Glauberman, Steven L.
Conference on the Boundaries of
Privacy in American Society
Woodrow Wilson School of Public
and International Affairs
November 19, 1971

FEDERAL AGENCIES

INVOLVED IN

DOMESTIC SURVEILLANCE

Steven L. Glauberman

Steven L. Glauberman

January 3, 1972

I. STATEMENT OF THE PROBLEM

The problem of this paper is to investigate the nature of domestic surveillance by agencies in the Federal Government, the extent to which this surveillance transgresses on the rights of privacy, and to determine what modifications in the law can redefine and protect these rights.

II. SUMMARY OF PRINCIPAL FINDINGS

1. The growing complexities of centralized government have increased the need for information-gathering activities.

2. The technological revolution produced the computer--a cybernetic creation which enhanced the governmental appetite for information.

3. The decennial census stipulated in the Constitution has included in recent years several possible privacy-intruding questions.

4. There is evidence that the confidentiality of the decennial census has been breached by interagency information transfer.

5. The United States Army has developed a highly complex information-gathering network with the expressed purpose of formulating contingency plans for domestic civil disorder, but which has grown beyond its mandate to create personality files.

6. The Justice Department has created a vast network of information data banks to aid in crime prevention.

7. The constitutionality of the electronic eavesdropping device has not been clearly defined by Congress or the Supreme Court, however, the Omnibus Crime Control and Safe Streets Act of 1968 has specified that for all wiretapping and eavesdropping, including national security cases, a court warrant is necessary.

8. Under the Nixon Administration, extensive surveillance of this nature has been conducted with national security surveillance being authorized solely by the Attorney General.

III. POLICY RECOMMENDATIONS

1. The Bureau of the Census must be prevented from disseminating any information to other federal agencies which it has garnered on a supposedly confidential basis.

In evaluating its operating function, the Bureau of the Census should review the 1970 census questions for violations of personal privacy, should distinguish between collective and individual data, and should determine the propriety of Census Bureau surveys for other agencies in light of voluntary response requirement. (pp.11-14).

2. The Congress of the United States should establish a congressional commission to supervise the separation of Army intelligence and Army security clearance files.

This commission should consist of eight members; four members from each house and their selection by each house should consist of two members from the respective Committee on Armed Services; and two members from the respective Committee on the Judiciary. Furthermore, this commission should be bipartisan in composition and the members shall serve nonconsecutive two year terms. (pp.26,27).

3. This commission in cooperation with the Office of the Secretary of Defense and respective Military Services, should regulate the computerized information retrieval networks.

Among its considerations, this commission will investigate military surveillance in sectors for which civilian law enforcement agencies are ordinarily responsible. (pp. 27, 28).

4. By an amendment to the Omnibus Crime Control and Safe Streets Act, the Congress should distinguish between the status of an alien and a citizen, and the situation of emergency and nonemergency with regard to surveillance authority.

This clarification will resolve the penumbra of discretion in previous wiretap grants. (pp. 38).

5. By an act of Congress, a new level of judicial authority should be created to review all authorizations for national security wiretapping, replacing the sole discretion of the Attorney General.

This court of warrants, as it shall be known, shall consider wiretap requests by federal agencies. It shall consist of three judges to be appointed by the President in the constitutionally prescribed process. (pp. 39 - 40).

6. The Federal Communications Commission should conduct an extensive policing of the nation's telephone lines to eliminate all unauthorized wiretapping and electronic eavesdropping.

Thus far, this independent commission has failed to exercise its legal duty. (p. 40).

IV. TABLE OF CONTENTS

		Page
I.	STATEMENT OF THE PROBLEM	ii
II.	SUMMARY OF PRINCIPAL FINDINGS	iii
III.	POLICY RECOMMENDATIONS	iv
V.	DISCUSSION	1
	Introduction	1
	Computers and Dossiers	4
	The Bureau of the Census	7
	Department of Defense-- Army Surveillance	14
	Department of Justice	28
	Electronic Eavesdropping and Wiretapping . . .	30
	National Security Eavesdropping	35
VI.	BIBLIOGRAPHY	42

V. DISCUSSION

Introduction

> The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. . . . They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone - the most comprehensive of rights and the right most valued by civilized men.[1]

Nearly two hundred years ago, the Founding Fathers empowered the federal government with the responsibility of promoting and preserving the general welfare of the people. At the same time, they assigned to federal jurisdiction the duty of protecting the liberties of the individual citizen among which was the right to privacy. To guarantee the success of this republican experiment, a national establishment was designed to formulate national priorities and translate these goals into realistic, concrete programs. Information about the citizenry and the society thus became a necessity for public policy making during the formative years of this nation. Dating from the first decennial census in 1790, the governmental information gathering role has expanded as government itself has grown in response to the proliferation of demands made upon the federal government. On the other hand, America has been careful to encourage its

---

[1]Louis D. Brandeis, Dissenting, Olmstead vs. U. S., 277 U. S. 438 (1928).

citizens to act free from an all encompassing sense of being observed and recorded. Indeed, the approach to privacy taken by Americans, developed from a tradition of limiting the surveillance power of authorities over the private activities of individuals and groups.

What then has stimulated the recent controversy and frenzy about the boundaries of privacy in American society? First, as a result of federal action in the wake of the great depression, the role of the federal government in the policy realm has been greatly augmented. Secondly, this increase in federal responsibility and demands placed upon federal officials has been accompanied by a parallel increase in the demand by the federal level for greater quantities of personal information from the individual. Complicating this expansive trend in the information-based society, the innovation of an inexorable reality of available new technology has led to faster, more efficient, more pervasive information gathering. Today, the accumulation of data about individuals for a variety of governmental purposes has become a major activity of many federal agencies. Quantitatively, the private life of the average American is the subject of ten to twenty dossiers of personal information in the field and computer data banks of government agencies.[1] For the first time in history, the

---

[1] "Senators Hear of Threat of a Dossier Dictatorship." New York Times, February 24, 1971.

ability to collect and store data has equaled the need for information about its citizens by the federal government.

The opportunity exists today to create meaningful programs and to measure their effectiveness. But in doing so, the government must guarantee Americans that the tonic of high speed, extensive information handling does not contain a toxic which will kill their privacy. Therefore, we are moved to examine the information-gathering techniques and the permeation of citizen surveillance. We are moved to analyze and carefully assess the importance of privacy in our society. What are the limits of legitimate interference of collective opinion with individual independence in the cybernetic revolution? What is the extent of federal information gathering? What federal agencies are employing undercover, concealed methods of surveillance? Is the need for information to promote the "general welfare" in a technologically abetted society incompatible with a notion of privacy? Now is the time to cement a balance between both sides of this scale of American society. Now is the time to determine to what extent Americans are willing to exchange some freedom and privacy in one area for other social gains.

This paper will examine these questions which embrace the United States in the 1970's. It will analyze first the methodology and the users of data collection and surveillance, and secondly, the cost of these activities in terms of the

see 4-a & 4-b (Addendum)

individual's right of privacy. Moreover, this paper will try to reveal some insights into how a society with a reputation for providing liberty can further provide limits on the surveillance power of authorities in order to ensure both the preservation of privacy and the solution to impending problems.

Computers and Dossiers

> Government should be allowed to know a great deal more than it does about the community it was selected to serve. This requirement is essential if we want to see decisions made on the basis of fact. You cannot manage an advanced society, which is a vast, complex interconnecting system unless the facts are available.[1]

Throughout the federal government records are maintained on individuals varying from agency to agency as to scope of information recorded. These differences reflect particular functions performed by each agency and the provisions of federal law which specify responsibilities, program administration, and national security implications of the agency's mission.[2]

The compiling of dossiers on individuals, however, is not a new phenomenon in this country. "The Federalists,

---

[1]Arthur R. Miller, The Assault on Privacy: Computers, Data Banks, and Dossiers, p. 126.

[2]"Controversy over Federal 'Data Banks,'" Congressional Digest, 50:10 October, 1971, p. 226.

The present scope of federal data gathering surveillance varies greatly from agency to agency. Records maintained by elements of the Federal Government on individuals and organizations particularly depict this diversity as to volume and scope of information recorded. Such differences reflect among other factors, particular functions performed by agencies involved, provisions of Federal law which specify responsibilities and programs administered by such agencies, national security implications of the agency's mission, and in some instances, differences in administrative philosophy among the Federal agencies and departments involved. Needless to say, the multitude of federal agencies is significant. Indeed, such a listing prominently includes the Census Bureau and Patent Office within the Department of Commerce, the Civil Service Commission, the Selective Service and several bureaus within the Department of Defense, Health, Education and Welfare, Housing and Urban Development, Justice, State, Transportation, and the Treasury. In addition, according to Frank Donner, who addressed the Princeton University Conference on the Federal Bureau of Investigation, there are approximately twenty federal agencies that are involved in surveillance-intelligence activities.[1]

---

[1]Frank Donner, "The Theory and Practice of American Political Intelligence," (Reprint from The New York Review of Books), 1971, p. 2. These include the FBI, Army, CIA, IRS,

Both types of activities have become pervasive in today's society.

In light of the extent of domestic information gathering and/or surveillance activities conducted by federal agencies, a study with the expressed purpose of evaluating the effect of agency surveillance on the individual's right to privacy will prove to be a formidable task. Regretfully, not every agency so involved can be sufficiently inspected at this time. Thus, for the purposes of this paper, it will focus only on the most dynamic, most intensive and most privacy-threatening activities. Accordingly, first the Bureau of the Census shall be considered because it is purported to have the most stringest code of confidentiality for data gathering. Nevertheless, as shall be depicted, the Census Bureau can and does pose serious danger to privacy. In addition, the subjects of this paper shall include those activities of the Department of the Defense, in particular the Army, and the Department of Justice. It is hoped that the reader will be given a more realistic perspective of the pervasiveness of governmental surveillance networks in view of those agencies which accentuate the extent of such activities and their counter effect on privacy.

Post Office, Secret Service, Customs Bureau, Civil Service Commission, Immigration and Naturalization Service, Navy, Air Force, Coast Guard, Passport Division of the State Department, Department of Justice, Department of Health, Education and Welfare, Office of Economic Opportunity.

enforcing the first Alien and Sedition Acts, doubtless compiled dossiers on known and suspected Jacobians. But when they had served their purpose in the prosecution of the suspects, they were apparently discarded."[1] However, as American society grew more complex, and as we have perceived more justifications why one man may have a legitimate interest in the affairs of another, the business of compiling personal dossiers has increased rapidly. Because law-enforcement agencies have a legitimate interest in a variety of information, they compile files. In the interests of efficiency, these records become permanent. Moreover, in addition to the degree of permanency achieved by a dossier, the tendency arose within the federal structure to interchange data when one agency had already compiled a file on a subject.

Despite the guarantees of the Constitution with respect to the arbitrary use of the recordkeeping and information power of government and the growing practice of interchange, the demands for efficiency were not exhausted. Responding to the need for efficiency, the technological revolution provided the computer--a cybernetic creation which greatly enhanced the governmental appetite for information. The limitations of prior efforts at information gathering

---

[1]Vern Countryman, "Computers and Dossiers," The Nation, 213:5, August 30, 1971, p. 134.

were no longer imposing, as the computer's capability brought forth an answer to efficiency, speed, and quantity of data capable of collection, storage, and access. Indeed, the computer's entry into governmental data collection casts a dark shadow on privacy. What has occurred in reality is the rapid adaptation of a technological system able to manipulate vast amounts of data by analyzing seemingly unrelated variables.

> Before the computer age, government also kept dossiers on individuals--criminals and non-criminals--which detailed their histories, personal habits, associations, and views. But they were contained in files handled manually--files that were laborious to locate, space consuming, and could not easily be transferred to other agencies interested in particular individuals.
>
> Today, however, information can be and is stored in computers or data banks, and can be sent almost instantaneously to a requesting agency. What is more, it is unlikely to be lost and takes up relatively little space.[1]

Among the federal agencies utilizing the computer data system, there are the Bureau of the Census, Internal Revenue Service, Departments of H. E. W. and H. U. D., and the law enforcement agencies, the Department of Justice (particularly the FBI) and the Department of Defense (particularly the Army). Thus, the computerized dossier has made it possible via remote-access, time-share systems to link all federal data banks

---

[1] "Invasions of Privacy," Congressional Quarterly, XXIX:9, February 26, 1971, p. 457.

through computer terminals and storage systems. Although as far as is known, this potential has not been activated. The capability exists not only to coordinate agency to agency information processes, but also for a third party to tap into federal computerized data retrieval systems and obtain personal information without government permission and knowledge.

The Bureau of the Census

The oldest and perhaps the largest data bank maintained by the federal government is the Bureau of the Census. In operation since the last decade of the eighteenth century, the Census Bureau is, in reality, the aggregate of two related processes. First, it conducts

> . . .the decennial census which has evolved from the simple enumeration of the populace called for by the United States Constitution to a comprehensive survey seeking numerous items of personal date designed to portray the quality of life in the nation.[1]

Primarily, questions regarding population, the census does serve the vital function of determining legislative apportionment and the allocation of federal funds. Secondly, the Bureau of the Census possesses the first if only legitimate

---

[1]Miller, op. cit., p. 127.

data bank in the nation with microfilm of all census records from 1900 to the present.

As evidenced by the last two decennial census questionnaires in 1960 and 1970, this query has developed into a sensitive probe of the activities and life styles of individual citizens. In 1960, one out of every four Americans received the "blue form" household questionnaire which requested information about individual housing and access to modern conveniences. Whereas questions such as "how many bedrooms are in your house or apartment," can be considered acceptable under the 1940 amendment to include a housing census, the admissibility of the following queries remains in some doubt:

> Do you have a clothes washing machine?
> Do you have an electric or gas clothes dryer?
> Do you have any television sets?
> Do you have any radios?
> Do you have air conditioning?
> How many passenger automobiles are owned or regularly used by the people who live here?[1]

Furthermore, the 1970 census was even more comprehensive from the standpoint of personal information gathered. Although the majority of Americans were subjected to a relatively mild interrogation, millions of citizens received consid-

---

[1]Vance Packard, The Naked Society, p. 268.

erably more extensive forms, incorporating additional questions with respect to health, employment, finances, and housing:[1]

> How much rent do you pay?
> How much did you earn in 1967?
> If married more than once, how did your first marriage end?
> Do you have a telephone? If so, what is the number?
> Do you have a bathtub or shower?
> Do you have a flush toilet?[2]

In addition, the Bureau of the Census extracts this information under the threat of criminal penalties. On the few occasions when the law was challenged, the Supreme Court upheld the broad discretion of the Bureau under the constitutional provisions and Section 221 of Title XIII, U. S. Code, 68 Stat. 1023; 71 Stat. 484:

> This section authorizes fine or imprisonment for anyone over 18 years of age who refuses to answer 'any of the questions on the schedule submitted to him' in connection with any duly authorized census or survey when requested to do so by the Secretary of Commerce.[3]

Nevertheless, the Bureau is enthusiastically respondent

---

[1] Miller, op. cit., p. 127.

[2] Ibid.

[3] Packard, op. cit., p. 269.

to include at the request of private enterprise and social planners, questions which will help them craftily solicit business. Commercializing census tracts has become a frequent activity of the Bureau as it provides a great deal of valuable and extensive statistical data to interested groups including business corporations.^ See 10-a & 10-b (Addendum) Individual information, however, remains available only to the individual concerned or his legal heirs.

The judicial decisions upholding the responsibility of the individual citizen to respond to each and every census question are correct. What behooves further investigating is the extent to which the decennial "enumeration" is conducted and the use to which the data is applied. As illustrated, the most recent census surveys include not only population information, but also probes into matters of race, industry, business, agriculture, marital status, family size, geographical location and mobility. In addition to the information, the Census Bureau also obtains information from other agencies such as the Internal Revenue Service, and the Department of H. E. W.'s Social Security Administration. Although the Census Bureau is not interested in individuals but in groups, the potential remains for interagency accessibility to census records. "The criticism leveled against it, notwithstanding, the Census Bureau has an unequaled record among federal agencies in pre-

Vance Packard calls this problem the right to be free from bureaucratic harassment. Moreover, it is necessary to understand not only how such questions overstep the authority of the Bureau of the Census, but also how they pose serious threats to privacy. Indeed, the answer lies not in the seeming innocence of the question, but instead the use to which the information is put. For example, today, any citizen or organization can write the United States Department of Commerce - Bureau of the Census in Washington, or one of the forty -two field offices of the Bureau, and for a price of $111.00 for the entire set of reports, or for a price ranging from $1.00 to $5.25 for an individual report, receive a copy of the 1970 Census of Housing - Final Report - Detailed Housing Characteristics HC (1) - B Series.

> These reports will focus on the housing subjects collected on a sample basis. Subjects to be included in these reports are tenure; occupancy and vacancy characteristics; utilization characteristics (number of rooms, number of persons, persons per room, and bedrooms); structural and plumbing characteristics (kitchen and plumbing facilities, bathrooms, units in structure, year structure built, access to unit, source of water, sewage disposal, basement, and elevator in structure); equipment (heating, air conditioning, telephone); fuels used for heating and cooking; appliances (clothes washer, clothes dryer, dishwasher, etc.); automobiles available; ownership of second home; and financial characteristics (value, rent). In addition, for areas with Negro and/or Spanish population of specified size, the reports present selected data for these subgroups. Statistics will be shown for some or all of the following areas: States and counties (by farm-nonfarm residence),

> standard metropolitan statistical areas, urbanized areas, and places of 2,500 inhabitants or more.[1]

Indeed, this information is broken down from national, regional and statewide statistics into municipal and sub-municipal areas. Admittedly, the Bureau of the Census still maintains the admirable regulation of personal information. Yet, by providing, for example, plumbing statistics to corporations in this line of business, which pinpoint particular areas of municipalities as characteristically in need of plumbing fixtures, these residents could be subjected to undue harassment.

> Furthermore, in 1960, the country was divided into tracts each containing 4000 to 7000 people. As a result, the Commerce Department, via the Census Bureau was able to provide a lot of valuable statistics to interested groups. . .including the Reuben H. Donnelly Corporation which had to a large extent built an empire on the basis of buying Census tracts and selling the information.[2]

Moreover, partial blame must be attributed to the Census Bureau because this information is not being used for the expressed use of related agencies.

---

[1] 1970 Census of Housing - Final Reports - Detailed Housing Characteristics HC(1) - B Series, U.S. Department of Commerce, Bureau of the Census, Taken from Publications Order Form, p. 2.

[2] Packard, op. cit., p. 271.

serving the confidentiality of personal information. But this past record is no guarantee for the future."[1]

Statutory limitations prohibited dissemination of information for identifying purposes. However, this means the propriety of releasing data depends on what a user might infer from the data.[2] Furthermore, disclosure decisions are left to Bureau workers who possess the ability of destroying the confidentiality of census data by complying with requests for small aggregates of computer microdata.

> Another potential loophole in the statutory scheme protecting census data can be found in the Secretary of Commerce's authority to furnish tracts to states and courts for geneological purposes. . . .Although this provision is primarily utilized by individuals who need information about themselves. . .particularly for proof of age in connection with. . .benefits, it operates as an ill-defined exception to the prohibition in the confidentiality of the Bureau's operation.[3]

In conclusion, despite essentially conducting a tightly knit process, the Bureau of the Census suffers from a limitation that confidentiality restrictions are made without giving the individual citizen involved easy access to the data and also, an opportunity to challenge disclosure.

---

[1]Miller, op. cit., p. 135.

[2]Countryman, op. cit., p. 145.

[3]Miller, op. cit., p. 137.

To remedy the present limitations and to prevent future abuses of this vast data bank, the Census Bureau, in effect, must remove itself as an avenue of information for other federal agencies and private business groups. Since the Census Act's confidentiality restrictions are applicable to Bureau officials who gather the information initially it is probable that "they cannot be enforced against a third party who lawfully obtains information from the Bureau and subsequently misuses it."[1] Moreover, this statute does not rule out the possibility of other federal agencies composing a questionnaire containing questions that appear on a census survey and imposing it on part of the public. "Many agencies use the ploy of having the Census Bureau conduct surveys for them."[2] Inevitably, the Census Bureau processes the surveys for the requesting agency and then transfers the information via computer tapes to that agency. Needless to say, "the excelled confidentiality record of the Bureau of the Census becomes irrelevant since it no longer can control the use or dissemination of the date."[3]

This administration of questionnaires for other federal agencies poses a potential and at times active threat to pri-

---

[1] Ibid., p. 138.

[2] Ibid., p. 139.

[3] Ibid.

vacy. In the case of surveys merely conducted by the Census Bureau for other elements of the federal government, failure to respond to these polls unlike the decennial census, are not subject to criminal penalties. Yet, nowhere on these probing interrogatories does this fact of voluntary compliance appear. In reality, the recipient becomes coerced by the seal of the Census Bureau. Senator Sam J. Ervin, Jr. (D-NC) chairman of Senate Judiciary Subcommittee on Constitutional Rights pointed to the correct mechanism to alleviate this condition:

> I differ with those who say that there are no existing checks on this developing power of computer technology, for I believe they already exist in our form of Government. The guarantees are established in our Constitution.[1]

Accordingly, the Census Bureau must endeavor to disassociate itself with abetting other federal agencies. It must also carefully review the questions to be placed on the decennial survey. Furthermore, it should not sacrifice the pretext of confidentiality that it purports to maintain for the sake of harmony with other agencies by serving as a center for information distribution and gathering responses to questions not related to their function.[A] See 13-a & 13-b (Addendum) With regard to access to individual dossiers, "The only 'need' for preserving keys to personal identity in the Bureau population statistics is that

---

[1] Congressional Digest, op. cit., p. 237.

Congress can aid in these privacy protecting endeavors by recalling from committee House of Representatives Bill 9527 since it gives the individual access to his records while at the same time restricting other's access to it. Indeed, this legislation would greatly diminish the possibility of disclosure after the Bureau transferred information to another agency. In addition, the misuse of the Bureau's seal could be avoided if the Bureau were (a) instructed by Congress as to what areas citizens may be questioned and required to respond; (b) required to clearly distinguish on the surveys between questions to which responses are mandatory and questions to which responses are voluntary; (c) allowed to report only aggregate data to other federal agencies; (d) enjoined from conducting surveys for, or reporting information to, private concerns.[1] Provisions similar to these are included in Senate Bill 1791 and consideration of this bill should be carried out by the Congress, too.

The record of the past is clear. The Bureau of the Census does have a commendable record for maintaining the confidentiality of personal data files."The rules of confidentiality in the treatment of responses to census questions are as firm and clear as they have ever been."[2]

---

[1]Steven Pavsner, Commissioner's Report to Conference, December 1, 1971, p. 2.

[2]William H. Chartener, U.S. Assistant Secretary of Commerce for Economic Affairs, Congressional Digest, op. cit. p. 252.

However, with regard to statistical data, the avenues for abuse are available. Other federal agencies often subcontract with the Census Bureau to conduct other agencies' surveys under the seal of the Bureau of the Census.

This examination, moreover, is designed to be prescriptive. For indeed, if the Federal Government's most security-oriented data collection agency can abuse the individual's right to privacy through use of statistical information, then one can be only be further anguished by the revelations concerning more personalized disclosures of such agencies as the Department of Health, Education and Welfare's Social Security and Aid to Dependent Children Administrations, and the Internal Revenue Service use of tax return information.

those keys facilitate keeping the statistics up to date and adapting them to new uses during the ten-year period between censuses."[1] How vital is that need, and could it not be met instead by taking a population census at more frequent intervals?

Department of Defense--Army Surveillance

> Within the past year, there has been a focus of official and public attention on the fact that for a period of time during the 1960's the Military Services were engaged in the collection and analysis of information on persons and organizations not affiliated with the Department of Defense. Clearly there is not precedent for the scope and intensity of information collection and analysis related to the civilian communities which occurred in the period in question. The character and extent of information collection undertaken by the military and the curtailment of this activity during the past two years can only be understood if related to the circumstances which initially led to the military involvement.[2]

With those words, Mr. Robert F. Froehlke, U. S. Assistant Secretary of Defense opened his testimony to the Senate Subcommittee on Constitutional Rights to elucidate about the nature of information collection by the Military Services, particularly the United States Army. What concerns us today is not the data pertinent to service personnel having current duty or standby status which is main-

---

[1] Countryman, op. cit., p. 149.

[2] Congressional Digest, op. cit., p. 236.

tained in the active files of the Department of Defense. Instead, the scope of Department of Defense information-gathering which is of paramount interest is the surveillance and intelligence operation which for the last decade has been conducted by the United States Army. In particular, this intelligence activity places emphasis on amassing information with regard to civilian politics and potential civil disturbances. Has the Army overstepped its authority to conduct security clearance investigations and to preserve the "domestic tranquility"? Are such surveillance activities transgressing upon the individual's right of privacy? And furthermore, has the Army, indeed curtailed surveillance activity during the past two years?

A number of instances in American history exemplify the use of National Guard or Federal Troops by civilian authorities in connection with domestic disturbances. Accordingly, Article IV, Section 4, of the Constitution of the United States provides:

> The United States shall guarantee to every State in this Union a Republican Form of Government, and shall protect each of them against Invasion; and on Application of the Legislature, or of the Executive (when the Legislature cannot be convened) against domestic Violence.[1]

---

[1] The United States Constitution, Article IV, Section IV.

Prior to 1960, instances of civil disturbances were ". . .sufficiently infrequent and isolated so as to preclude any necessity for detailed contingency planning by Federal civilian or military authorities."[1] However, in the early 1960's, civil disturbances became more frequent and more intense, particularly; as the barriers of race began to dissipate throughout the nation. Federal officials charged with responsibility for the commitment, deployment, or potential deployment of Federal troops made a request for improved planning in federal assistance to states and local communities during civil disturbances. Prior to the summer of 1967, the involvement of the Military Services in collection of civil disturbance information could be characterized as minimal but increasing. July and August of 1967, however, marked a turning point. Rioting in Newark and Detroit, respectively, motivated civilian and military officials at the highest levels of government to place heavy emphasis "on improving the preparedness of the Federal Government structure including the military" to respond to large-scale civil disturbances.[2]

Nevertheless, during 1967, the character of civil disturbances metamorphosized from largely racial matters precipitated by a chance incident to pre-planned, pre-announced

---

[1]Congressional Digest, op. cit.

[2]William Beecher, "Laird Picks Panel to Curb Army Spying on Civilians, New York Times, February 19, 1971.

assemblies of people across the nation to protest the Vietnam war. It was the cumulative impact of these developments which led the Army "being asked to plan for possible commitment of Federal troops in as many as 25 major cities concurrently."[1] Upon commendation by the Kerner Commission report, the Army's involvement in collection and analysis of information on civilians and organizations not affiliated with the Defense Department was made operative.

> Although all of the Military Services were subjected to requirements connected with information collection related to civil disturbances, the Department of the Army, had the responsibility for the principal effort.[2]

The genesis of Army investigative and related counter-intelligence organizations in the collection and utilization of information began on January 1, 1965, when the United States Army Intelligence Command CONUS Intelligence commenced gathering all the previously parceled information units. The Commander of CONUS (Army's acronym for Continental United States) reserved to himself the authority to approve any covert collection. In retrospect, it becomes evident that initially only "a small proportion of the total effort was used for collection or processing of civil disturbance information."[3] The great majority of investigative personnel

---

[1] Congressional Digest, p. 238.

[2] Ibid.

[3] Ibid. p. 240.

were engaged in the routine personnel background investigations.

As civil violence proliferated in the first six months of 1968, however, law enforcement agencies, including those on the Federal level, made known to high civil authorities, their lack, in quantity and quality, of the necessary resources to cope with increasing demands for information. As a consequence, a more comprehensive and detailed intelligence document, the Department of the Army Civil Disturbance Information Collection Plan, was issued. It "provided that predisturbance information would be obtained by drawing on other Federal as well as State and local forces."[1] Commenting further on the Collection Plan, Froehlke stated:

> If the Army must be used to quell violence it wants to restore law and order as quickly as possible and return to its normal protective role--to do this it must know in advance as much as possible about the well springs of violence and the heart and nerves of chaos. . . .It is highly improbable that many of the requirements listed could be obtained by other than covert collection.[2]

Thus, the stage was set for the beginning of army spying. This build up of an army intelligence mechanism is a concentration of authority for the wrong reasons.

---

[1] Ibid. p. 240.

[2] Ibid. p. 242.

> The records clearly indicate that military resources were employed because civilian agencies--Federal, State, and local--had demonstrated a lack of capability to provide the quantity and type of information believed to be necessary effectively to cope in a timely fashion with the emergency then prevailing.[1]

However, bureaucratic inability to cope with civil disorder is a false pretense for creating a mechanism which potentially could and in actuality has transgressed the legal boundaries of privacy. True, the original purpose was somewhat legitimate in that an early warning system for pending civil disturbance was necessary in case the Army might be called upon to quell it. Yet, today, this operation has proliferated into a surveillance organ designed to gather dossiers on not only violence-prone organizations, but such non-violent groups as the Southern Christian Leadership Conference and the NAACP, and on files devoted exclusively to descriptions of the lawful political activity of civilians.

There can be no question that the Army needs information to aid civilian authorities in potential riot or disaster situations. Moreover, prior to exposing its personnel to military secrets, it has to check into their past behavior for evidence of disloyalty and unsuitability. The Army must investigate any disaster which might disrupt the nation's lines of supply. And finally, it has the obligation to keep informed about the whereabouts and activities of left and right wing, ultra-militant subversives. "But must it also

---

[1] Congressional Digest, op. cit., p. 244.

distribute and store detailed reports on the political beliefs and actions of individuals and groups?"[1]

At present, the Army publishes a "blacklist" encyclopedia of profiles of people who in the opinion of the Intelligence Command officials, might cause trouble for the Army.[2] Secondly, the Army, too, foreseeing that computer technology permits the most extensive collection and retrieval systems for information, has developed a computerized data bank at the Investigative Records Repository at Fort Holabird in Baltimore, Maryland. Supplementing its seven million individual security-clearance dossiers, the Army data bank feeds both "incident reports," relating to the Army's role in domestic disturbances and "personality reports," extracted from these incident reports. Furthermore, these personality reports generate new files on the political activities of civilians wholly unassociated with the military.

What is perhaps most remarkable about this domestic intelligence network is its potential for growth and interagency access.

---

[1]Christopher Pyle, "Conus Intelligence: The Army Watches Civilian Politics," Washington Monthly, 1:12, January, 1970, p. 8.

[2]Ibid. p. 6.

> Because the Investigative Records Repository is one of the federal government's main libraries for security clearance information, access to its personality files is not limited to Army officials. Other federal agencies now drawing on its memory banks include the FBI, the Secret Service, the Passport Office, the CIA,. . .the Civil Service Commission, the Atomic Energy Commission. . .the Navy, and the Air Force. In short, the personality files are likely to be made available to any federal agency that issues security clearances, conducts investigations, or enforces laws.[1]

The complexity of the Army intelligence network did not end with the Fort Holabird Army computer. Before public outrage of the past year forced Army curtailment of camouflauge of civilian surveillance, there was established a computer-indexed, microfilm archive of intelligence reports at the Alexandria, Virginia headquarters of the Counter Intelligence Analysis Division (CIAD). Two other computerized data banks were maintained at Fort Monroe, Virginia, and Fort Hood, Texas. In addition, the 300 stateside Army intelligence offices maintained noncomputerized, regional files on local political groups and individuals. The Army also distributed to its branches and various government agencies 375 copies of an encyclopedic "compendium" of individuals and organizations.[2]

To provide the information for these computerized

---

[1] Ibid. p. 6.

[2] Christopher Pyle, "Conus Revisited: The Army Covers Up," Washington Monthly, 2:5, July, 1970, p. 51.

dossiers, the Army has utilized its own plainclothes agents as well as sources from other agencies, federal, state, and local, and news media clippings and radio monitored broadcasts. Covert surveillance reports filter in from former agents such as John O'Brien, a member of the 113th Military Intelligence Group who related his CONUS section amassed data on Illinois citizens who espoused discontent with the military involvement in Southeast Asia. Reportedly, two of the more prominent subjects were Senator Adlai E. Stevenson III (D-Ill) and Representative Abner Mikva.[1] However, some subjects of surveillance were of legitimate interest such as Weathermen subversives, but many others were engaged in constitutionally-defensible activities such as writing letters to congressmen, signing petitions, and marching in peaceful demonstrations. One area of continued undercover military spying intrusion has been the nation's colleges and universities, scene of scores of anti-war protests, moratoriums and the May, 1970 student strikes. During the latter protests against Administration policies in Southeast Asia, Army intelligence activities were widespread and intensified. Succumbing to its "obligation" for Vietnam protest, Princeton University joined hundreds of colleges in campus disruption. According to university officials and local police, several plain-clothes "students" were seen inconspicuously taking

---

[1] "Army Files: 'Clear and Present Danger' to Freedom," Congressional Quarterly, XXIX:10, March 5, 1971, p. 511.

photographs of demonstrators at a sit-in on the grounds of the Institute for Defense Analysis (IDA)[1] Although identification was never substantiated, students were known to be paid informants by several law-enforcement, surveillance agencies.[2] In light of the extent of Army intelligence activities, the rule of the game seems to be that nothing is too trivial to investigate.

Considering the limits of authority, the Army's surveillance endeavors provide a weak defense for preserving the domestic peace.

> The Army justification for the collection of domestic political information generally is based on its responsibility to maintain order in case of major riots or civil insurrection.[3]

However, in the event of insurrection, it would be the civilian police agents that would be responsible for the arrest of guerillas and insurgents. Moreover, there appears to be a total lack of justification for the maintenance of files on elected political leaders. Although the personality files and blacklists were designated to facilitate

---

[1]Confidential Interview A., Princeton, N. J., November 3, 1971.

[2]Ibid.

[3]"The Invisible Intruders," Saturday Review, No. 19, January 30, 1971, p. 20.

selective arrests of subversives, this fails to account for the fact that the Army lacks authority to round up suspects the moment civil disturbance seems imminent. Moreover, "the seizure of civilians on suspicion of conspiring or attempting to overthrow the government by unlawful means. . . continues to be the responsibility of local and state police and of the FBI."[1] Only in the rare case of martial law, when civilian law enforcement has been unable to function, the Army is given all governmental authority. Perhaps then, it might need these personality files, blacklists, and the mammoth, interconnecting data retrieval system.

Does the Army need to conduct civilian surveillance and keep its own dossier on the politics of law-abiding citizens and groups? What makes its agents more competent than the FBI or local police departments? In addition, "are the civilian authorities so uncooperative that the Army must substantially duplicate their efforts?"[2] According to the present Administration, the authority for the Army program comes from the Constitution, Article II which permits the President to engage in whatever "intelligence activities

---

[1]Pyle, op. cit., p. 8.

[2]Ibid., p. 9.

[3]Ibid.

are necessary to protect the nation. . . ."[1] Contrasting this inherent-powers doctrine, the Army's authority to collect domestic intelligence is limited by those laws which distinguish the Army's responsibility for law enforcement from that of other agencies. Once again, responsibility lies with the FBI rather than the military. Furthermore, Army authority is confined to the policing of political activity only within the armed services and those laws under federal-state agreements where Army installations are governed.

The effect of this dossier-feeding surveillance is all too clear as a result of recent public outrage against Army spying.

The Defense Department, however, in other less-publicized ways, encroaches upon the individual's right to be free of bureaucratic harassment by its labeling anyone working for a private defense contractor as a security risk without offering the worker a chance to confront his accusers. The Defense Supply Agency additionally maintains an index file of 1.5 million personnel cards detailing security clearance information for individuals employed by contractors engaged in classified work for the Department of Defense.

---

[1]"The Scope of Present Federal Activity," Congressional Digest, op. cit., p. 227.

Obviously, the Department must have the power to protect its classified information. But in protecting the national security, flagrant abuses of individual rights have occurred.[1]

In conducting surveillance activities under the guise of intelligence needs, the Department of Defense, therein the Army, has overlooked a fundamental principle in American government: that the military authority shall remain subordinate to civilian control.^ The maintenance of political dossiers and military surveillance, is in contrast to the aforementioned principle.

See 26-a, 26-b, & 26-c (Addendum)

What check and balance recourse do citizens presently have? Secretary Laird's formation of a high level civilian-dominated board to assume direct control of investigations in this country by military intelligence is at best only a beginning.[2] Because these civilian officials are career Defense Department bureaucrats, the return of an overzealous military to its proper perspective necessitates effective and assertive action. Therefore, a new civilian review board should be established. This commission should be created immediately by Congressional mandate and should consist of four members of each house of Congress; furthermore, it should be bipartisan in nature with commission members chosen

---

[1]Greene vs. McElroy, 360 U. S. 474 (1959).

[2]Beecher, op. cit.

This realization becomes self-evident in view of two considerations. First, as depicted earlier, throughout times of peace within this century, law enforcement and the prevention of crime and civilian insurrection has always been the responsibility of civilian agencies from local police departments on upward to the federal government's arm, the Federal Bureau of Investigation. To maintain the domestic tranquility, civilian law enforcement agencies will more than likely require some form of intelligence information. Nevertheless, these surveillance activities should be conducted by civilian agencies, and not the military services. Second, it seems apparent from the statements of denial issued by the Office of the Secretary, that the Secretary of Defense has not issued explicit orders permitting or recommending military surveillance of civilian activities. Nor is it self-evident that these orders are emanating from the White House. Hence, if these premises are correct, then perhaps it might not be too speculative to assert that military officials are overstepping their authority because they are engaging in activities of a highly dubious nature in view of their jurisdiction. Indeed, these activities do not merely require field decisions made by military personnel, but instead, they demand policy decisions set forth by civilian officials in the Department of Defense or the Executive Office of the President.

Despite Assistant Secretary of Defense Robert F. Froehlke's assertion that:

> The records clearly indicate that military resources were employed because civilian agencies - Federal, State and local - had demonstrated a lack of capability to provide the quantity and types of information believed to be necessary effectively to cope in a timely fashion with the emergency then prevailing.[1]

the solution to this situation is not a transgressing military establishment. Henceforth, the civilian authorities within the Department of Defense and in the Congress should investigate these allegations to allay those fears of an uncontrollable military undercover operation.

Furthermore, we must not forget the traditions of this country's founding principles. Conservatives remind us of loyalty and past accomplishments, many of which we can truly view with pride, and the radical left points out that our existence as a Nation is founded on revolutionary action. The military establishment has played a large part in the forming of our traditions and a civilian government, aware of the abuses by Britain, also established firm principles which we now revere as tradition. Perhaps no other tradition is so vital to the security of our form of government than the separation of civil hegemony over the military. This tradition has been imperiled in recent years

---

[1]Robert F. Froehlke, remarks before the Subcommittee on Constitutional Rights of the Senate Committee on the Judiciary on March 2, 1971, Congressional Digest, op. cit. p. 244.

by the growth of the domestic intelligence operations of the U.S. Army, at times supported by similar activities of the Navy and the Air Force.

Moreover, questions should be raised as to whether civilian officials in the Department of Defense are permitted access to these personality files and surveillance - intelligence information.

However, these conclusions must not rule out completely all military intelligence operations. To prohibit unconditionally these activities, on the other hand, could be in the long run dentrimental to the national security of the United States. For example, if another crisis situation similar to the 1962 Cuban missile crisis precipitated, it might become necessary for military intelligence to be employed where the Armed Services would derive original jurisdiction and hence, become immediately involved. Yet, this conditional surveillance permit for the military would not be legitimate in cases where civilian responsibilities and capabilities were inadequate or insufficient.

from the rolls of the Armed Services (2) and Judiciary (2) Committees of each house. Finally, members are to be chosen by each house, respectively, and shall serve two-year terms, according to the Congressional calendar. No senator or representative shall serve consecutive two-year terms.

It shall be the expressed duty of the commission to supervise the separation of the CONUS intelligence and security-clearance data retrieval systems. This objective could be achieved by establishing separate headquarters, preferably in separate cities for these two information systems. Although physically separate headquarters would be expensive, since it would probably require two separate communications and information storage systems, the computerization of the data-retrieval networks should be better protected from abusive interagency or third party intrusion. Such a commission could satisfy both the "public's need for a regularized system of independent scrutiny and the Army's need for friendly critics capable of alerting it to the legal, moral, and political implications of its domestic intelligence program.

In the final analysis, this commission should evaluate the legitimacy of this aspect of military intelligence according to the degree the activity serves to help forewarn of impending civil disorder. Moreover, it should consider the extent to which military data collection inhibits

political participation and deprives dissenters of the rights of free speech and association, the right to petition the government for redress of grievances, and the right of privacy guaranteed by the First, Fourth, Fifth, and Ninth Amendments to the Constitution.

Department of Justice

Within the structure of the Federal Government, nowhere is intelligence information more vital to the sector's proper functioning than in the Department of Justice. Indeed, this area of government has given rise to a number of "data bank" files of instantly available information which can be rapidly transmitted, upon request, to authorized agencies and individuals throughout the country. In crime control, needless to say, the benefits of this information network have been widely acknowledged. Increasingly, in recent years, however, as technology has revamped intelligence and crime-prevention methods, the basic question at issue is the power of the Justice Department to monitor the activities of individuals when there is no probable cause to believe they have committed a crime.

Nowhere else in the federal establishment is the range of information collection and surveillance activities so varied as in the Department of Justice. Accordingly, there are no less than ten data banks within the Justice

Department. These include the Civil Disturbance System (Subject File-13,200 files; Incident File-14,000); the computerized Organized Crime Intelligence System (400,000 cards); Addict Files of the Bureau of Narcotics and Dangerous Drugs (70,000 files); the Defendant Statistical Program (2900 individuals arrested for drug violations, data in statistical form only); FBI Fingerprint and Criminal Identification Files (199 million cards) and the newly converted nationwide computerized system known as the National Crime Information Center; the known Professional Check Passers File (PROCHECK* 2000 tape storage records); Immigration and Naturalization Service-Alien Reports File (approximately 4.3 million per year); Master index (40 million persons admitted or excluded from this country since 1952 as well as sponsors of record); and the Non Immigrant Index (500,000 individuals admitted temporarily).[1]

Suffice it to say that this multitude of information is available only to the direct access of Justice Department officials. However, in all data banks, information is made available on a need-to-know basis to other Federal agencies and law enforcement bodies. These information-gathering storage and retrieval systems are outlined in the provisions of Part II, Title 28, U. S. C., Section 534, which states as

---

[1] "The Scope of Present Federal Activity," Congressional Digest, p. 228-230.

follows:

> (a) The Attorney General shall-
> (1) acquire, collect, classify, and preserve identification, criminal identification, crime, and other records; and
> (2) exchange these records with, and for the official use of, authorized officials of the federal government, the states, cities, and penal and other institutions.[1]

Electronic Eavesdropping and Wiretapping

Of paramount concern to the recent debate over the boundaries of privacy, the use of wiretapping and electronic eavesdropping devices has stirred the most controversy because there is posed an actual threat to the rights of free expression and freedom from unreasonable search guaranteed by the First and Fourth Amendments.

Until 1968, federal law on wiretapping was embodied in the Communications Act of 1934 (47 U. S. C. 605), which was a general statute aimed at protecting the privacy of citizens using the telephone or telegraph communications. The Act read in part:

> ". . .and no person not being authorized by the sender shall intercept any communication and

---

[1]William H. Rehnquist, testimony before the Committee on the Judiciary, Subcommittee on Constitutional Rights, March 9, 1971, 92nd Congress, 1st Session, Privacy and Federal Data Banks, excerpted from Congressional Digest, p. 246.

> divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person. . . ."[1]

The statute exempted such matters as routine work by communications workers and transmissions relating to ships in distress. Yet, few people are aware that another clause includes the following:

> ". . .and no person having received such intercepted communication. . .shall. . .use the same or any information therein contained for his benefit or for the benefit of another not entitled thereto.[2]

In 1941, the Justice Department ruled that a violation of Section 605 required both an interception and a divulgence outside the Federal Government; that ruling interpreted the Act as meaning that the Federal Government could wiretap as long as the contents of the communication were not divulged.[3] The FBI and the Internal Revenue Service, in particular, followed that interpretation. As a result, undisclosed wiretapping by the Federal Government was little publicized but relatively widespread because the Government chose to read "divulge" as meaning a public presentation.

After World War II, Congress in several years con-

---

[1]"Congress Again Considers Controversial Wiretap Issue," Congressional Quarterly Weekly Report, April 14, 1967, p. 592.

[2]Packard, op. cit., p. 311.

[3]Congressional Quarterly Weekly Report, op. cit.

sidered legislation aimed at restricting the amount of wiretapping but permitting use of wiretap evidence in national security prosecutions. No final passage was ever procured. During the Kennedy Administration, endorsement was made for proposals authorizing federal agencies to wiretap in cases of national security and organized crime. A somewhat more restrictive bill was sent to Congress providing those authorizations but limiting state wiretapping and outlawing all other private eavesdropping. Congress, however, once again failed to take action.

This pattern of inaction persisted until mid-1968. Despite President Johnson's call for a Right to Privacy Act in 1967, which would have limited all police and private wiretapping except federal law enforcement officers, who would be authorized by the President to wiretap or eavesdrop in national security cases, the legislative branch was reluctant to report any bill.[1]

Moreover, pre-1968 Supreme Court decisions were likewise indecisive. Several Court decisions were previously based upon physical intrusion of privacy. This, however, evades the real issue of eavesdropping on privacy created by technological achievements. Although many points of law still need to be settled, in the Katz vs. U. S. ruling in

---

[1] Ibid.

1967, the Supreme Court settled a major question, namely, whether a wiretap or eavesdrop constituted a "search or seizure" within the meaning of the Fourth Amendment. By a 7-1 vote, the Court held that a conversation was a "thing" that could be seized by a wiretap and that a wiretap was a "search and seizure" in the constitutional sense.[1] The effect of bringing electronic surveillance within the Fourth Amendment was not to ban it but to require police to obtain warrants before placing a tap or bug.

Furthermore, the Katz decision overruled two long-standing decisions: Olmstead vs. U. S. (1928), which was the first wiretap case brought before the Court and Goldman vs. U. S. (1942). In the former decision, the Court there ruled by a 5-4 vote that use of wiretap evidence in federal courts did not of itself violate the Fourth Amendment protection against unreasonable search or the Fifth guarantee against self-incrimination. The second case was premised on the fact that the Court found no objection to the use of evidence obtained by a detectaphone placed against the wall of the defendant's room. The Court reasoned that since there had been no physical trespass, there was no violation of the Fourth Amendment. That theory was abandoned in Katz.[2]

---

[1]Adam Carlyle Breckenridge, The Right to Privacy, p. 22.

[2]Packard, op. cit., p. 316.

consensual bugging (bribe recording) by all government agencies in 1969 and 504 requests for 1970.[1]

National Security Eavesdropping

Throughout the many years of prolonged debate on the issue of privacy-invading surveillance, there has been substantial unanimity that some kind of eavesdropping should be permitted in national security cases. In jurisprudential terms, the Supreme Court has never addressed the question of national security exceptions to requirements for court warrants in any and all searches and seizures. The Court, most probably, would never deny the President the right to act without a warrant, if no time existed to get one. But what if there is time?

The Omnibus Crime Bill institutionalizes the President's powers by saying that the Act shall not:

> . . .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 to protect national security information against foreign intelligence activities. . .(Or) 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 and existence of the Government.[2]

---

[1] Ibid.

[2] U. S. 90th Congress, 2nd Session. PL90-351. Omnibus Crime Control and Safe Streets Act, Title III, Section 2511 (3). June 19, 1968.

> . . . .We have not argued against the need to get authorization for such a wiretap. Instead, we maintain that in national security cases the authorization required by the Constitution is that of the President of the United States, acting through his Attorney General, rather than that of a local magistrate.[1]

The reasons for this authority pertain to the sensitivity of the information involved, and the unique position of the President to evaluate information submitted by several independent agencies within the intelligence community, especially compared to any magistrate.[2]

Nevertheless, in an equivocally emphatic manner, certain reservations to this Justice Department assertion must be set forth. First, the power to engage in warrantless electronic surveillance and wiretapping in situations involving "national security," represents a danger to the free exercise of political freedom and the protection guaranteed under the Fourth Amendment. The forty-eight hour emergency tap exception in domestic or internal security, and the warrantless surveillance of foreign subversion has been dramatically extended by the Attorney General into a carte blanche to engage in electronic surveillance of Americans whenever he deems it important from a national security

---

[1] John N. Mitchell. "Wiretapping and Our National Security." Congressional Record, U. S. 92nd Congress, 1st Session. S9753-S9754. June 23, 1971.

[2] Ibid.

standpoint. Such action removes the constitutional check and balance between the judicial and the executive branches.

Secondly, this is not to dispute the Attorney General's premise:

> Certainly, in this period of intensified organized crime activity, we cannot afford to shun a method that is both effective and compatible with constitutional law.[1]

However, Assistant Attorney General William H. Rehnquist's testimony to the Senate Subcommittee on Constitutional Rights is more perplexing:

> But it will come as no surprise, I am sure, for me to state that the Department will vigorously oppose any legislation which, whether by opening the door to unnecessary and unmanageable judicial supervision of such activities or otherwise, would effectively impair this extraordinary important function of the Federal Government.[2]

Yet, a distinction should be made between aliens and citizens and between emergency and non-emergency situations. No executive agency should have the right to eavesdrop electronically upon any citizen except under a court warrant, or in a national emergency. The power which is claimed for the

---

[1] Congressional Quarterly Weekly Report, op. cit. p. 430.

[2] Rehnquist, op. cit., p. 248.

←——Attorney General, as a confidant of the President, is purely discretionary and contrary to the letter and spirit of Title III of the 1968 Act. As previously mentioned, neither the Congress nor the Supreme Court has defined precisely the national security case. PL 90-351 did, on the other hand, specify authorization procedure for seeking court warrant in national security cases and limited warrantless taps to emergency tap to last no more than forty-eight hours. The locus of discretion is not truly at issue because there are legalities to rule on and such legalities have always resided in the judicial branch. Moreover, the primary thrust of the Fourth Amendment has been to protect privacy by placing a judicial officer between the law enforcement officer and the individual. Clearly, the President nor the Attorney General fills this specification. Therefore, this authority to grant permission, indeed a legal warrant, should in national security cases be decided by a three-member judicial review board. These judges should be treated with the same accord as any member of the eleven U. S. Court of Appeals panel, but should be distinct from all other tribunals, and have no other duties except to grant or deny a warrant for electronic eavesdropping or wiretapping authority in national security cases. See 39-a, 39-b, & 39-c (Addendum)

This court of warrants shall consider no other cases except those pertaining to these surveillance activities so

This court of national security warrants will not need to be concerned with requests for wiretapping or electronic surveillance in cases where national security considerations are not at issue. Indeed, these cases are already provided for judicial consideration in sections of Title III of the 1968 Omnibus Crime Control and Safe Streets Act which specifies that warrants for cases where national security is not at stake necessitate court orders prior to any surveillance.

However, the court of warrants, heretofore described, will have a limited jurisdiction; that is to say, it will rule on the legality or illegality of requests for wiretapping and electronic eavesdropping in national security cases only. Previously, in these cases, the Attorney General of the United States had claimed discretionary power to determine when the national security was endangered, and when therefore, such surveillance methods should be employed. Moreover, these three judges would decide these requests for national security wiretapping in a fashion similar to a grand jury whereby they would determine whether the government's evidence indicated that indeed, the national security was threatened.

Nevertheless, this stringent limitation in the scope of activity of this court of warrants will not necessarily imply either an overworked or under-employed court. Instead, this circumscription in authority serves as an internal security check because these judges will be made privy to

information vital to the national security. Therefore, they should not be influenced by any other considerations while serving on this particular and highly unique court. Furthermore, this tripartite panel, in all likelihood, will not be any more overworked according to present statistical evidemce provided by the Department of Justice, which places the number of national security wiretaps well under seventy-five in any one year (for example, on March 17, 1967 then-Attorney General Ramsey Clark told the House Judiciary Committee that he had about 38 national security wiretaps. Similarly, on February 14, 1970, Mr. J. Edgar Hoover testified that he had 36 telephone surveillances and two microphone installations in such FBI security cases).[1] From the startling sameness of these estimates, one might conclude that the national security wiretaps are long-standing installations associated with foreign embassies and related installations and residences. Moreover, it is equally unlikely, that this court would become overburdened by a multitude of cases any greater than the Supreme Court of the United States which seems to survive its busy session each year. In addition, this court is only ruling on requests for national security wiretaps and it should leave the handing down of monumental judicial decisions with judicial philosophy to the Supreme Court. Furthermore, fear of an underemployed court of warrants should also be

---

[1] "Privacy of Communications in American Life: Eavesdropping and Mail Covers," Federation of American Scientists Newsletter, February, 1971, p. 6.

clarified. Present statistics indicate that the court would have sufficient business with which to be concerned. However, the number of cases should not be the most important criteria used to measure the utility of this court. Instead, the need for the court of warrants should be evaluated in terms of whether it will serve the interests of those agencies dedicated to protecting the national security, and at the same time, the individuals right to privacy.

as not to interfere with the appeals process of the Federal Judiciary. Furthermore, these three judges should be appointed by the President with the advice and consent of the United States Senate, similar to all other nominations. Finally, to avoid any buildup of bureaucratic anomalies, this tripartite judicial panel should be rotated every two years. Wiretap authorizations should be limited to 45 days, renewable for extensions of 20 days. This panel should be instructed to make sure that all material obtained pursuant to court authorized surveillance would be required to be destroyed unless actually introduced as evidence in a criminal matter. See 40-a (Addendum)

Moreover, the Federal Communications Commission should wake up to its responsibility for policing the nation's telephone lines to ensure privacy including locking all terminal and feeder boxes.[1] In particular, as in the surveillance operations of the Army, public officials must be exempt from any eavesdropping attempts and repeat of the alleged Boggs wiretap by the FBI should be thoroughly investigated, and if it did occur, prohibited.[2]

These measures are not designed to hinder crime-prevention and crime-protection efforts. The large number of arrests, particularly in the field of organized crime and

---

[1] Packard, op. cit., p. 315.

[2] "FBI Controversy: Wiretapping Charge and Denial." Congressional Quarterly Weekly, April 9, 1971, p. 793.

However, a period of sixty days would be recommended at the present time, for destroying all material not used in criminal prosecution which was obtained through surveillance activities. The duration of this period, however, should be thoroughly investigated and studied in view of the present day problem of a slow, lengthy judicial process of case handling.

VI. BIBLIOGRAPHY

Bibliographies Prepared by Other Writers

Miller, Arthur R. The Assault on Privacy: Computers, Data Banks, and Dossiers. Ann Arbor, Michigan, University of Michigan Press, cop. 1971.

Westin, Alan F. Privacy and Freedom. 1st ed. New York, Antheneum, cop. 1967.

Books and Pamphlets

Breckenridge, Adam Carlyle. The Right to Privacy. Lincoln, University of Nebraska Press, cop. 1970.

Chapman, John W., and Pennock, J. Roland. eds. Privacy: NOMOS XIII. New York, Atherton Press, cop. 1971. (Series of essays providing various perspectives on privacy issue).

Donner, Frank. " The Theory and Practice of American Political Intelligence." (Reprint from The New York Review of Books, cop. 1971).

Dulles, Allen. The Craft of Intelligence. New York, Harper and Row, Inc., cop. 1963.

Lister, Charles. " Statement on behalf of the American Civil Liberties Union on Privacy and Government Data Banks before Subcommittee on Constitutional Rights, Committee on the Judiciary." (Reprint from Congressional Record, October 7, 1971).

Long, Edward V. The Intruders. New York, Frederick A. Praeger, cop. 1971.

Miller, Arthur R. The Assault on Privacy: Computers, Data Banks, and Dossiers. Ann Arbor, University of Michigan, cop. 1971.
(Very current analysis of computer revolution).

Neuborne, Burt. " Testimony on behalf of American Civil Liberties Union before the Senate Subcommittee on Constitutional Rights." (Reprint from Congressional Record, February 23, 1971).

Packard, Vance. The Naked Society. New York, David McKay Company, Inc., cop. 1964.
(Although dated, this book was helpful in tracing surveillance developments in the federal agencies in order to gain starting point for further research).

Rosenberg, Jerry M. The Death of Privacy. New York, Random House, cop. 1969.

Slough, M.C. Privacy, Freedom, and Responsibility. Springfield, Charles C. Thomas Company, cop. 1969.
(This book was written with a different perspective on the range of computer - undercover information gathering activities. This analysis depicted certain beneficial aspects of the surveillance and computer revolution).

Westin, Alan F. Privacy and Freedom. 1st ed. New York, Atheneum, cop. 1967.

Periodicals and Newspapers

"The Assault on Privacy." Newsweek: : 15-20. July 27, 1970.

Batten, James K. "Sam Ervin and the Privacy Invaders." The New Republic. : 19-23. May 8, 1971.

Beany, William M. "The Right to Privacy and American Law." Law and Contemporary Problems, 31:253 - 271. Spring 1966.

Beecher, William. "Laird Picks Panel to Curb Army Spying on Civilians." New York Times, February 19, 1971.

Bloustein, Edward J. "Privacy, Tort Law, and the Constitution: Is Warren and Brandeis 'Tort Petty' and Unconstitutional As Well?" Texas Law Review, 46:611-630. April, 1968.

Bradley, Roger. "Warrantless Welfare Searches Violate Recipient's Constitutional Rights." Syracuse Law Review, 19:95-101, Fall, 1967.

"Cellar Says Wiretapping Policy May Be Leading to Police State." New York Times, April 26, 1971.

Clark, Ramsey. "Demeaning Human Dignity." Saturday Review, :29-32; April 17, 1971.

Comment: "Privacy, Defamation, and the First Amendment: The Implications of Time, Inc. v. Hill." Columbia Law Review, 67:926-952. 1964.

"Controversy over Federal Collection of Data on Private Individuals." Congressional Digest, 50:225-256. October, 1971.

Countryman, Vern. "Computers and Dossiers." The Nation, 213:134-143. August 30, 1971.

Dunn, E.S. "The Idea of a National Data Center and the Issue of Personal Privacy." American Statistician, 21:21-27. February, 1967.

Ervin, Sam J. "The Freedom to Speak." New York Times, October 3, 1971.

Graham, Fred P. "White House View of Wiretap Right Denied on Appeal." New York Times. April 9, 1971.

_____. "Mitchell Upholds Wiretap of 'Dangerous Radicals.' " New York Times, June 12, 1971.

Halloran, Richard. "Army Spied on 18,000 Civilians in 2-Year Operations." New York Times, January 18, 1971.

_____. "Senators Hear of Threat of a Dossier Dictatorship." New York Times, February 24, 1971.

_____. "Senators Told Johnson Officials Began Army Checks on Civilians." New York Times, March 3, 1971.

_____. "Richardson Says Data Banks Must Be Controlled." New York Times, March 16, 1971.

_____. "Justice Aide Says Government Has the Right to Put a Senator Under Surveillance." New York Times, March 18, 1971.

Herbers, John. "Senator Ervin Thinks the Constitution Should Be Taken Like Mountain Whiskey - Undiluted and Untaxed." New York Times Magazine Section, November 15, 1970.

"The Invisible Intruders." Saturday Review, :19-20. January 30, 1971.

Karabian, Walter. "Case against Wiretapping." Pacific Law Journal, 1:133-145. January, 1970.

Karst, Kenneth L. "The Files: Legal Controls over the Privacy and Accessibility of Stored Personal Data." Law and Contemporary Problems, 31:342-376. Spring, 1966.

King, Donald B. "Electronic Surveillance and Constitutional Rights: Some Recent Developments." The George Washington Law Review, 33:240-270. October, 1964.

Lewin, Nathan. "Privacy and the Third-Party Bug." The New Republic, :12-17. April 17, 1971.

Michael, Donald N. "Speculations on the Relations of the Computer to Individual Freedom and the Right to Privacy." The George Washington Law Review, 33:270-287. October, 1964.

Miller, Arthur R. "The National Data Center and Personal Privacy." Atlantic, 220:53-57. November, 1967.

Notes, "Privacy and Efficient Government: Proposals for a National Data Center." Harvard Law Review, 82:400-418. December, 1968.

Owen, Stephen T. "Eavesdropping at the Government's Discretion - First Amendment Implications of the National Security Eavesdropping Power." Cornell Law Review, 56: 161-170. November, 1970.

"Privacy of Communications in American Life: Eavesdropping and Mail Covers." Federation of American Scientists Newsletter, Number 24. February, 1971.

Prosser, William L. "privacy." California Law Review, 48:383-423. August, 1960.

Pyle, Christopher H. "CONUS Intelligence: The Army Watches Civilian Politics." The Washington Monthly, 1:4-16. January, 1970.
(This article as well as the one following were two of the best primary sources of military surveillance.)

_____. "CONUS Revisited: The Army Covers Up." The Washington Monthly, 2:49-58. July, 1970.

Ripley, Anthony. "Big Man on the Cover: Police Undercover Agent." New York Times, March 29, 1971.

Rogers, William P. "The Case for Wiretapping." Yale Journal Journal, 63:792-798. April, 1954.

Schmidt, Dana Adams. "Ervin Announces Nixon Revival of Subversives Board." New York Times, October 6, 1971.

Schrag, Peter. "Dossier Dictatorship." Saturday Review. :24-25. April 17, 1971.

Schwartz, Herman. "The Legitimation of Electronic Eavesdropping: The Politics of Law and Order." Michigan Law Review, 67: 455 - 511. January, 1969.

"Senators Hear of a Threat of a Dossier Dictatorship." New York Times, February 24, 1971.

Sherrill, Robert. "The Assault on Privacy." New York Times Book Review, March 14, 1971.

"A Shift Reported in Surveillance." New York Times, February 25, 1971.

Smith, Robert M. "F.B.I. Said to Bug a House Member." New York Times, April 16, 1971.

_____. "Supreme Court to Weigh Mitchell's Wiretap View." New York Times, June 22, 1971.

_____. "F.B.I. Is Said to Have Cut Direct Liason with C.I.A. New York Times, October 10, 1971.

Sovern, Michael I. "Mitchell and the Wiretap." New York Times, September 28, 1971.

"Who Dug for Dirt on Earth Day?" Newsweek. :23-24. April 26, 1971.

Wicker, Tom. "Preventive Government." New York Times, July 1, 1971.

Government Publications

Congressional Quarterly Weekly Report. Volume 25: Numbers 15,29. Congressional Quarterly, Inc., Washington, cop. 1968.

Congressional Quarterly Weekly Report. Volume 26: Number 29. Washington, Congressional Quarterly, Inc., cop. 1968.

Congressional Quarterly Weekly Report. Volume 27: Number 28. Washington, Congressional Quarterly, Inc., cop. 1969.

Congressional Quarterly Weekly Report. Volume 29: Numbers 8,9, 10, 11, 15, 17, 32. Washington, Congressional Quarterly, Inc., cop. 1971.

Congressional Record. U.S. 92nd Congress, 1st Session. 117: S9752-S9754; S9870-9880. Washington, Government Printing Office, June 23, 1971.
(These inserts are made by Senator Ervin and Senator Dole: They deal with wiretapping in National Security Cases especially an address by Attorney General Mitchell.)

U. S. 87th Congress, 2nd Session. Senate Committee on the Judiciary. Wiretapping and Eavesdropping. Summary - Report of Hearings 1958-1961. Washington, Government Printing Office, 1962.

U. S. 90th Congress, 2nd Session. House Committee on Government Operations. Privacy and the National Data Bank. House Report No. 1842. Washington, Government Printing, 1968.

U. S. 91st Congress, 1st Session. Senate Committee on the Judiciary Subcommittee on Constitutional Rights. Privacy, The Census and Federal Questionnaires. Hearings ... on S. 1791. Washington, Government Printing Office, 1969.

U. S. 92nd Congress, 1st Session. U.S. House of Representatives. H. R. 9527. Washington, Government Printing Office, June 30, 1971.

U. S. 92nd Congress, 1st Session. U.S. Senate. S. 1438. Washington, Government Printing Office, April 1. 1971.

U.S. 90th Congress, 2nd Session. PL 90-351. Omnibus Crime Control and Safe Streets Act. Washington, Government Printing Office, June 19, 1969.

U. S. 92nd Congress, 1st Session. Senate Committee on the Judiciary, Subcommittee on Constitutional Rights. Hearings on Privacy and Federal Data Banks. Washington, Government Printing Office, March 9, 1971 .

Judicial Decisions

Greene vs. McElroy, 360 U. S. 474 (1959).

Katz vs. U. S. , 389 U. S. 347 (1967).

Olmstead vs. U. S. , 277 U. S. 438 (1928).

Interviews

Confidential Interview A., Princeton, N.J., November 3, 1971.

CONGRESSIONAL RECORD REFERENCES
SENATOR ERVIN'S SPEECHES
ON
PRIVACY, FEDERAL EMPLOYEES, COMPUTERS AND DATA BANKS

DATE	VOLUME	NUMBER	DESCRIPTION
Federal Employees and Privacy			
7/18/66	112	114	"New Invasions of the Privacy of Federal Employees" First Federal employee speech before the employee privacy bill was introduced. Documents some problem areas.
8/9/66	112	130	Introduction of Federal Employee Bill (S. 3779). A Bill to Protect the Constitutional Rights of Government employees and to prevent unwarranted invasions of their privacy. Describes specific privacy invasions leading to the bill.
2/21/67	113	26	"Protection of Constitutional Rights of Government Employees and to Prevent Unwarranted Invasions of Their Privacy - Protection of the Military". Introduction of S. 1036, military bond bill, and reintroduction of the Employee Privacy Bill as S. 1035.
4/25/67	113	63	Speech by Senator Ervin on "The Right of Privacy" at the Institute of Governmental Affairs, the University of Wisconsin. Discusses concepts of employment, and privacy, and the Constitution. Government employees being forced to buy savings bonds, subjected to extensive questioning concerning their personal lives and beliefs, etc.
10/5/67	113	159	"S. 1035, An Act to Protect the Constitutional Rights of Employees of the Executive Branch of Government and to Prevent Unwarranted Governmental Invasions of Their Privacy." (Contains a number of articles and editorials commenting on Senate passage of S. 1035 and the controversy over CIA-NSA-FBI coverage by bill.
5/1/68	114	73	"S. 1035 and Employee Right to Privacy - Congress' Last Clear Chance". (Contains various articles and editorials on the bill; discusses progress.)
6/13/68	114	101	"S. 1035 - Employee Privacy and 20th Century Witchcraft: The Lie Detector". Prepared address by Senator Ervin on November 16, 1967, on abuses of polygraphs.

6/17/68	114	103	"S. 1035 and Employee Privacy" - Address before the National Association of Internal Revenue Employees. (Speech by George B. Autry)
7/2/68	114	114	"Employee Rights and Invasions of Privacy - S.1035" Before Congressman Henderson's House Post Office and Civil Service Subcommittee on Manpower and Civil Service. (Contains CIA-NSA-FBI memoranda and lie detector)
1/31/69	114	21	"S.782 - Introduction of Bill for Protection of Constitutional Rights of Government Employees and to Prevent Unwarranted Invasions of their Privacy." (Reintroduction of employee privacy bill. Contains correspondence between Chairman Macy of the Civil Service Commission and Senator Ervin)
6/30/69	115	108	"Privacy, the Census and Federal Questionnaires" (Mentions hearing held 7/1/69 which studied census, privacy and federal questionnaires. Also mentioned S. 1791 - a proposal introduced for discussion purposes during hearings. Bill represents an attempt to set reasonable standards for the wholesale statistical data collecting conducted by the Census Bureau and other agencies. Has Ervin and Miller hearing statements.
5/1/69	116	69	"Letter Opening and the Bill of Rights: Petty Monarchists in Executive Branch" (Contains regulation authorizing Post Office Department to open first-class letter mail believed to contain dutiable or prohibitive matter.)
4/1/71	117	47	"S. 1438 - Introduction of Bill for Protection of Constitutional Rights of Government Employees and to Prevent Unwarranted Invasions of Their Privacy."
5/11/71	117	68	"Statement by Senator Ervin before House Subcommittee on Privacy on S. 1438" (Discusses Sensitivity Training)
6/24/71	117	98	"S. 2156 - A Bill to Protect Against Invasion of Privacy by Prohibiting Lie Detectors" (Discusses use of Polygraph in government agencies and various states)

COMPUTERS AND DATA BANKS

3/8/67	113	37	"The Computer and Individual Privacy", speech by Senator Ervin before the American Management Association New York City, March 6, 1967

11/10/69	115	184	"Computers and Individual Privacy", Senator Ervin's speech before the Wharton School of Finance. Discusses computer abuses and need for independent regulatory agency and other remedies to control computers and protect rights. (Also cites Secret Service data bank.)
12/15/69	115	208	"Secret Service Guidelines: Protection of the President and Protection of Individual Rights." (Contains bills introduced in Great Britain and Canada seeking to regulate computer invasions of privacy. Also contains correspondence between Senator Ervin and Treasury regarding the Secret Service guidelines issued to federal employees to encourage reporting on private citizens.
2/3/70	116	13	"Computers, Data Banks and Constitutional Rights" (Contains Washington Monthly article by Chris Pyle on CONUS Intelligence and Senator Ervin's correspondence with Army on Army surveillance and computer systems. First speech by Senator Ervin on this subject
3/2/70	116	30	"Privacy and Army Data Banks: Constitutional Rights and Military Wrongs". (Includes Subcommittee's correspondence with Army about amount and kinds of personal information they have on people)
6/22/70	116	103	"Industry Call to Action on Privacy and Computers" Contains speech of Robert Henderson, Honeywell Corp., giving insight on the privacy problem and computers.
7/29/70	116	129	"Army Maintains Deterrent Power Over Civilian Rights" Releases correspondence between Senator Ervin and Department of Army regarding disclosure of Army's surveillance of private citizens; contains letter to Attorney General, news articles and editorials.
9/8/70	116	155	"Announcement of Hearings: Federal Data Banks and the Bill of Rights" (Describes scope of the hearings scheduled for October 1970, but held in February and March 1971; constitutional issues, examples of government data banks; news articles.
12/29/70	116	202	"More on Army Political Surveillance" Contains news articles on John O'Brien's allegations against Army.
12/16/70	116	202	"Army Surveillance of Civilians" Discusses disclosures by former Army agent John O'Brien of Army's surveillance of private citizens.
2/8/71	117	13	"Announcement of Hearings on Computers, Data Banks and the Bill of Rights." (Describes Feb-March 1971 hearings; witnesses, issues; more examples of government computer systems and data banks for intelligence purposes.)

CONGRESSIONAL RECORD References: Prepared Statements of some Witnesses, Submitted during Senate Constitutional Rights Subcommittee Hearings on Privacy, Computers, and Data Banks; placed in Record by Senator Ervin.

DATE	VOLUME	NUMBER	PAGE	DESCRIPTION
5/13/71	117	70	S6861	Statement of Christopher Pyle, lawyer and former U.S. Army Captain in Army Intelligence; history of CONUS Intelligence program for recording civilian activities; other government gathering and storage of data for intelligence purposes.
5/18/71	117	73	S2701	Statement of Ralph M. Stein, former analyst with U.S. Army Intelligence. Describes operation of Army program; analysis and use of dossiers; computerizing and micro-filming of data.
5/19/71	117	73	S7313	Statements of John M. O'Brien, Edward Sohier, and Laurence F. Lane, former Army intelligence agents. (Description of their data-gathering activities in Army surveillance program.)
5/26/71	117	79	S7838	Statement of Robert F. Froehlke, Assistant Secretary of Defense for Administration. Describes history of Army surveillance for civil disturbance purposes; theory, legality of program; cites statistics for many other military data banks and computerized information systems.
6/14/71	117	90	S8947	Statement of Alexander Polikoff, counsel for the American Civil Liberties Union in its suit against the Defense Department concerning Army domestic surveillance. Describes findings of fact on the Army program as introduced into Federal District Court in Chicago.
6/29/71	117	100	S10224	Statement of William H. Rehnquist, Assistant Attorney General. Discusses the constitutionality and legality of Army surveillance as well as Justice Department and other government data-gathering.
7/28/71	117	119	S12390	Statement of Elliot L. Richardson, Secretary of Health, Education, and Welfare, on data programs of his department, on need for controls, and on use of social security number as a universal identifier.

*Hearings conducted before Senate Constitutional Rights Subcommittee on February 23, 24, 25; March 2, 3, 4, 9, 10, 11, 15 and 17, 1971.

Vinson, Eric H.
Conference on the
Boundaries of Privacy
Woodrow Wilson School of
Public & International Affairs
December 29, 1971

THE SCOPE OF SURVEILLANCE ACTIVITY