap Statutes

Section 605 and Title III were premised on a few basic yet important principles which should be kept in mind when reviewing the statutes.

The basic purpose for enacting §605 in 1934 was to protect the integrity or the privacy of the Nation's communication's systems. In an effort to reach that goal, the statute regulated the conduct of personnel who worked for communications companies, and anyone else who might attempt to invade the integrity of such systems without proper authority.

Unfortunately the framers of the legislation fell somewhat short of their goal. They required, for example, that, before a violation could be shown, there must be both an interception and a divulgence of a communication, rather than a mere interception. This additional requirement allowed much wiretapping to slip through the crack. And, to the extent the drafters intended §605 to cover all electronic communications or electronic interceptions, they failed for Section 605 is, by its terms, limited to wire and radio communications, thereby exempting a host of esoteric communication techniques which would be developed in later years; e.g., laser and micro-wave communications.

Thirty-four years later, Congress enacted another wiretap statute; it too, however, had some important gaps.

The new statute, Title III, overlapped its predecessor by taking over the regulating of wire communications, but it also expanded the coverage to a new area: oral communications. Still, like §605, there were some noticeable gaps. First, the statute does not cover communications transmitted purely by radio; therefore, such communications require the "divulgence" element of §605. In addition, the new statute is limited to aural acquisitions (through the sense of hearing), thereby eliminating from its coverage many other surveillance techniques.[1] As mentioned earlier, though, the most important aspect of Title III is that it exempted from its coverage, as well as from §605, the President's power to authorize NSES.

With this as background, we turn first to a review of the specific statutory prohibition of §605 and Title III; then we will look at the Presidential power "exemption."

* * *

The stark contrast between the simplicity of the descriptions of the President's NSES power and the

---

[1] E.g., silent messages sent by electrical impulses, rather than by a voice which can be heard.

complex scope of §605 should, standing alone, prompt some sympathy for fledgling agencies created -- as were CIA in 1948 and NSA in 1952 -- in the midst of this development and then charged with the very serious task of gathering adequate intelligence to protect the Nation's security. An analysis of the 1934 Act quickly reveals why.

One of the earliest courts to analyze §605, Sablowsky v. United States, 101 F. 2d 183 (3rd Cir. 1938), started by noting that §605 has four major clauses. The first provides in essence that:

> No person receiving or transmitting any communication shall divulge the contents [improperly]. __/

Sablowsky held that this referred to a communications company employee and prohibited him from divulging something he had

---

__/ Each clause has many phrases and words we will ignore for our purposes here, for they are often synonyms which the drafters hoped would make sure that no unintentional gaps were left. For example, when referring to a communication, the Act refers to its "existence, contents, substance, purport, effect or meaning." We have selected one -- contents -- to represent the group. Also, for this part of the discussion, we will review §605 as it existed prior to the 1968 Act.

received lawfully.[1] (A major part of the task force's investigation involved telegraph and telephone company personnel who had helped various agencies to intercept and receive many private communications.)

The third clause, which, like the first, involves receivers, prohibits someone not entitled to receive a communication from doing so (e.g., by means of an extension phone or by having a communications company employee assigned to a "non-receiving job provide a copy of a message) if its use will be for the benefit of himself or someone else. The unique aspect of this clause, as contrasted with the first, is that it is not illegal merely to divulge it; rather it must be used for some benefit.

---

[1] By received, we mean obtained by a person and by a method in a way the sender or receiver would expect. This we contrast with the term "intercepted," which is the unexpected obtaining of a communication between a sender and receiver. See, e.g., Reitmeister v. Reitmeister, 162 F. 2d 691 (2nd Cir. 1947).

> The interception forbidden by Section 605 of the Communications Act of 1934, 47 U.S.C.A. §605, must be by some mechanical interpositions in the transmitting apparatus itself, that is the interjection of an independent receiving device between the lips of the sender and the ear of the receiver.

But, cf., United States v. Sullivan, 116 F. Supp. 480 (D.D.C. 1953) and United States v. Polakoff, 112 F. 2d 888 (2nd Cir. 1940), certiorari denied, 311 U.S. 653 (1940), holding that the means employed to accomplish the interception is irrelevant.

The second clause says that:

> . . . no person not being authorized by the sender shall intercept any communication and divulge the contents of such intercepted communication to any person; . . .

The important distinction between this clause and the first and third, is that it involves intercepting, rather than receiving. And, it refers to "any communication," rather than to "interstate or foreign communication by wire or radio." To date, no court has held that the second clause has a narrower scope than the first and third; rather, Sablowsky, supra, and Weiss v. United States, 308 U.S. 321 (1939) seem to indicate that the term "any communication" not only includes interstate and foreign communications, but also includes intrastate communications. Thus, to this extent, the second clause includes the scope of the first and third and, in addition, it seems to prohibit the interception of other communications. —/ Tracking the first-third-clause-procedure, the fourth clause covers what the second did not -- those who acquire an intercepted message:

—/ Unlike the rather extensive legislative history of Title III, the complete legislative history for §605 says:

> Section 605, prohibiting unauthorized publication of communications, is based upon section 27 of the Radio Act and extends it to wire communications.

Thus, there is no definition of the term "any communication," thereby inviting some confusion.

> . . . no person having received such intercepted communication shall divulge or publish the contents or use the same or any information therein contained for his own benefit or for the benefit of another not entitled thereto: * * *.

Some of the less-obvious "gaps" in the statute now begin to emerge. While under clauses one and two, neither the lawful receiver nor the unauthorized interceptor is expressly barred from using the message for his or another's benefit, the unauthorized receiver has an "escape" under clause three for he can divulge it so long as there is no benefit derived. The fourth clause is comparatively "tighter", for one who acquires an unauthorized interception cannot do anything with it. Finally, there is a problem as to what the term "use" means., but a discussion of that will be deferred until later, when potential defenses are discussed.

If all of this seems to give rise to some confusion, the 1968 Act added still more.

* * *

On June 19, 1968, §605 was amended in conjunction with the enactment of Title III, 18 U.S.C. §2510, et seq.

In order to understand the scope of Title III, it would be helpful to establish a few definitional "guideposts." The statute covers wire and oral communications; wire communication is defined as:

> any communication made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign communications (Emphasis supplied).

On first reading this would seem to suggest that the system the Act protects is a point-to-point wire system, i.e., a telegraph or telephone wire. The problem with this interpretation though, is that it is much too primative in light of techniques now available and in light of the make-up of our Nation's communication system.

That system could be characterized as one which is contiguous, switched (e.g., from wire to cable to microwave), automatic, and self-routing. Its "wireless" components include a multi-channel microwave carriers system capable of carrying up to 2,000 communications on some channels. International commercial radio-telephone communications can be transmitted by high-frequency, single or multi-channel

telephony which enters the national communications network through what are known as "gateways." (This is a means to pass from one system to another). As we will discuss, high-frequency telephony is considerably more susceptible to interception by comparatively unsophisticated equipment, such as ship-to-shore radio or the ordinary Zenith transoceanic-type portable radio than other systems.

Microwave transmissions are also used, usually in a "straight line". They can cover much higher frequencies than "high frequency telephony" which follows the curvature of the earth. Thus, it has been estimated that the radio portion of a high frequency single-channel radio-telephone communication from Montevideo, Uruguary, to New York City, could be intercepted with relatively unsophisticated radio receivers over an area of perhaps 30 percent of the earth's surface, and high frequency multi-channel transmissions may also be de-channeled by "homemade" amateur equipment. (Indeed, an index of the users of international radio frequencies is reportedly published by the FCC and may be obtained from the Government Printing Office.)

Though the term "wire communication" as used in the statute would include these systems, we believe it is limited to communications passing through our Nation's communications network. (Both case law and the legislative history seem to suggest that 2510 et seq. have no extra-territorial application where a "foreign" communication system is used.)

The second definition of importance is "oral communication" which is defined as:

> any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation.

Once again, while wire communications are covered regardless of whether any expectation of privacy exists, only those oral communications uttered under circumstances justifying a reasonable expectation of privacy are protected. An example of the problem one encounters in applying these two is set forth in United States v. Hall, 488 F. 2d 193 (9th Cir. 1973).[/]

[/] Early in 1971, a Tucson housewife was listening to a high-band receiver and overheard two men talking on radio telephones in their cars. (This type of radio is not unique; it is sold on the open market to the general public to permit them to listen to police and fire broadcasts. On these same frequencies radio telephone communications are broadcast.) After listening for a period of time she became suspicious and reported the conversations to State authorities who also monitored the conversations. As a result, the defendants were arrested and convicted for possession drugs. (footnote continued on page 25)

Having specified the types of communications (wire and oral) to be protected,[/] Title III defined the term interception:

> the aural acquisition of the contents of any wire or oral communication through the use of any electronic, mechanical, or other device.

There are two important elements here (1) "aural" and (2) "through the use of a device."

Although the word "aural" is not defined in the statute, the legislative history discusses it specifically and says it excludes all other means of acquisition:

(footnote continued from page 24)

Although the appellate court held that Title III did not protect communications between two mobile radio telephones, because they were oral communications uttered with no reasonable expectation of privacy, the court went on to hold they would not reach the same result where a radio telephone called a regular telephone, because that would have been a case where the latter instrument involved a wire communication, and that is protected without qualification as to an expectation of privacy. This result was accurately described by the court when it said, "We realize that our classification of a conversation between a mobile and a land-line telephone as a wire communication produces what appears to be an absurd result." Then, the court went on to compound the problem when it said that:

> . . . any citizen who listens to a mobile telephone band does so at its own risk, and scores of mariners who listen to the ship-to-shore frequency, commonly used to call to a land-line telephone, commit criminal acts.

[/] Another "gap" problem is that Title III does not cover the "receiving" of a wire communication, as do clauses one and three of §605.

> Paragraph (4) defines "intercept" to include the aural acquisition of the contents of any wire or oral communication by any electric, mechanical, or other device. Other forms of surveillance are not within the proposed legislation. See Lee v. United States, 47 S. Ct. 746, 274 U.S. 559 (1927); Corngold v. United States, 367 F. 2d (9th 1966). An examination of telephone company records by law enforcement agents in the regular course of their duties would be lawful because it would not be an "interception". (United States v. Russo, 250 F. Supp. 55 (E.D. Pa. 1966). The proposed legislation is not designed to prevent the tracing of phone calls. The use of a "pen register", for example, would be permissible. But see United States v. Dote, 371 F. 2d 176 (7th 1966).

1968 U.S. Code and Adm. News at 2178. This is of more than passing significance, for it seems to exclude from the statute's coverage all communications transmitted mechanically, i.e., transmitted by signals independent of sound, for example, by electrical pulse.

The phrase "acquisition through the use of any . . . device" is another important limitation, for it makes it clear that the congressional concern was with the activity engaged in at the time of the communication which causes the communication to be overheard by uninvited listeners; that is, the contemporaneous surveillance (by hearing, recording, or otherwise) was at the center of congressional concern. See, e.g., United States v. Turk, 526 F. 2d 654, 658-659 (5th Cir. 1976).

With these aside, we can turn now to a brief look at the proscriptions of Title III. They are, in essence, as follows:

> (1) . . . [A]ny person who
>
> (a) willfully intercepts, endeavors to intercept, or procures any other person to intercept . . . any wire or oral communication. . . .
>
> * * *
>
> (b) willfully discloses, or endeavors to disclose, to any other person the contents or any wire or oral communication, knowing or having reason to know that the information was obtained through the interception or a wire or oral communication. . .
>
> (c) willfully uses, or endeavors to use, the contents of any wire or oral communication, knowing or having reason to know that the information was obtained through the interception of a wire or oral communication. . . .

shall be fined not more than $10,000 or imprisoned not more than five years, or both.

Title III is, in a phrase, an "interception-disclosure-use" statute. But, perhaps the most important aspect of the Act is the exemption to both statutes which it provides in §2511(3):

> Nothing contained in this chapter or in section 605 of the Communications Act of 1934 (48 Stat. 1143; 47 U.S.C. 605) shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign

> intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities. Nor shall anything contained in this chapter be deemed to limit the constitutional power of the President to take such measures as he deems necessary to protect the United States against the overthrow of the Government by force or other unlawful means, or against any other clear and present danger to the structure or existence of the Government.__/

We are now ready to review the activities which were investigated, and some of the central questions we will be focusing on in the rest of the summary will be (1) does the activity under investigation come within a prohibition listed in the statutes (2) and if so, is it exempted by §2511(3). And, even though the exception was not spelled out until 1968, we will also be considering such prosecutive problems and potential defenses as lack of intent or good faith reliance on prior history, the lack of any definitive guidance, and reassurances of legality by high government officials.

__/ As was indicated earlier, this was an expansion of Director Hoover's descriptions many years earlier; and, in 1970 the Supreme Court held, in Keith, that the President did not have the power described in the second (last) sentence of this section.

In addition to the difficulty one could expect trying to apply all of these principals to the following facts, there is another problem that should be kept in mind.

Today, we tend to be quite jaded about these matters, for almost everyday we read in the newspapers of a new intelligence-gathering program or technique. Up until the Keith case was decided in 1970, however, very few people even knew about national security wiretapping. For those who did, it was almost impossible to find out anything definitive about the power, for "one simply does not inquire into such matters." In addition, the state of the law was still very much undecided (as noted earlier, it was not until 1967 that the Supreme Court held in Katz that wiretapping protected people in addition to places.) Thus, up until a few years ago this entire matter was shrouded in secrecy, and the lack of any public information, coupled with what now must be considered naive acceptance of claims of national security power, quite understandably could cause some confusion. The problem then will be to try to avoid seeing -- and judging -- everything with the benefit of what might be called 1977 hindsight.

[redacted]

A

"Major Operations"

A number of the activities the task force investigated involved programs which spanned many years and which tended to ebb and flow over the period. And, more often than not, the program lacked a specific directive, order, or statutory basis; instead, its authority was a combination of elements. For our purposes here, we will select one such program (perhaps the most pervasive), trace its development, and then explain why a prosecution would be inappropriate. We believe the same principals which dictated that conclusion apply as well to the other programs which will be discussed, but much more briefly.

"SHAMROCK" was one of the most pervasive programs the task force discovered, spanning over 30 years; like so many things that grow to massive proportions, however, "SHAMROCK" started very innocently.

(footnote continued from page)

In addition to these, the task force discovered a second category of activity , which, though questionable, was non-prosecutable. For example, NSA and CIA engaged in a number of support activities which helped wiretapping programs. They obtained telephone toll records, [redacted] supplied the D.C. Police Department and the Secret Service with wiretapping equipment, supplied an office to assist in a program to review domestic telegram traffic, and recruited agents and introduced others to them (agency representatives and personnel provided to assist their communication carriers). All of these activities, while relating to other various wiretapping programs, did not themselves involve intercepting communications; thus, they clearly did not violate the wiretap statutes.

Faced with the ever-increasing threats posed by Japan and Germany, Director Hoover started working with the Department on a proposed executive order to permit the program, but before the Order could be finalized, Pearl Harbor intervened.

Congress, acting with uncharacteristic swiftness, enacted what was later to be called the Censorship law, and on December 22, 1941, the Solicitor General told the Bureau that the proposed Executive Order would no longer be necessary, for the newly created Office of Censorship would have full authority over international communications, and the FBI could obtain any that it needed from that Office in the future.

While all this was occurring, though, the Bureau was moving ahead. Very soon after December 7, the Bureau was requested by the State Department to ask the appropriate cable companies to hold up the transmissions of messages to certain countries for 24 hours, and then to make copies of the cables available for review. The requests were made and suprisingly, yet understandably, the companies readily agreed. The Attorney General was promptly advised, thereby putting the Department on notice the program had begun.

/cont'd
cooperate, but this time they did so expressly on the ground that they felt they were prohibited by law from doing so and would be subject to possible prosecution if they complied! As we shall see, this was a continuing concern of the companies and, unfortunately, their initial instincts would, many years later, prove to be correct.

Once again, as in 1940, the cable companies' survival instincts were aroused, but this time they were in a different position: they were already supplying the cable copies. Nevertheless, their concern soon mounted, prompting them to seek assurances that the "federal government [could] guarantee to (sic) commercial communication companies against criminal liabilities resulting from these companies furnishing to the Army certain documents and traffic."[1]

Twice -- in 1947 and again in 1949 — the companies were given the assurances they sought. Of more than passing interest, though, was something else than Secretary Forrestal said to a group of executives of IT&T and RCA:[2]

> . . . while it was always difficult for any member of the Government to attempt to commit his successor, he could assure the gentlemen present that if the present practices were continued the Government would take whatever steps were possible to see to it that the companies involved would be protected.

---

[1] For some unexplained reason, no mention was made of the companies' practice of supplying copies to the Bureau.

[2] Initially, Secretary of Defense Forrestal told the group he was speaking for President Truman in commending them for their cooperation and requesting their continued assistance because the intelligence constituted a matter of great importance to the national security. Two years later, on May 18, 1949, Secretary of Defense Johnson met with officials of the same companies and stated that President Truman, Attorney General Tom Clark, and he endorsed the Forrestal statement and would provide them with a guarantee against any criminal action which might arise from their assistance. Former Secretary of Defense Laird, as late as 1973 when the program was halted, said "SHAMROCK" was also tacitly endorsed by him.

He also said that, so long as the present Attorney General was in office, he could give assurances that the Department of Justice would also do all in its power to give the companies full protection. In an effort to clarify this latter point, a company official inquired if Mr. Forrestal was speaking not only for the Office of the Secretary of Defense, but also in the name of the President of the United States. Mr. Forrestal replied that that was correct.

Two years later, essentially the same representations were made, however, the memorandum reflecting that fact had an interesting pair of handwritten notes, one saying, "OK'd. by the President and Tom Clark," and signed by Louis Johnson, and the other initialed as approved, "T.C.C.," presumably meaning then Attorney General Tom Clark.

Though Congress repealed the Censorship law, it recognized the need of the President to get advise in certain domestic, foreign, and military areas, particularly as they relate to national security matters, so in response to that need, Congress enacted a law which established the National Security Council (NSC). Five years later, in 1952, the President signed a directive which created the National Security Agency; the functions assigned to it included responsibility for "SHAMROCK".

For the better part of the next two decades, the Bureau worked closely with the newly-created Agency, becoming a regular courier between the Agency and the companies for the purpose of picking up cable traffic. Then, for reasons not of moment here, the Bureau withdrew its participation in the program in 1973, and in May of 1975, "SHAMROCK" was halted entirely when the Agency also stopped the practice.

When NSA first assumed responsibility for the "SHAMROCK" operation in 1952, the practice and the procedures had already been established for more than a decade. Those procedures permitted NSA employees access to all diplomatic messages handled by the RCA, ITT, and Western Union offices located in New York City and Washington, D. C., as well as the RCA and ITT offices in San Francisco. RCA provided NSA employees with duplicates (drop copies) of all international messages, thus requiring NSA employees to visually screen and select out diplomatic messages for microfilming on NSA-owned machines located on the RCA premises. Western Union and ITT (starting in 1945), went further, providing NSA agents with a daily microfilm of diplomatic messages which had already been selected out and photographed by company employees on NSA-owned photo machines. The investigation also shows that NSA employees were given access to all perforated paper tape copies of international messages transmitted by RCA and possibly from ITT.

[redacted] NSA started to select out other international messages containing the names of persons on what was called the watch lists.[1] [redacted]

Statutes

Though it would seem that the companies, the FBI, and NSA violated clauses one and three of §605,[2] there are a number of problems with trying to prosecute anyone for this activity, including the following possible defenses:

(1) Prior Presidents and Attorneys General had notice of and, in at least one case, appeared to approve the operation;

(2) Two Secretaries of Defense had tried to give the companies immunity;

(3) Clause one of §605 permits companies to disclose information "upon demand of lawful authority;"[3]?

---

[1] This was a list of names maintained by NSA for other investigative agencies of persons about whom the agencies wanted investigative information, usually for domestic security reasons. This use of this list continued until 1973 when Attorney General Richardson terminated the practice.

[2] Title III does not apply for the collection method was non-aural -- copies of telegrams and magnetic tapes containing electrical impulses. Accord, Smith v. Nunker, 356 F. Supp. 44 (D.C. Ohio, 1972)

[3] A few years ago, a United States attorney asked the Department what that exemption encompassed, and in reply we said the term "embraces any state or federal agency authorized by state or federal law to demand, by subpoena or otherwise, the production of books, records, papers, or other documents," (Emphasis supplied.) While the statute speaks in terms of a "demand," the requests to the companies here were, at most, patriotic pleas plus parting (footnote continued)

(4) There was no divulgence outside the Executive Branch, so there was no divulgence within the meaning of §605;

(5) A use which benefits the Government is not the type of "use" contemplated by the statute;

(6) It is not illegal to "ask" a company to give out copies of cables. If the company complies, it may be violating the statute but the recipient would not; and

(7) The putative defendants acted in good faith, and they lacked the necessary intent to prove a violation of the law.

In addition to these problems, there are a number of other reasons which militate against prosecution.

First, as is clear from a review of a evolution of the President's power from its inception, the true scope of the President's power (with which the Bureau and the Agency were familar) was unknown. And although by today's standards the power was virtually open ended, "SHAMROCK" would have fitted quite easily, then within its parameters, especially in 1941 when the program started. That, coupled with the notice to the Attorney General could lead one to believe he had accepted it under the President's NSES power.

1/(footnote cont'd)
promises of protection. Still there is a question whether the agencies could be said to come within the demand part; moreover, this defense could only be advanced by the companies, not the Agencies.

Second, it would be singularly unfair to carve out for prosecution those who carried out the program the last three years it was in existence when they had no reason to question the legality of a program that had gone on for 30 years.

Third, although it is not directly controlling here, the directive which created NSA and gave it certain powers to collect information expressly provided that because of the special nature of their work, prohibitions contained in "orders, directives, policies. . . of the Executive Branch relating to the collection . . . of intelligence . . . shall not be applicable to [such] activities, unless specifically so stated. . . ." Thus, agency employees could very easily have concluded that if there was a prohibition to the program, it did not apply to them (Throughout all of this, it is also important to keep in mind that the potential defendants are all laymen and, as we have seen, the law in this area is complex.)

Fourth, Congress, by funding this program, undoubtedly had some understanding of its existence. We also know that various Presidents and cabinet officers knew of the program but did nothing to halt it, thereby permitting agency personnel to believe it had Executive approval.

Fifth assuming it could be shown that a President impliedly authorized the program, and assuming he had the power to do so, Section 2511(3) would exempt the program from either wiretap statute coverage. Finally, even if the statute (§605) applies all of these reasons indicate the potential defendants acted in good faith sufficient to negate the criminal intent.

For all of these reasons, the task force recommends against prosecution of power and agency personnel for operation "SHAMROCK"

As noted earlier, other programs will be discussed briefly. While each employed different means of surveillance, presenting different problems under §605 and/or §2511, they share many common defenses. More important, the basic question involved -- whether it is just to prosecute individuals for these activities -- remains the same.

* * *

NSA had two other programs that fall within the "Major Operation" group -- MINERET and [redacted]

MINERET was started in July of 1969, and it formalized the agency's practice of collecting information for the Secret Service and the FBI about people in whom they had an interest. (e.g., civil disturbance and national security information).

MINERET gathered intelligence from a variety of communication programs involving both aural and non-aural communications. Some

of the input for this program came from operation "SHAMROCK", but other than that, the MINERET input came from communications that had at least one terminal in a foreign country. (The interceptions occurred both from within and without the United States.)

In mid-1970, MINERET was enlarged to include checking to see if any intelligence concerning narcotic trafficking was picked up incidentally as a by-product of its work. Later, it included the use of a watch list

[redacted]

The task force recommends against prosecution for a number of reasons.

First, the Attorney General decided in 1971 that electronic surveillance to obtain intelligence concerning potential domestic violence was within the President's national security

power. Second, as late as November of 1975, the Attorney General suggested to the Senate Select Committee that it was arguable there was no reason for people to expect privacy if their communications are transmitted by radio; therefore, the Fourth Amendment would not apply. (This conclusion would include the wiretap statutes as well.) These positions would undoubtedly be asserted as a defense to any prosecution. In addition, there is the problem of the TOP SECRET order concerning NSA mentioned earlier, and which suggested they were not under the same prohibitions as other members of the community. On that point, the Senate Select Committee concluded in a recent report that there were no existing statutes which controlled, limited, or defined the intelligence activities of the NSA; that no statute or executive order prohibits NSA from monitoring a telephone circuit with one terminal in the United States; and that there is no statute which prohibits the watch list program. 1/

So, as with "SHAMROCK" an argument could be made that MINERET [redacted] violated at least one if not both of the wiretap statutes; however, any prosecution would have to overcome all of these problems, and the prospects of that seem very slim. For these reasons, the task force recommends against prosecution of any agency personnel for MINERET [redacted] activities.

1/ S. Rep. No. 94-755, 94th Cong., 2nd Sess., Book ___ pp. 736, 756, 761 (1976).

* * *

The final "major operation" involves a program first named NARCOG.

In October 1969 the President, deeply concerned with a number of serious problems arising from international narcotics traffic, established the White House Task Force on Heroin Suppression, and CIA was directed by the President to provide the task force with assistance. A CIA office of Narcotics Coordinator was established (and later reorganized under the name of NARCOG) to provide representation of CIA on the working group, liaison with other agencies, and intelligence reports and studies concerning the principal areas of task force concern [redacted]

In August 1971, the President up-graded the priority of the program by replacing the task force with a Cabinet Committee on International Narcotics Control (CCINC). The CIA Coordinator was named chairman of a subcommittee, and it continued to provide BNDD (also a member of the Intelligence Subcommittee) with foreign narcotics intelligence.

The information gathered by CIA was obtained primarily as the result of incidental surveillance by NSA (e.g., MINERET [redacted] and then a review to see if any by-product of the NSES activity involved drugs. In addition, CIA engaged in other overseas interceptions specifically conducted to gather international narcotics intelligence.

When overseas CIA stations inadvertently acquired information concerning the narcotics trafficking activities of U.S. citizens as the result of electronic surveillance, the local CIA official would reportedly surrender the information to his local BNDD counterpart and take steps to insure that no further collection on the U.S. citizen occurred.

The task force believes a prosecution for NARCOG would be inappropriate in light of the problems which arise because of the implied Presidential authorization which caused the activities to start. In addition, neither NSA nor CIA conducted any specific surveillance of American citizens specifically to meet its responsibility under NARCOG; the only information supplied was information gathered from intelligence collected for other purposes; in short, it was by-product information. (To whatever extent CIA wiretapped, it was (with one exception discussed next) done totally outside the country, and it did not involve this Nation's communication system, and therefore it did not violate the wiretap statutes.) For these reasons, the task force recommends against prosecution.

"Minor Operations"

[redacted]ran for a four month period during 1972-73 during which the CIA intercepted (by radio) certain radio

telephone communications between this country and Latin America (the surveillance was directed against a foreign target) for the purposes of gathering narcotics information. The interceptions occurred within this country.

There are, as we discussed earlier, a number of directives authorizing CIA to gather intelligence information and those, coupled with the President's insistence that the agency contribute to the maximum extent possible and "mobilize its full resources to fight the international drug trade." could be construed by some to be tantamount to Presidential authorization under §2511(3). In addition, it was during this time that the President considered narcotics control a matter of foreign policy. He said it was imperative to halt the flow of drugs; that drugs were a menace to the general welfare of the country, that the drug fight was one of the most important, the most urgent national priorities; and that keeping drugs out of the country was as important as keeping the enemy from entering.

Congress has also recognized the need for such intelligence and the general propriety of utilizing CIA and NSA to obtain it, at least to the extent it provided for the funding of such programs and received reports of the results, e.g., budget requests.

While these factors do not bar a prosecution as such, they do act to cloud the issue considerably so the chances of a conviction are considerably slim.

[redacted]

* * *

[redacted]

Also of importance here is the fact that the program was conducted pursuant to the agency's guidelines and approved by its general counsel. For these reasons, the agency personnel could be said to have acted in good faith which, if true, would tend to frustrate any chance of proving the requisite criminal intent.

Accordingly, the task force recommends against prosecution.

* * *

[redacted]

[redacted]

[redacted]

* * *

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

The chance of a successful prosecution are not very good for an important element, criminal intent, would be difficult to prove, and there are serious questions whether the temporary-interception-and-destruction practice would satisfy the "divulgence" or "use" elements of 605.

For all of these reasons the task force recommends against prosecution for these testing practices.

CONCLUSION

This report quite obviously did not focus on the particulars upon which affirmative prosecutive decisions may be made in specific cases. Rather, it attempted to provide the important legal and factual detail one should consider in determining whether inquiry into any specific activities should be terminated for lack of prosecutive potential or whether further investigation should be pursued, e.g., by grand jury.

The task force recommends that all further inquiry be terminated, for there appears to be little likelihood, if any, that convictions could be obtained on the basis of currently available evidence or evidence which might reasonably be developed.

The investigation has not revealed for instance a single case in which intelligence obtained by means of electronic surveillance was gathered or used for personal or partisan political purposes. The participants in every questionable operation, however oblivious or unmindful, appear to have acted under at least some colorable semblance of authority in what they conscientiously deemed to be the best interests of the United States. While they may be regarded from our current perspective as having abused their broad discretionary power on occasion, that ill-defined power was conferred upon them and their agencies with a bevy of sweeping Presidential claims of power, Executive orders and directives, legislation and (e.g., the National Security Act) and a number of NSCIDs. If the intelligence agencies possessed too much discretionary authority with too little accountability, that would seem to be a 35-year failing of Presidents and the Congress rather than the agencies or their personnel.

In addition to all of these problems, there is the specter, in the event of any prosecution, that there is likely to be much "buck-passing" from subordinate to superior, agency to agency, agency to board or committee, board or committee to the President, and from the living to the dead.

Directions to CIA and NSA are implemented via National Security Council Intelligence Directive (NSCIDs). Since the President has the only "vote" on the Council, its NSCIDs are deemed by both CIA and NSA to bear his imprimatur.

The NSCID primarily applicable to CIA, NSCID 1, directs the DCI to establish comprehensive national intelligence objectives generally applicable to foreign countries, to coordinate all foreign intelligence activities, to see that such intelligence is disseminated to various executive agencies, and to ensure that on matters affecting national security the intelligence community is fully supported by all knowledge and technical talent available to the Government.

The 1972 revision of NSCID 1 reiterated all these functions, and made clear that the production of intelligence required by "the President and other national consumers" was of the highest priorty. This revision implemented a November 1971, memorandum from President Nixon, the objective of which was to establish overall goals for the intelligence community and to provide more efficient use of resources by these agencies in collecting intelligence. In 1974, President Ford reaffirmed these goals in a memorandum to the DCI, noting his expectation that the heads of the departments having foreign intelligence responsibilities would cooperate fully and provide the DCI with all possible assistance.

OPTIONAL FORM NO. 10
JULY 1973 EDITION
GSA FPMR (41 CFR) 101-11.6

~~TOP SECRET~~ - COMINT MATERIAL ATTACHED

UNITED STATES GOVERNMENT

Memorandum

TO : Robert L. Keuch
Deputy Assistant Attorney General
Criminal Division

DATE: March 4, 1977

FROM : George W. Calhoun
Chief, Special Litigation

SUBJECT: Prosecutive Summary

Attached hereto is a copy of a draft of the prosecutive summary. (Corrections are being made).

As you will see, it contains some detailed information which might otherwise be unnecessary, but because Mr. Civiletti does not have a background in this area, the report has been expanded to fill him in and give him a perspective.

It goes without saying you should make any changes you wish, and if it is not acceptable at all, let me know. Also, if you need the underlying report let me know.

~~TOP SECRET~~

CLASSIFIED MATERIAL ATTACHED

Other practical considerations include the implications and complexities of providing discovery of national security materials (e.g., NSC, PFIAB, DOD, and White House documents and record), as well as sensitive foreign intelligence gathering methodology and technology to any potential defendant and to the public (as the result of any trial). These considerations become particularly acute when weighed against the minimal chances of sustaining the technical proof of violations and the probable lack of juror enthusiasm for convicting those whom the defense may plausibly portray as dedicated employees who only followed orders in trying to protect the national interest, i.e., keep heroin out of the United States.

Rather than to look to possible prosecutions to provide any remedial help, the better remedy might be to seek and to undertake administrative revision of policies and programs. These could include the following proposals:

1. Governmental agencies charged with the research and development of electronic equipment essential to the national security should be provided with clearly defined authority and procedures for testing such equipment against appropriate communications systems.

2. Consideration should be given to seeking specific Congressional and Presidential designation of certain international criminal activities as matters affecting the national security (e.g., international narcotics trafficking, gun-running, etc.) for purposes of foreign intelligence-gathering.

3. National security intelligence agencies should be authorized to provide appropriate U.S. law enforcement agencies with criminal intelligence incidentally obtained in the exercise of their lawful functions, including information indicating criminal activity on the part of U.S. citizens.

4. An effort should be made (consistent with the constitutional rights of criminal defendants) to secure legislation and/or rules changes to prevent the public identification of national security agencies as the source of criminal intelligence incidentally obtained in the exercise of their lawful functions, at least where such evidence is not introduced at trial.

5. The authority of the CIA, NSA and FBI to perform their respective missions in the field of electronic surveillance should be clearly delegated and delineated with specific procedures prescribed for the lawful exercise of that authority.

6. The Office of General Counsel for each intelligence agency should be staffed with one or more attorneys with expertise in electronic surveillance law and Federal criminal law and procedure.

7. Agency personnel should be required to consult their General Counsel and confirm, in advance, the legality of all electronic surveillance projects.

* * *

The recommendations of the task force set forth above are (accepted) (rejected).

BENJAMIN R. CIVILETTI
Assistant Attorney General
Criminal Division