Exhibit 1

ant to civilan rule, they provided that the President should be the Commander in Chief. To assure that the people always controlled the Armed Forces, Congress alone was empowered to make "rules for the Government and regulation of the land and naval forces."

Mr. President, I recall these basic constitutional principles today because they will be devastated beyond repair if the collection of unwarranted files and development of data banks for survillance purposes is not halted, and if some all-out controls are not set on the activities of those who control the computers and guard the files in our great information systems.

The Army political surveillance program is, however, only one of many data systems in the hands of an ever-curious executive branch.

In the total recall of vast computer systems rests a potential for control and intimidation which is alien to our form of government and foreign to a society of free men. Regardless of the purpose, regardless of the confidentiality, regardless of the harm to any one individual, the very existence of Government files on how people exercise first amendment rights, how they think, speak, assemble, and act in lawful pursuits, is a form of official psychological coercion to keep silent, and to refrain from acting. Because it is more insidious, it is a coercion far more effective and intimidating than any tyranny experienced by the Founding Fathers.

It is a violation of the first amendment rights of our entire Nation.

Mr. President, I think we have serious cause for concern.

I ask unanimous consent that the Washington Monthly article by Mr. Pyle and my letter to Secretary Resor be printed in the RECORD following my remarks, together with articles from the New York Times of January 16, 1970, the Washington Star of January 15, 1970, the Fresno Bee of January 28, 1970, and the New York Post of January 27, 1970.

There being no objection, the items were ordered to be printed in the RECORD, as follows:

JANUARY 22, 1970.

Hon. STANLEY R. RESOR,
Secretary of the Army,
Washington, D.C.

DEAR MR. SECRETARY: In connection with our study of computers, privacy and constitutional rights, the Constitutional Rights Subcommittee is conducting a survey of the development and maintenance of data banks by Federal departments and agencies.

One of our purposes is to determine whether or not such data systems are being developed in accordance with constitutional standards of privacy and due process of law for the individual citizens involved. Another purpose is to help Congress ascertain the need for comprehensive legislation to govern all computerized data banks on individuals.

Our attention has been particularly directed to reports of the development and expansion of data banks at Fort Holabird, containing information on the personalities, on the political, economic, and social beliefs and on the lawful community activities of American citizens.

To assist the Subcommittee in its study, we should appreciate your explaining for us: (1) the present situation concerning collection and storage of Army intelligence and other investigative data on private individuals, particularly at the Investigative Records Repository, but also at other data centers operated by the Army; and (2) future plans for expanding and further computerizing the present system.

Specifically, we should receive responses to the following questions:

1. Under what statutory and administrative authority was the investigative Records Repository established, and for what purpose? What is the relationship of this activity to the responsibilities of the Armed Forces? Please supply copies of pertinent statutes, regulations and memoranda.

2. Is all military intelligence data on individuals filed in this center? Is it computerized?

3. How many subject individuals are presently recorded in the system at the Records Center?

4. What categories of information about individuals are contained in this data bank? Are there any published or unpublished regulations or instructions governing the type of information appropriate for the files, how it is to be gathered, and how its accuray is to be determined? If so, please supply copies.

5. Are there plans to expand the scope of these files in number and subject matter? If so, how would this specifically alter the existing data system?

6. Is the subject individual, or his representative, allowed to review the data on record about him, to supplement his file and to explain or rebut material he considers inaccurate?

7. What provisions are made for deleting material found to be inaccurate or inappropriate, either spontaneously by the Army or on motion of the individual concerned?

8. What limitations are placed on access to the file or to information contained in it? What security procedures or devices are employed to prevent unauthorized access to the data file or improper use of the information? Who specifically has access to this data? For what reasons and on what authority is access granted?

9. What other agencies have access to these files? For what purposes? Under what restrictions?

10. Is a record maintained of the details of inspection or use of the file or data on an individual?

11. How is this information collected and by whom? Is it collected by investigators or from third parties? Is it solicited from the individual himself, or is it collected from other records?

12. Do you have published or unpublished regulations or guidelines concerning use and availability of these files? If so, please supply copies.

13. Do you have published or unpublished regulations or guidelines concerning the gathering, screening and accuracy of data in these files? If so, please supply copies.

14. To what extent are these files computerized? What are your plans for computerizing further?

15. The Subcommittee is interested in learning the truth about current reports that the Army plans to connect its intelligence teletype reporting system to a computerized data bank at the Investigative Record Repository. If so, what are your plans for safeguarding the accuracy of the data collected and its relevance to the area of your responsibility?

16. What other data banks are maintained or supported by the Department of the Army on private citizens? To the extent possible, please supply for each of these the information requested for the Fort Holabird data banks.

Enclosed is a *Congressional Record* excerpt describing the scope of the Subcommittee's interest in the government's use of data banks on individuals.

Your assistance in our study is deeply appreciated.

With all kind wishes, I am,

Sincerely yours,

SAM J. ERVIN, Jr.,
Chairman, U.S. Senate, Committee on the Judiciary, Subcommittee on Constitutional Rights.

[From the Washington Monthly, January 1970]

CONUS INTELLIGENCE: THE ARMY WATCHES CIVILIAN POLITICS

(By Christopher H. Pyle)

(NOTE.—Christopher H. Pyle, a Ph.D. candidate at Columbia University, has recently completed two years service as a captain in Army Intelligence. The information in this article comes from briefings he received at the headquarters of the U.S. Army Intelligence Command, and from the observations of friends and acquaintances who served in intelligence units throughout the United States and Europe. None of it carries a security classification of any kind.)

For the past four years, the U.S. Army has been closely watching civilian political activity within the United States. Nearly 1,000 plainclothes investigators, working out of some 300 offices from coast to coast, keep track of political protests of all kinds—from Klan rallies in North Carolina to anti-war speeches at Harvard. This aspect of their duties is unknown to most Americans. They know these soldier-agents, if at all, only as personable young men whose principal function is to conduct background investigations of persons being considered for security clearances.

When this program began in the summer of 1965, its purpose was to provide early warning of civil disorders which the Army might be called upon to quell. In the summer of 1967, however, its scope widened to include the political beliefs and actions of individuals and organizations active in the civil rights, white supremacy, black power, and antiwar movements. Today, the Army maintains files on the membership, ideology, programs, and practices of virtually every activist political group in the country. These include not only such violence-prone organizations as the Minutemen and the Revolutionary Action Movement (RAM), but such nonviolent groups as the Southern Christion Leadership Conference, Clergy and Laymen United Against the War in Vietnam, the American Civil Liberties Union, Women Strike for Peace, and the National Association for the Advancement of Colored People.

The Army obtains most of its information about protest politics from the files of municipal and state police departments and of the FBI. In addition, its agents subscribe to hundreds of local and campus newspapers, monitor police and FBI radio broadcasts, and, on occasion, conduct their own undercover operations. Military undercover agents have posed as press photographers covering anti-war demonstrations, as students on college campuses, and as "residents" of Resurrection City. They have even recruited civilians into their service—sometimes for pay but more often through appeals to patriotism. For example, when Columbus University gave its students the option of closing their academic records to routine inspection by government investigators, the 108th Military Intelligence Group in Manhattan quietly persuaded an employee of the Registrar's Office to disclose information from the closed files on the sly.

Typical of the hundreds of reports filed by Army agents each month are the following, taken from the unclassified intelligence summary for the week of March 18, 1968:

"Philadelphia, Pa.: A. The Philadelphia Chapter of the Women's Strike for Peace sponsored an anti-draft meeting at the First

Unitarian Church which attracted an audience of about 200 persons. Conrad Lynn, an author of draft evasion literature, replaced Yale Chaplain William Sloane Coffin as the principal speaker at the meeting. Following a question and answer period, Robert Edenbaum of the Central Committee for Conscientious Objectors stated that many Philadelphia lawyers were accepting draft evasion cases. The meeting ended without incident.

"B. Rev. Albert Cleage, Jr., the founder of the Black Christian Nationalist Movement in Detroit, spoke an an estimated 100 persons at the Emmanuel Methodist Church. Cleage spoke on the topic of black unity and the problems of the ghetto. The meeting was peaceful and police reported no incidents.

"Chicago, Ill: Approximately 300 members of Veterans for Peace and Women for Peace held a peaceful demonstration at the Museum of Science and Industry protesting an exhibit by the U.S. Army. Several demonstrators entered the building in spite of warnings by museum officials and 6 were arrested on charges of disorderly conduct, resisting arrest and criminal trespassing. Five of those arrested were juveniles."

To assure prompt communication of these reports, the Army distributes them over a nationwide wire service. Completed in the fall of 1967, this teletype network gives every major troop command in the United States daily and weekly reports on virtually all political protests occurring anywhere in the nation.

The Army also periodically publishes an eight-by-ten-inch, glossy-cover paperback booklet known within intelligence circles as the "blacklist." The "blacklist" is an encyclopedia of profiles of people and organizations who in the opinion of the Intelligence Command officials who compile it, might "cause trouble for the Army." Thus it is similar to less formal lists which the Department of Health, Education, and Welfare has maintained to exclude politically unpopular scientists from research contracts and consultant work.

Sometime in the near future the Army will link its teletype reporting system to a computerized data bank. This computer, to be installed at the Investigative Records Repository at Fort Holabird in Baltimore, eventually will be able to produce instant printouts of information in 96 separate categories. The plan is to feed it both "incident reports" and "personality reports." The incident reports will relate to the Army's role in domestic disturbances and will describe such occurrences as bombings, mass violence, and arms thefts. The personality reports—to be extracted from the incident reports—will be used to supplement the Army's seven million individual security-clearance dossiers and to generate new files on the political activities of civilians wholly unassociated with the military.

In this respect, the Army's data bank promises to be unique. Unlike similar computers now in use at the FBI's National Crime Information Center in Washington and New York State's Identification and Intelligence System in Albany, it will not be restricted to the storage of case histories of persons arrested for (or convicted of) crimes. Rather it will specialize in files devoted exclusively to descriptions of the lawful political activity of civilians. Thus an IBM card prepared many months ago for the future computer file of Arlo Tatum, executive secretary of the Central Committee of Conscientious Objectors, contains a single notation—that Mr. Tatum once delivered a speech at the University of Oklahoma on the legal rights of conscientious objectors.

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 Central Intelligence Agency, the National Security Agency, the Civil Service Commission, the Atomic Energy Commission, the Defense Intelligence Agency, 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.

Headquarters for the collection and coordination of this information is a wire-mesh "cage" located inside a gray metal warehouse at Fort Holabird. The official designation of the office is "CONUS Intelligence Branch, Operations IV, U.S. Army Intelligence Command." CONUS is the Army's acronym for Continental United States. Direction of this program is in the hands of Major General William H. Blakefield, head of the U.S. Army Intelligence Command at Fort Holabird. Established in 1965, the Command coordinates the work of a number of counter-intelligence "groups" formerly assigned to the G–2 offices of the major stateside Armys, Accordingly, its principal function is not to collect intelligence but to protect the Army from espionage, sabotage, and subversion. Its main job is to investigate persons being considered for security clearances and to inspect military installations for adequate physical, wire-communications, and document security.

CONUS Intelligence Branch, also known as "Ops Four," is commanded by a major and run by a civilian. They supervise the work of about a dozen persons, who work in shifts around the clock. Most are WAC typists who operate the teletype consoles that link the Intelligence Command to the Pentagon and to intelligence units around the country. It is here that reports from agents are received, sorted, and retransmitted. Because its staff is small and the volume of reports large, Ops Four rarely has the time to verify, edit, or interpret the reports before passing them on to "user organizations."

Daily recipients of this raw intelligence include all of the Army's military intelligence groups within the United States, riot-control units on stand-by alert, and the Army Operations Center at the Pentagon. The Operations Center, sometimes called the "domestic war room," is green-carpeted suite of connecting offices, conference rooms, and cubicles from which Army and Defense Department officials dispatch and coordinate troops that deal with riots, earthquakes, and other disasters. Recipients of weekly CONUS intelligence summaries, also prepared at Fort Holabird, include not only those on the daily distribution, but such unlikely organizations as the Army Materiel Command, the Military District of Washington, the Air Defense Command, and Army headquarters in Europe, Alaska, Hawaii, and Panama.

What is perhaps most remarkable about this domestic intelligence network is its potential for growth. Uninhibited by Congressional or Presidental oversight, it has already expanded to the point where it in some ways rivals the FBI's older internal-security program. If the Army's fascination with the collection of domestic intelligence continues to grow as it has in the recent past, the Intelligence Command could use military funds to develop one of the largest domestic intelligence operations outside of the communist world. Before this happens, the American public and its elected representatives ought to demand a say in the development of this program.

THE ARMY'S NEEDS

Intentionally or not, the Army has gone far beyond the limits of its needs and authority in collecting domestic political information. It has created an activity which, by its existence alone, jeopardizes individual rights, democratic political processes, and even the national security it seeks to protect.

There is no question that the Army must have domestic intelligence. In order to assist civilian authorities, it needs maps and descriptions of potential riot or disaster areas, as well as early warning of incidents likely to provoke mass violence. Before trusting its employees or prospective employees with military secrets, it has to look into their past behavior for evidence of disloyalty or unsuitability. The Army also must investigate train wrecks, fires, and other disasters which may disrupt its lines of supply. And where ultra-militant groups seek to attack military installations, destroy files, or abuse soldiers, it has the right and obligation to keep informed about the groups' specific objectives, plans, and techniques.

The Army needs this kind of information so that it can fulfill long-established, legitimate responsibilities. But must it also distribute and store detailed reports on the political beliefs and actions of individuals and groups?

Officials of the Intelligence Command believe that they must. Without detailed knowledge of community "infrastructure," they argue, riot-control troops would not be able to enforce curfews or quell violence. To support this contention, they cite the usefulness of personality files and blacklists in breaking up guerrilla organizations in Malaya and South Vietnam. One early proponent of this view was the Army's Assistant Chief of Staff for Intelligence during 1967–1968, Major General William P. Yarborough. At the height of the Detroit riots of 1967 he instructed his staff in the domestic war room: "Men, get out your counterinsurgency manuals. We have an insurgency on our hands."

Of course, they did not. As one warroom officer who attempted to carry out the General's order later observed: "There we were, plotting power plants, radio stations, and armories on the situation maps when we should have been locating the liquor and color-television stores instead." A year later the National Advisory Commission on Civil Disorders reached a similar conclusion about the motives of ghetto rioters. "The urban disorders of the summer of 1967," it declared unequivocally, "were not caused by, nor were they the consequence of, any organized plan or 'conspiracy.'" After reviewing all of the federal government's intelligence reports on 23 riots, it found "no evidence that all or any of the disorders or the incidents that led to them were planned or directed by any organizations or groups, international, national, or local."

Intensive investigations subsequently conducted by local police departments, grand juries, city and state committees, and private organizations have concurred. One of the more recent, a study of 1968 "urban guerrilla" activities by the Lemberg Center for the Study of Violence at Brandeis University, is typical. It found that press and police accounts of shooting incidents were grossly exaggerated. While acknowledging that there had been "a few shoot-outs with the police" some of which "may have been planned," the Center concluded that there was "no wave of uprisings and no set pattern of murderous conflict" from which one could predict organized violence even remotely resembling guerrilla warfare.

But even if there were grounds for making such a prediction, the Army's case for personality files and blacklists would remain weak. The purpose of these records, according to counterinsurgency manuals, is to facilitate the selective arrest of guerrillas and insurgents. However, within the United States the Army has no authority to round up suspects the moment civilians take up arms. The seizure of civilians on suspicion of conspiring or attempting to overthrow the government by unlawful means or of inciting people to crime is, and continues to be, the responsibility of local and state police and of the FBI. The President may order Army units to help state or federalized National Guard troops keep the peace or fight

guerrillas, but the Army does not acquire authority to arrest civilians unless and until civilian law enforcement has broken down and a declaration of martial law puts all governmental authority in the area of conflict in the hands of the military. In that highly remote circumstance, the Intelligence Command might have some need for personality files and blacklists on criminally inclined, politically motivated civilians. By then, however, it certainly would have full access to the more extensive and up-to-date files of the civilian agencies and thus would not have had to prepare its own.

The Army's need to keep its own dossiers on the politics of law-abiding citizens and groups makes even less sense. So long as there is a possibility that peaceful protests may get out of hand, some surveillance undoubtedly is in order. But must the Army conduct it? Are its agents and record keepers more competent than those of the FBI or of the police departments of the cities in which large demonstrations typically occur? Are the civilian law enforcement agencies so uncooperative that the Army must substantially duplicate their efforts?

More extraordinary still is why the Intelligence Command each week alerts military headquarters in Alaska, Hawaii, Panama, and Europe to stateside non-events like the following:

"Miami, Fla.: A spokesman for the Southern Students Organizing Committee announced plans for a demonstration to be held on the campus of the University of Miami in the morning. According to the spokesman, a group of anti-war/draft supporters will participate in the demonstration.

"Philadelphia, Pa.: Members of the Vietnam Week Committee composed largely of professors and students of the University of Pennsylvania, will conduct a "sleep-in" to protest the scheduled appearance of Dow Chemical Company recruiters on campus. The next day, 19 March, the same organization will sponsor a protest rally on campus."

Perhaps the best answer to all of these questions is that much of the CONUS intelligence program serves no military need at all. But if this is so, then where does the Army get the authority to run it?

THE ARMY'S AUTHORITY

According to the Nixon Administration, authority for this kind of program comes from the Constitution. So, at least, the Justice Department claimed last June in a brief defending the FBI's failure to obtain search warrants before tapping telephone calls of what were then the "Chicago Eight." The Justice Department argued that Article Two of the Constitution authorizes the President and his agents to engage in whatever "intelligence-gathering operations he believes are necessary to protect the security of the nation" and that this authority "is not dependent upon any grant of legislative authority from Congress, but rather is an inherent power of the President, derived from the Constitution itself." Thus, the Department contended, "Congress cannot tell the President what means he may employ to obtain information he needs to determine the proper deployment of his forces."

If this is so, then Army agents do have the authority to undertake any surveillance that does not run afoul of the Constitution and the courts; indeed, they can investigate anything that is normally investigated by the federal government's civilian agencies. Moreover, they do not have to obey laws like the Omnibus Crime Control Act of 1968, which forbids most wiretapping and electronic eavesdropping without prior judicial authorization in the form of a warrant.

Fortunately, the "inherent powers doctrine," as this theory is called, has few supporters. The courts have never accepted the proposition that Congress is powerless to prescribe how the President shall exercise his executive powers. Indeed, in 1952, the Supreme Court rejected President Truman's claim to inherent power to seize the nation's steel mills to avert a strike which threatened the flow of equipment and supplies to American troops fighting in Korea. If there were no constitutional Presidential power to meet that emergency, it is unlikely that one exists to authorize the intelligence powers which the government claims today.

It is far more probable that the courts would endorse a conflicting view: that the Army's authority to collect domestic intelligence is limited by, and can only be inferred from, those laws which traditionally mark off the Army's responsibility for law enforcement from that of other agencies. These include not only the statutes which restrict the Army to a back-up function in times of riot, but the laws which assign surveillance of unlawful political activity within the United States to the FBI and the Secret Service. Other sources of the Army's authority include the Uniform Code of Military Justice, which permits investigation of unlawful political activity within the armed services, and those laws and federal-state agreements under which the Army governs many of its installations. These rules, and not the vague provisions of Article Two, are the legitimate sources of the military's domestic-intelligence powers.

Yet even if the current Administration's claim to an inherent constitutional power to watch lawful political activity were to be accepted by the courts, the surveillance itself probably would be forbidden by the Bill of Rights. The reason is the chilling effect which knowledge of surveillance has upon the willingness of citizens to exercise their freedoms of speech, press, and association, and their right to petition the government for redress of grievances.

Ten years ago the federal courts would not have accepted this contention. Then the courts were hesitant even to accept constitutional challenges to the government's collection of political information when the plaintiffs could prove that the investigators had no other purpose than to deter them from exercising their rights under the First Amendment. Recently, however, the courts have begun to accept the proposition that vague and overbroad laws and administrative actions are unconstitutional if they inhibit the exercise of those rights, regardless of whether that effect was intended.[1]

[1] Typical of this growing body of constitutional interpretation is the 1965 case of *Lamont* v. *Postmaster General*. There the Supreme Court struck down a federal statute which authorized the Post Office to suspend delivery of unsolicited mail which the government agents regarded as "Communist political propaganda" until the addressee returned a reply post card declaring that he wished to received the mail. The Court, in a unanimous opinion, held that the effect of this practice, whatever the government's purpose, was to abridge freedom of speech by inhibiting the right to read.

Even more on point is the decision of a New Jersey Superior Court which last August declared most of that state's domestic intelligence system unconstitutional. In *Anderson* v. *Sills*, a suit filed by the American Civil Liberties Union on behalf of the Jersey City branch of the NAACP, the court held: "The secret files that would be maintained as a result of this intelligence system are inherently dangerous, and by their very existence tend to restrict those who would advocate . . . social and political change."

Had the New Jersey authorities been able to show a more urgent need for the records, the court might not have taken such a categorical position. But the police, like the Army, had cast their net so widely that it was bringing up huge quantities of information on wholly lawful political activities. Accordingly, the court brushed aside the state's claim to good intentions and found that the program had a chilling effect upon the exercise of First Amendment rights. It ordered all forms and files destroyed, "except where such information will be used to charge persons with specifically defined criminal conduct."

If people are likely to be deterred in the exercise of their rights by state intelligence systems, they undoubtedly will be inhibited by knowledge that reports of individual participation in public demonstrations are being made daily to the Pentagon, selected troop units, and an interagency data bank at Fort Holabird. Thus, even if the Army's collection of personality files and blacklists is not limited by legislation, it still may be unlawful.

THE PROGRAM'S IMPACT

Beyond the Army's need for the present CONUS intelligence program and its authority to pursue it lies the matter of its impact upon the public interest. In particular, there is its effect upon the rights of individuals, the democratic process, and the nation's security.

The impact which the program can have upon the exercise of political rights needs no further explication. The threat it poses to job rights and privacy, however, may not be so apparent.

Like the freedom from inhibitory surveillances, the job rights threatened are rights in the making. As yet no one has established a legal right to a job that requires a security clearance or to a security clearance essential to a job. Nevertheless, in recent years the courts have begun to recognize that those who already hold federal jobs and security clearances have a right not to be deprived of either without just cause or, at the very least, without the rudiments of fairness. The impending marriage of the CONUS intelligence wire service to a computer could nullify even this protection, by filling security-clearance dossiers with unverified and potentially erroneous and irrelevant reports. These reports would then be used to determine who should, and who should not, receive security clearances.

If the men and women who adjudicate security clearance were competent to evaluate such unreliable information, its inclusion in security files might be less cause for concern. Unfortunately, they are not. The most highly trained adjudicators—civilians employed by the stateside army commands—receive only nine days of job instruction on loyalty determinations at the Army Intelligence School. Moreover, this training does not even touch upon the subject of suitability, although almost 98 per cent of all clearances denied today are ostensibly rejected on that ground. The least trained adjudicators—intelligence officers assigned to field commands—receive exactly two classroom hours on loyalty and two on suitability while being trained to become investigators. Because of this extremely brief training, it is not unusual for an adjudicator to conclude that a person arrested in connection with a political protest is not suited for a security clearance, regardless of the circumstances of his arrest, the legality of his detention, or his innocence of the charges.

The adjudicators' lack of training is compounded by security regulations which permit—indeed, seem to require—the denial of clearances on less evidence than would support a magistrate's finding of "probable cause." In other words, it is not a question of whether reliable evidence indicates that the individual cannot be trusted with state secrets, but of whether the granting of the clearance would be "clearly consistent with

the interests of national security." No one really knows what this ambiguous phrase means, but in practice it frequently is used to justify findings of guilt by association. For example, soldiers and civilian employees of the Army with foreign-born spouses are virtually blocked from jobs requiring access to especially sensitive intelligence. Their association with a spouse who once "associated with foreigners" is taken as proof of their vulnerability to recruitment by foreign agents. Moreover, in nearly all other cases, adjudicators usually have to make their decisions without knowing the source of the evidence, without hearing the accused confront his accusers, or without hearing the accused defend himself with knowledge of their identity.

Given the tenuousness of the right to due process under these conditions, the influx of CONUS intelligence reports can make the system even more unjust than it is now. At the present time, little information on political activity is developed in the course of most background investigations. Army investigations, in particular, tend to be superficial; in some sections of the country shortages of personnel, caused by the war in Vietnam, have forced the Intelligence Command to abandon interviews of character references in favor of questionnaires-by-mail as its main means of inquiry. But if these questionnaires were to be supplemented by CONUS political reports, the number of clearances unjustly denied would skyrocket. These injustices would occur not only within the military; they would reverberate throughout all federal agencies with access to the Fort Holabird data bank.

The Army's domestic-intelligence program also imperils numerous expectations of privacy, some of which enjoy the status of legal rights. It does so by exposing Americans to governmental scrutiny, and the fear of scrutiny, to an extent to which they have never been exposed before. Even the Budget Bureau's ill-starred proposal to consolidate the federal government's statistical records into a National Data Center would not have brought together so much information about individual beliefs and actions.

The privacy of politically active citizens is especially threatened by the Army's practice of watching political protests, large and small, throughout the United States. To the potential protester, it is one thing to expect local press and police coverage; it is quite another to expect a military surveillance which specializes in keeping permanent records of lawful political activity.

What effect awareness of the CONUS intelligence program will have on the vast majority of people who are not politically active is more difficult to predict. By itself, news that the Army is watching civilian politics is not likely to cause most people to worry personally about their privacy. But it would be one more increment in a growing pattern of governmental intrusiveness that could have a significant cumulative impact.

Such a pattern is now well established. Among the more widely publicized activities in recent years have been the CIA's surreptitious financing of student groups, labor unions, and foundations (despite the territorial limits of that agency's mandate), the Post Office's use of peepholes in restroom walls, and the Defense Department's misuse of lie dectectors. Others include countless illegal wiretaps by the FBI, the Internal Revenue Service, and the Department of the Interior. More recently, the publication of confidential FBI wiretap information by *Life* and *Newsweek* which linked Jet's quarterback Joe Namath to Mafia figures suggests that the FBI has now assumed responsibility for enforcing professional football's code of conduct.

The cumulative impact of such abuses of power and privacy eventually must convince even the most anonymous of individuals that the United States is moving towards a society in which no one has control over what others know about him. Public awareness of the Army's activities cannot but hasten this conviction.

The unregulated growth of CONUS intelligence machinery also threatens the country's political health. It does so both by inhibiting political participation and by enhancing the potential clout of demagogues and others who would misuse security files for partisan or personal purposes.

The most immediate risk posed, of course, is to political participation. Once citizens come to fear that government agencies will misuse information concerning their political activities, their withdrawal from politics can be expected. This withdrawal can occur in a variety of ways. Some people may decline to become involved in potentially controversial community organizations and projects. Others may go further and avoid all persons who support unpopular ideas or who criticize the government. Some may refuse to object to the abuse of government authority, especially when the abuse is committed in the name of national security. Others may even stop reading political publications, out of fear that the government might learn of their reading habits and disapprove. Indeed, an adjudicator of security clearances once asked me if she could lose her clearance if she allowed her daughter to subscribe to *The National Observer!*

Inhabitions generated by awareness of extensive domestic surveillance are likely to be strongest at the local level. This is where most citizens participate in politics if they become involved at all. The withdrawal can be expected to occur all across the political spectrum, although the strongest objections to surveillance will undoubtedly come from the left. Those most likely to be deterred, however, are not the extremists of the right or the left, whose sense of commitment runs deep, but the moderates, who normally hold the balance of power. Depletion of their ranks would, of course, strengthen the influence of the extremists, polarize debate, increase animosities, and decrease tolerance. As political positions rigidify, compromise and flexibility would become harder to achieve. And the capacity of government to renew itself and promote responsible progress would also suffer.

A less immediate but no less serious danger lies in the potential for misuse inherent in the Army's extensive files on individuals and groups. It is frightening to imagine what could happen if a demagogue in the Martin Dies-Joseph McCarthy tradition were to gain access to the computer the Army seeks now, or if an Otto Otepka in uniform were to leak a copy of the Intelligence Command's so-called "blacklist" to friends in Congress, or if a General Edwin Walker were to take charge of the Intelligence Command.

Such speculation assumes, of course, that the Army cannot guarantee the inviolability of its files. The assumption, unfortunately, has some validity. Only last year, information from the Army's confidential service record on New Orleans District Attorney Jim Garrison was leaked to the press. Officers at the Investigative Records Repository at Fort Holabird (which functions as the Army's lending library for such files) suspected that the leak came from a civilian agency in Washington. They were helpless to do anything about it, however, because they had no system of records accountability by which they could fix responsibility. When asked why such a system did not exist, one officer told me: "We probably couldn't stop it [the leaks] if we tried."

Finally, the unregulated growth of domestic intelligence activity can have the paradoxical effect of undermining the very security it seeks to protect. It can do so in at least two ways. First, by increasing the "cost" of lawful political activity, it tends to force extremist groups to go underground, there to act out their us-versus-them view of politics by criminal means. Second, by intruding too closely into the lives of government employees (or prospective employees), it tends to inhibit them from applying for jobs requiring security clearances or from exercising initiative and imagination in those jobs. A good intelligence officer must be able to analyze and report accurately, and to do so he must feel free to immerse himself in the ideas and culture of the people he studies. A good scientist must have freedom to pursue his curiosities, or he is not likely to work for the government, which rarely pays as much as private industry. The direct consequence of programs which deny this freedom is to impair the quality of secret work and the caliber of the men who do it. As John Stuart Mill warned over a century ago:

"A state which dwarfs its men, in order that they may be more docile instruments in its hands, even for beneficial purposes, will find that with small men no great things can really be accomplished."

WHAT CAN BE DONE?

If the Army has exceeded the limits of its needs and authority to establish a domestic intelligence program which endangers numerous public interests, what steps should be taken to curb its excesses?

An obvious first step is a court challenge of the Army's authority to possess information for which it has no substantial need. The main target of such a lawsuit should be the personality files and blacklists describing the lawful political activities of individuals and groups. A second target should be the collection and storage of information on individuals and groups suspected of participating in unlawful political activity—except where that information is essential to an "early warning" system, or where the persons involved are associated with the armed forces, or where the information is collected in the course of security investigations.

The lawsuit's argument should be twofold: (1) the Army has no substantial need for either kind of information, and (2) the very existence of the program inhibits the exercise of First Amendment rights. Such a suit should seek a court order declaring the Army's possession of both kinds of information to be unconstitutional; it should also ask the court to enjoin future collection and storage of such information and to direct the destruction of all existing personality files and blacklists.

While such a lawsuit stands a good chance of success, it could take years to litigate. Moreover, a favorable decision could be ignored or evaded for many more years. Thus, while the symbolic value of such a decision would more than justify the time and expense, an effective challenge of the intelligence program will require the development of legislative and administrative remedies as well.

Whoever attempts to devise these remedies should be prepared to undertake subtle analyses of competing interests and values, for while the excesses of the program must be permanently curbed, the Army's ability to fulfill its responsibilities must not be impaired.

Ideally, legislative and executive analyses should be based on the kinds of questions I have already asked: What are the Army's real domestic intelligence needs? What authority does it have to initiate specific activities to meet those needs? What threats to liberty does each domestic intelligence effort pose?

The analysis should begin by demanding a justification for each alleged intelligence need in terms of the Army's authority to meet such a need and its purpose in trying to do so. Each need should then be weighed

against the threats it may pose to the rights of individuals, to the vitality of the political process, and to the security of the nation. Where the risk is clear and the need doubtful, the Army should be denied authority to satisfy the need. Where the threat and the Army's need are both evident, less hazardous alternatives ought to be considered. In this circumstance, the capacity of politically responsible officials to control the alternatives should be weighed. Where reliable controls cannot be devised, the intelligence effort should not be authorized—even though the denial of authority may deprive the government of useful knowledge about the domestic political scene. If the imposition of these restraints poses a risk to internal security, then we must accept that risk as the price for individual liberties and a truly democratic political system.

The Congressional power of inquiry should be exercised first. Few Americans—including most members of Congress—know anything about the activities and plans of the domestic intelligence community. Many do not even realize that the growth of formal and informal ties among law-enforcement, intelligence, and security agencies has made it necessary to think in such terms.

For maximum effectiveness, Congress should hold open hearings not only to inform itself and the public, but to remind the intelligence community in general, and the Army in particular, that their authority to spy on civilian politics must be construed strictly, in accordance with such established principles as civilian control of the military, Presidential control of the bureaucracies, state and civilian primacy in law enforcement, compartmentalization and decentralization of intelligence duties, and obedience to law. Where it is not, corrective legislation should be promised.

A special effort should be made in the course of these hearings to inform the domestic intelligence community that Congress does not accept the Justice Department's position that "Congress cannot tell the President what means he may employ to obtain the information he needs."

Congress should also exercise its appropriations power so as to encourage major reforms in the Army's program. Specifically, it should block all funds for the planned computer unless and until the Army agrees to:

(1) Instruct its agents to limit their collection of CONUS intelligence to reports of incidents, except where the reports describe violations of the Uniform Code of Military Justice or of Army regulations. This would dry up the source of most blacklists and personality files.

(2) Forbid the Intelligence Command to convert incident reports into personality reports, except where they relate to criminal or deviant activity by persons subject to military law or employed by the military. Thus storage of information about named civilians unassociated with the armed forces would be doubly foreclosed, should such information be reported by mistake or as an essential element of an incident report.

(3) Establish effective technological, legal, and administrative safeguards against the abuse of individual rights in the process of collecting, reporting, storing, and disseminating domestic intelligence or personnel security information. For example, the Army should forbid its agents to infiltrate civilian political groups. (If it fails to do so, Congress should make such infiltration a federal crime, just as it is now a crime for a local military commander to order his troops to serve in a sheriff's posse.) Computer storage systems also should be encouraged, since they can be equipped with more effective safeguards against misuse than is possible in document storage systems. However, these safeguards must be carefully designed, regularly tested, and reinforced by laws and regulations to deter those who might seek to circumvent them.

(4) Establish separate headquarters, preferably in separate cities, for the CONUS-intelligence and personnel-security staffs. So long as the two programs are located at the some headquarters (they now share the same room and some of the same personnel), the danger of informal leakage of CONUS intelligence material to the adjudicators will remain high. Establishment of physically separate headquarters would be expensive, since it would probably require two separate communications and information storage systems. Separate storage systems, however, could be more safely computerized. Thus some of the additional expense might be recouped through increased efficiency.

(5) Request that the United States Judicial Conference or some similar body nominate a civilian advisory board to review and report annually on the sufficiency of the Intelligence Command's procedures for safeguarding individual rights. Such a board 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. How successful such a board can be is open to question; much depends upon how skillfully its members can be chosen so as to assure both military and public confidence in their capacity for balanced and constructive judgments.

(6) Improve the professional quality of Intelligence Command personnel and security-clearance adjudicators. In the final analysis, the Army must be the front-line defender against the dangerous consequences of its own actions. Thus, among other things, the Army should be encouraged to end the overcrowding and understaffing of its Intelligence School, to revise and expand the curriculum of its agents' course, and to transfer the training of security-clearance adjudicators to an accredited law school or the Practising Law Institute, a non-profit organization well known for its practical courses for lawyers and laymen on specialized legal subjects.

Needless to say, each of these reforms should be initiated by the President or the Army without waiting for Congressional encouragement. In addition, the President should appoint a panel of distinguished citizens, on the order of the Kerner Commission, to look into the conduct of all domestic intelligence activities. He should also ask an organization like the highly prestigious American Law Institute to draft a new executive order and code of regulations to govern the granting of security clearances.

Implementation of these reforms can do much to bring the Army's domestic intelligence practices in line with its legitimate responsibilities. But it is not enough to reform the Army. The Intelligence Command is only one member of a huge, informal community of domestic intelligence agencies. Other members of the community include not only the FBI, the Secret Service, the Air Force, and the Navy, but hundreds of state and municipal police departments. Some of the latter are surprisingly large. The New York City Police Department's Bureau of Special Services, for example, employs over 120 agents and has an annual budget in excess of $1 million.

Each of these organizations now shares with the Army the capacity to inhibit people in the exercise of their rights, even without trying. By collaborating, they could become a potent political force in their own right. Thus as the Army, the FBI, and the Justice Department strive to coordinate these agencies through the establishment of wire services, hot lines, and computerized data banks, it is essential that the American public and its representatives be equally energentic in the imposition of checks and balances. In particular, special efforts should be made to prevent needless concentrations of information. The United States may be able to survive the centralization of intelligence files without becoming totalitarian, but it most certainly cannot become totalitarian without centralized intelligence files. The checks must be designed with the most unscrupulous of administrators in mind. The fact that we may trust the current heads of our investigative agencies is no guarantee that these agencies will not one day come under the control of men for whom the investigatory power is a weapon to be wielded against political and personal foes.

[From the New York (N.Y.) Times, Jan. 16, 1970]

EX-OFFICER SAYS ARMY SPIES ON CIVILIAN ACTIVISTS—1,000 PLAINCLOTHESMEN SAID TO REPORT ON VIRTUALLY ALL POLITICAL GROUPS

WASHINGTON, January 15.—A former Army intelligence officer said in a magazine article today that nearly 1,000 plainclothes Army investigators keep track of civilian political activity across the country and submit regular reports to a collection headquarters at Fort Holabird in Baltimore.

Christopher H. Pyle, a former captain in Army Intelligence who is now studying for a doctorate in political science at Columbia University, said Army detectives attend political rallies, protest marches and other gatherings, but base most of their reports on the files of "municipal and state police departments and of the F.B.I."

"To assure prompt communication of these reports," Mr. Pyle said, "the Army distributes them over a nationwide wire service. Completed in the fall of 1967, this Teletype network gives every major troop command in the United States daily and weekly reports on virtually all political protests occurring anywhere in the nation."

Mr. Pyle said the investigators monitor "protest politics" ranging from Ku Klux Klan rallies in North Carolina to meetings of the Women's Strike for Peace in Philadelphia.

"Today, the Army maintains files on the membership, ideology, programs, and practices of virtually every activist political group in the country," he said.

The article was published today in The Washington Monthly, a magazine focusing on problems in American politics and government.

BLACKLIST ALLEGED

Mr. Pyle also said in the article that the Army periodically publishes an eight-by-ten-inch glossy-cover booklet known within intelligence circles as the "blacklist."

Mr. Pyle said this is an encyclopedia of profiles of people and organizations who, in the opinion of the intelligence command officials who compile it, might "cause trouble for the Army."

The surveillance program was started in 1965, Mr. Pyle said, but at that time was designed only to give military officials early warning of possible civil disorders. The program was gradually widened to include most forms of political protest activity, he said.

The investigators are all Army personnel, he said. About 75 per cent are enlisted men and 25 per cent are lieutenants or captains. Mr. Pyle added in a telephone interview, saying that the detectives have top-secret clearances.

The Army also plans, according to Mr. Pyle, to link its Teletype systems to a computerized data bank at Fort Holabird, to which Federal agencies such as the Secret Service, the Federal Bureau of Investigation and the Central Intelligence Agency will have access.

Spokesmen at the intelligence command at Fort Holabird and at the Pentagon declined comment on Mr. Pyle's article.

Mr. Pyle, 30 years old, received an Army