C. EXCESSIVE USE OF INTRUSIVE TECHNIQUES

Major Finding

The intelligence community has employed surreptitious collection techniques—*mail opening, surreptitious entries, informants,* and "traditional" and highly sophisticated forms of electronic surveillance—to achieve its overly broad intelligence targeting and collection objectives. Although there are circumstances where these techniques, if properly controlled, are legal and appropriate, the Committee finds that their very nature makes them a threat to the personal privacy and Constitutionally protected activities of both the targets and of persons who communicate with or associate with the targets. The dangers inherent in the use of these techniques have been compounded by the lack of adequate standards limiting their use and by the absence of review by neutral authorities outside the intelligence agencies. As a consequence, these techniques have collected enormous amounts of personal and political information serving no legitimate governmental interest.

Subfindings

(a) Given the highly intrusive nature of these techniques,[1] the legal standards and procedures regulating their use have been insufficient. There have been no statutory controls on the use of informants; there have been gaps and exceptions in the law of electronic surveillance; and the legal prohibitions against warrantless mail opening and surreptitious entries have been ignored.

(b) In addition to providing the means by which the Government can collect too much information about too many people, certain techniques have their own peculiar dangers:

(i) Informants have provoked and participated in violence and other illegal activities in order to maintain their cover, and they have obtained membership lists and other private documents.

(ii) Scientific and technological advances have rendered traditional controls on electronic surveillance obsolete and have made it more difficult to limit intrusions. Because of the nature of wiretaps, microphones and other sophisticated electronic techniques, it has not always been possible to restrict the monitoring of communications to the persons being investigated.

(c) The imprecision and manipulation of labels such as "national

[1] The techniques noted here do not constitute an exhaustive list of the surreptitious means by which intelligence agencies have collected information. The FBI, for example, has obtained a great deal of financial information about American citizens from tax returns filed with the Internal Revenue Service. (See IRS Report: Sec. I, "IRS Disclosures to FBI and CIA.") This section, however, is limited to problems raised by electronic surveillance, mail opening, surreptitious entries informants and electronic surveillances.

security," "domestic security," "subversive activities," and "foreign intelligence" have led to unjustified use of these techniques.

Elaboration of Findings

The preceding section described how the absence of rigorous standards for opening, controlling, and terminating investigations subjected many diverse elements of this society to scrutiny by intelligence agencies, without their being suspected of violating any law. Once an investigation was opened, almost any item of information about a target's personal behavior or political views was considered worth collecting.

Extremely intrusive techniques—such as those listed above—have often been used to accomplish those overly broad targeting and collection objectives.

The paid and directed informant has been the most extensively used technique in FBI domestic intelligence investigations. Informants were used in 83% of the domestic intelligence investigations analyzed in a recent study by the General Accounting Office.[1a] As of June 30, 1975, the FBI was using a total of 1,500 domestic intelligence informants.[2] In 1972 there were over 7,000 informants in the ghetto informant program alone. In fiscal year 1976, the Bureau has budgeted more than $7.4 million for its domestic intelligence informant program, more than twice the amount allocated for its organized crime informant program.[3]

Wiretaps and microphones have also been a significant means of gathering intelligence. Until 1972, the FBI directed these electronic techniques against scores of American citizens and domestic organizations during investigations of such matters as domestic "subversive" activities and leaks of classified information. The Bureau continues to use these techniques against foreign targets in the United States.

The most extensive use of electronic surveillance has been by the National Security Agency. NSA has electronically monitored (without wiretapping in the traditional sense) international communication links since its inception in 1952; because of its sophisticated technology, it is capable of intercepting and recording an enormous number of communications between the United States and foreign countries.[4]

All mail opening programs have now been terminated, but a total of twelve such operations were conducted by the CIA and the FBI in ten American cities between 1940 and 1973.[5] Four of these were operated by the CIA, whose most massive project involved the opening of more than 215,000 letters between the United States and the Soviet Union over a twenty-year period. The FBI conducted eight mail opening programs, three of which included opening mail sent between two points in the United States. The longest FBI mail opening program

---

[1a] Report to the House Committee on the Judiciary, by the Comptroller General of the United States, "FBI Domestic Intelligence Operations—Their purpose and scope: Issues that Need to be Resolved," 2/24/76, p. 96.

[2] FBI memorandum to the Select Committee, 11/28/75.

[3] Memorandum, *FBI Overall Intelligence Program FY 1977 Compared to FY 1976* undated. The cost of the intelligence informant program comprises payments to informants for services and expense as well as the costs of FBI personnel, support and overhead.

[4] See NSA Report: Sec. I, "Introduction and Summary."

[5] See Mail Opening Reports: Sec. I, "Summary and Principal Conclusions."

lasted, with one period of suspension, for approximately twenty-six years.

The FBI has also conducted hundreds of warrantless surreptitious entries—break-ins—during the past twenty-five years. Often these entries were conducted to install electronic listening devices; at other times they involved physical searches for information. The widespread use of warrantless surreptitious entries against both foreign and domestic targets was terminated by the Bureau in 1966 but the FBI has occasionally made such entries against foreign targets in more recent years.

All of these techniques have been turned against American citizens as well as against certain foreign targets. On the theory that the executive's responsibility in the area of "national security" and "foreign intelligence" justified their use without the need of judicial supervision, the intelligence community believed it was free to direct these techniques against individuals and organizations whom it believed threatened the country's security. The standards governing the use of these techniques have been imprecise and susceptible to expansive interpretation and in the absence of any judicial check on the application of these vague standards to particular cases, it was relatively easy for intelligence agencies and their superiors to extend them to many cases where they were clearly inappropriate. Lax internal controls on the use of some of these techniques compounded the problem.

These intrusive techniques by their very nature invaded the private communications and activities both of the individuals they were directed against and of the persons with whom the targets communicated or associated. Consequently, they provided the means by which all types of information—including personal and political information totally unrelated to any legitimate governmental objective—were collected and in some cases disseminated to the highest levels of the government.

Subfinding (a)

Given the highly intrusive nature of these techniques, the legal standards and procedures regulating their use have been insufficient. There have been no statutory controls on the use of informants; there have been gaps and exceptions in the law of electronic surveillance; and the legal prohibitions against warrantless mail opening and surreptitious entries have been ignored.

1. The Absence of Statutory Restraints on the Use of Informants

There are no statutes or published regulations governing the use of informants.[6] Consequently, the FBI is free to use informants, guided only by its own internal directives which can be changed at any time by FBI officials without approval from outside the Bureau.[7]

---

[6] Title 28 of the United States Code provides only that appropriations for the Department of Justice are available for payment of informants. 28 U.S.C. § 524.

[7] The Attorney General has announced that he will issue guidelines on the use of informants in the near future, and our recommendations provide standards for informant control and prohibitions on informant activity. (See pp. 328.) In addition, the Attorney General's recently promulgated guidelines on "Domestic Security Investigations" limit the use of informants at the early stages of such inquiries and provide for review by the Justice Department of the initiation of "full investigations" in which new informants may be recruited.

Apart from court decisions precluding the use of informants to entrap persons into criminal activity, there are few judicial opinions dealing with informants and most of those concern criminal rather than intelligence informants.[8] The United States Supreme Court has never ruled on whether the use of intelligence informants in the contexts revealed by the Committee's investigation offend First Amendment rights of freedom of expression and association.[9]

In the absence of regulation through statute, published regulation, or court decision, the FBI has used informants to report on virtually every aspect of a targeted group or individual's activity, including lawful political expression, political meetings, the identities of group members and their associates, the "thoughts and feelings, intentions and ambitions," of members,[10] and personal matters irrelevant to any legitimate governmental interest. Informants have also been used by the FBI to obtain the confidential records and documents of a group.[11]

Informants could be used in any intelligence investigation. FBI directives have not limited informant reporting to actual or likely violence or other violations of law.[12] Nor has any determination been made concerning whether the substantial intrusion represented by informant coverage is justified by the government's interest in obtaining information, or whether less intrusive means would adequately serve the government's interest. There has also been no requirement that the decisions of FBI officials to use informants be reviewed by anyone outside the FBI. In short, intelligence informant coverage has not been subject to the standards which govern the use of other intrusive techniques such as electronic surveillance, even though informants can produce a far broader range of information.

2. Gaps and Exceptions in the Law of Electronic Surveillance

Congress and the Supreme Court have both addressed the legal issues raised by electronic surveillance, but the law has been riddled with gaps and exceptions. The Executive branch has been able to apply vague standards for the use of this technique to particular cases

[8] In a criminal case involving charges of jury bribery, *United States* v. *Hoffa*, 385 U.S. 293 (1966), the Supreme Court ruled that an informant's testimony concerning conversations of a defendant could not be considered the product of a warrantless search in violation of the Fourth Amendment on the ground the defendant had consented to the presence of the informant. In another criminal case, *Lewis* v. *United States*, 385 U.S. 206 (1966), the Court stated that "in the detection of many types of crimes, the Government is entitled to use decoys and to conceal the identity of its agents."

[9] In a more recent case, the California Supreme Court held that secret surveillance of classes and group meetings at a university through the use of undercover agents was "likely to pose a substantial restraint upon the exercise of First Amendment rights." *White* v. *Davis*, 533 Pac. Rep. 2d, 223 (1975) Citing a number of U.S. Supreme Court opinions, the California Supreme Court stated in its unanimous decision:

"In view of this significant potential chilling effect, the challenged surveillance activities can only be sustained if [the Government] can demonstrate a 'compelling' state interest which justifies the resultant deterrence of First Amendment rights and which cannot be served by alternative means less instrusive on fundamental rights." 533 Pac. Rep. 2d, at 232

[10] Gary Rowe testimony, 12/2/75 Hearings, Vol. 6, pp. 111, 118.

[11] Cook, 12/2/75, Hearings, Vol. 6, p. 111.

[12] The FBI Manual of Instructions proscribes only reporting of privileged communications between an attorney and client, legal "defense plans or strategy," "employer-employee relationships" (where an informant is connected with a labor union), and "legitimate institution or campus activities" at schools. (FBI Manual Section 107.)

as it has seen fit, and, in the case of NSA monitoring, the standards and procedures for the use of electronic surveillance were not applied at all.

When the Supreme Court first considered wiretapping, it held that the warrantless use of this technique was constitutional because the Fourth Amendment's warrant requirement applied only to physical trespass and did not extend to the seizure of conversation. This decision, the 1928 case of *Olmstead* v. *United States*, involved a criminal prosecution, and left federal agencies free to engage in the unrestricted use of wiretaps in both criminal and intelligence investigations.[13]

Six years later, Congress enacted the Federal Communications Act of 1934, which made it a crime for "any person," without authorization, to intercept and divulge or publish the contents of wire and radio communications. The Supreme Court subsequently construed this section to apply to federal agents as well as to ordinary citizens, and held that evidence obtained directly or indirectly from the interception of wire and radio communications was not admissible in court.[14] But Congress acquiesed in the Justice Department's position that these cases prohibited only the divulgence of contents of wire communications outside the executive branch,[15] and Government wiretapping for intelligence purposes other than prosecution continued.

On the ground that neither the 1934 Act nor the Supreme Court decisions on wiretapping were meant to apply to "grave matters involving the defense of the nation," President Franklin Roosevelt authorized Attorney General Jackson in 1940 to approve wiretaps on "persons suspected of subversive activities against the Government of the United States, including suspected spies."[16] In the absence of any guidance from Congress or the Court for another quarter century, the executive branch first broadened this standard in 1946 to permit wiretapping in "cases vitally affecting the domestic security or where human life is in jeopardy,"[17] and then modified it in 1965 to allow wiretapping in "investigations related to the national security."[18] Internal Justice Department policy required the prior approval of the Attorney General before the FBI could institute wiretaps in particular cases,[19] but until the mid-1960's there was no require-

---

[13] *Olmstead* v. *United States*, 277 U.S. 438 (1928).

[14] *Nardone* v. *United States*, 302 U.S. 397 (1937); 308 U.S. 338 (1939).

[15] For example, letter from Attorney General Jackson to Rep. Hatton Summers, 3/19/41; See Electronic Surveillance Report: Sec. II.

[16] Memorandum from President Roosevelt to the Attorney General 5/21/40.

[17] Letter from Attorney General Tom C. Clark to President Truman, 7/17/46.

[18] Directive from President Johnson to Heads of Agencies, 6/30/65.

[19] President Roosevelt's 1940 order directed the Attorney General to approve wiretaps "after investigation of the need in each case." (Memorandum from President Roosevelt to Attorney General Jackson, 5/21/40.) However, Attorney General Francis Biddle recalled that Attorney General Jackson "turned it over to Edgar Hoover without himself passing on each case" in 1940 and 1941. Biddle's practice beginning in 1941 conformed to the President's order. (Francis Biddle, *In Brief Authority* (Garden City: Doubleday, 1962), p. 167.)

Since 1965, explicit written authorization has been required. (Directive of President Johnson 6/30/65.) This requirement however, has often been disregarded. In violation of this requirement, for example, no written authorizations were obtained from the Attorney General—or from any one else—for a series of four wiretaps implemented in 1971 and 1972 on Yeoman Charles Radford, two of his friends, and his father-in-law. See Electronics Surveillance Report; Sec. VI.

(Continued)

ment of periodic reapproval by the Attorney General.[20] In the absence of any instruction to terminate them, some wiretaps remained in effect for years.[21]

In 1967, the Supreme Court reversed its holding in the *Olmstead* case and decided that the Fourth Amendment's warrant requirement did apply to electronic surveillances.[22] It expressly declined, however, to extend this holding to cases involving the "national security."[22a] Congress followed suit the next year in the Omnibus Crime Control Act of 1968, which established a warrant procedure for electronic surveillance in criminal cases but included a provision that neither it nor the Federal Communications Act of 1934 "shall limit the constitutional power of the President."[23] Although Congress did not purport to define the President's power, the Act referred to five broad categories which thereafter served as the Justice Department's criteria for warrantless electronic surveillance. The first three categories related to foreign intelligence and counterintelligence matters:

> (1) to protect the Nation against actual or potential attack or other hostile acts of a foreign power;
>
> (2) to obtain foreign intelligence information deemed essential to the security of the United States; and
>
> (3) to protect the national security information against foreign intelligence activities.

The last two categories dealt with domestic intelligence interests:

> (4) to protect the United States against overthrow of the government by force or other unlawful means, or
>
> (5) against any other clear and present danger to the structure or existence of the government.

In 1972, the Supreme Court held in *United States* v. *United States District Court*,[23a] that the President did not have the constitutional power to authorize warrantless electronic surveillances to protect the

---

(Continued)
The first and third of these taps were implemented at the oral instruction of Attorney General John Mitchell. (Memorandum from T. J. Smith E. S. Miller, 2/26/73.) The remaining taps were implemented at the oral request of David Young, and assistant to John Ehrlichman at the White House, who merely informed the Bureau that the requests originated with Ehrlichman and had the Attorney General's concurrence. (Memorandum from T. J. Smith to E. S. Miller, 6/14/73.

[20] Attorney General Nicholas Katzenbach instituted this requirement in March 1965. (Memorandum from J. Edgar Hoover to the Attorney General, 3/3/65.)

[21] The FBI maintained one wiretap on an official of the Nation of Islam that had originally been authorized by Attorney General Brownell in 1957 for seven years until 1964 without any subsequent re-authorization. (Memorandum from J. Edgar Hoover to the Attorney General, 12/31/65, initialed "Approved: HB, 1/2/57.")

As Nicholas Katzenbach testified: "The custom was not to put a time limit on a tap, or any wiretap authorization. Indeed, I think the Bureau would have felt free in 1965 to put a tap on a phone authorized by Attorney General Jackson before World War II." (Nicholas Katzenbach testimony, 11/12/75, p. 87.)

[22] *Katz* v. *United States*, 389 U.S. 347 (1967).

[22a] The Court wrote: "Whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security is a question not presented by this case." 389 U.S. at 358 n. 23.

[23] 18 U.S.C. 2511 (3).

[23a] 407 U.S. 297 (1972)

nation from domestic threats.[24] The Court pointedly refrained, however, from any "judgment on the scope of the Presidents' surveillance power with respect to the activities of foreign powers, within or without this country." [25] Only "the domestic aspects of national security" came within the ambit of the Court's decision.[26]

To conform with the holding in this case, the Justice Department thereafter limited warrantless wire tapping to cases involving a "significant connection with a foreign power, its agents or agencies.[27]

At no time, however, were the Justice Department's standards and procedures ever applied to NSA's electronic monitoring system and its "watch listing" of American citizens.[28] From the early 1960's until 1973, NSA compiled a list of individuals and organizations, including 1200 American citizens and domestic groups, whose communications were segregated from the mass of communications intercepted by the Agency, transcribed, and frequently disseminated to other agencies for intelligence purposes.[29]

The Americans on this list, many of whom were active in the anti-war and civil rights movements, were placed there by the FBI, CIA, Secret Service, Defense Department, and NSA itself without prior judicial warrant or even the prior approval of the Attorney General. In 1970, NSA began to monitor telephone communications links between the United States and South America at the request of the Bureau of Narcotics and Dangerous Drugs (BNDD) to obtain information about international drug trafficking. BNDD subsequently submitted the names of 450 American citizens for inclusion on the

---

[24] At the same time, the Court recognized that "domestic security surveillance" may involve different policy and practical considerations apart from the surveillance of 'ordinary crime,' 407 U.S. at 321, and thus did not hold that "the same type of standards and procedures prescribed by Title III [of the 1968 Act] are necessarily applicable to this case." (407 U.S. at 321.) The Court noted:

"Given the potential distinctions between Title III criminal surveillances and those involving the domestic security, Congress may wish to consider protective standards for the latter which differ from those already prescribed for specified crime in Title III. Different standards may be compatible with the Fourt Amendment." (407 U.S. at 321.)

[25] 407 U.S. at 307.

[26] 407 U.S. at 320. *United States* v. *United States District Court* remains the only Supreme Court case dealing with the issue of warrantless electronic surveillance for intelligence purposes. Three federal circuit courts have considered this issue since 1972, however. The Third Circuit and the Fifth Circuit both held that the President may constitutionally authorize warrantless electronic surveillance for foreign counterespionage and foreign intelligence purposes. [*United States* v. *Butenko*, 494 F.2d 593 (3d Cir. 1974), *cert. denied sub nom. Ivanov* v. *United States*, 419 U.S. 881 (1974); and *United States* v. *Brown*, 484 F.2d 418 (5th Cir., 1973), *cert. denied* 415 U.S. 960 (1974).] The District of Columbia Circuit held unconstitutional the warrantless electronic surveillance of the Jewish Defense League, a domestic organization whose activities allegedly affected U.S. Soviet relations but which was neither the agent of nor in collaboration with a foreign power. [*Zweibon* v. *Mitchell*, 516 F.2d 594 (D.C. Cir., 1975) (*en banc*).]

[27] Testimony of Deputy Assistant Attorney General Kevin Maroney, Hearings before the Senate Subcommittee on Administrative Practice and Procedures, 6/29/72, p. 10. This language paralled that of the Court in *United States* v. *United States District Court*, 407 U.S. at 309 n. 8.

[28] Although Attorney General John Mitchell and Justice Department officials on the Intelligence Evaluation Committee apparently learned that NSA was making a contribution to domestic intelligence in 1971, there is no indication that the FBI told them of its submission of names of Americans for inclusion on a NSA "watch list." When Assistant Attorney General Henry Petersen learned of these practices in 1973, Attorney General Elliott Richardson ordered that they be terminated. (See Report on NSA: Sec. I, "Introduction and Summary.")

[29] See NSA Report: Sec. I, "Introduction and Summary."

Watch List, again without warrant or the approval of the Attorney General.[30]

The legal standards and procedures regulating the use of microphone surveillance have traditionally been even more lax than those regulating the use of wiretapping. The first major Supreme Court decision on microphone surveillance was *Goldman* v. *United States*, 316 U.S. 129 (1942), which held that such surveillance in a criminal case was constitutional when the installation did not involve a trespass. Citing this case, Attorney General McGrath prohibited the trespassory use of this technique by the FBI in 1952.[31] But two years later—a few weeks after the Supreme Court denounced the use of a microphone installation in a criminal defendant's bedroom [32]—Attorney General Brownell gave the FBI sweeping authority to engage in bugging for intelligence purposes. ". . . (C)onsiderations of internal security and the national safety are paramount," he wrote, "and, therefore, may compel the unrestricted use of this technique in the national interest." [33]

Since Brownell did not require the prior approval of the Attorney General for bugging specific targets, he largely undercut the policy that had developed for wiretapping. The FBI in many cases could obtain equivalent coverage by utilizing bugs rather than taps and would not be burdened with the necessity of a formal request to the Attorney General.

The vague "national interest" standards established by Brownell, and the policy of not requiring the Attorney General's prior approval for microphone installations, continued until 1965, when the Justice Department began to apply the same criteria and procedures to both microphone and telephone surveillance.

3. Ignoring the Prohibitions Against Warrantless Mail Opening and Surreptitious Entries

Warrantless mail opening and surreptious entries, unlike the use of informants and electronic surveillance, have been clearly prohibited by both statutory and constitutional law. In violation of these prohibitions, the FBI and the CIA decided on their own when and how these techniques should be used.[35]

Sections 1701 through 1973 of Title 18 of the United States Code forbid persons other than employees of the Postal Service "dead letter" office from tampering with or opening mail that is not addressed to them. Violations of these statutes may result in fines of up to $2000

[30] Memorandum from Iredell to Gayler, 4/10/70; See NSA Report: Sec. I, Introduction and Summary. BNDD originally requested NSA to monitor the South American link because it did not believe it had authority to wiretap a few public telephones in New York City from which drug deals were apparently being arranged. (Iredell testimony, 9/18/75, p. 99.)

[31] Memorandum from the Attorney General to Mr. Hoover, 2/26/52.

[32] *Irvine* v. *California*, 347 U.S. 128 (1954).

[33] Memorandum from the Attorney General to the Director, FBI, 5/20/54.

[35] While such techniques might have been authorized by Attorneys General under expansive "internal security" or "national interest" theories similar to Brownell's authorization for installing microphones by trespass, the issue was never presented to them for decision before 1967, when Attorney General Ramsey Clark turned down a surreptitious entry request. There is no indication that the legal questions were considered in any depth in 1970 or 1971 at the time of the "Huston Plan" and its aftermath. See Huston Plan Report: Sec. III, Who, What, When and Where.

and imprisonment for not more than five years. The Supreme Court has also held that both First Amendment and Fourth Amendment restrictions apply to mail opening.

The Fourth Amendment concerns were articulated as early as 1878, when the Court wrote:

> The constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be. Whilst in the mail, they can only be opened and examined under like warrant . . . as is required when papers are subjected to search in one's own household.[36]

This principle was reaffirmed as recently as 1970 in *United States* v. *Van Leeuwen*, 396 U.S. 249 (1970). The infringement of citizens' First Amendment rights resulting from warrantless mail opening was first recognized by Justice Holmes in 1921. "The use of the mails," he wrote in a dissent now embraced by prevailing legal opinion, "is almost as much a part of free speech as the right to use our tongues." [37] This principle, too, has been affirmed in recent years.[38]

Breaking and entering is a common law felony as well as a violation of state and federal statutes. When committed by Government agents, it has long been recognized as "the chief evil against which the wording of the Fourth Amendment is directed." [39]

In the one judicial decision concerning the legality of warrantless "national security" break-ins for physical search purposes, United States District Court Judge Gerhard Gesell held such entries unconstitutional. This case, *United States* v. *Ehrlichman*,[40] involved an entry into the office of a Los Angeles psychiatrist, Dr. Lewis Fielding, to obtain the medical records of his client Daniel Ellsberg, who was then under federal indictment for revealing classified documents. The entry was approved by two Presidential assistants, John Ehrlichman and Charles Colson, who argued that it had been justified "in the national interest." Ruling on the defendants' discovery motions, Judge Gesell found that because no search warrant was obtained:

> The search of Dr. Fielding's office was clearly illegal under the unambiguous mandate of the Fourth Amendment. . . [T]he Government must comply with the strict constitutional and statutory limitations on trespassory searches and arrests even when known foreign agents are involved.... To hold otherwise, except under the most exigent circumstances, would be to abandon the Fourth Amendment to the whim of the Executive in total disregard of the Amendment's history and purpose.[41]

---

[36] *Ex Parte Jackson*, 96, U.S. 727, 733 (1878).

[37] *Milwaukee Pub. Co.* v. *Burleson*, 255 U.S. 407, 437 (1921) (dissent).

[38] See *Lamont* v. *Postmaster General*, 381 U.S. 301 (1965); *Procunier* v. *Martinez*, 416 U.S. 396 (1975).

[39] *United States* v. *United States District Court*, 407 US 297, 313 (1972).

[40] 376 F. Supp. 29, (D.D.C. 1974).

[41] 376 F. Supp. at 33.

In the appeal of this decision, the Justice Department has taken the position that a physical search may be authorized by the Attorney General without a warrant for "foreign intelligence" proposes.[42] The warrantless mail opening programs and surreptitious entries by the FBI and CIA did not even conform to the "foreign intelligence" standard, however, now were they specifically approved in each case by the Attorney General. Domestic "subversives" and "extremists" were targeted for mail opening; and domestic "subversives" and "White Hate groups" were among those targeted for surreptitious entries.[43] Until the Justice Department's recent statement in the Ehrlichman case, moreover, no legal justification had ever been advanced publicly for violating the statutory or constitutional prohibitions against physical searches or opening mail without a judicial warrant, and none has ever been officially advanced by any Administration to justify warrantless mail openings.

Subfinding (b)

In addition to providing the means by which the Government can collect too much information about too many people, certain techniques have their own peculiar dangers:

(i) Informants have provoked and participated in violence and other illegal activities in order to maintain their cover, and they have obtained membership lists and other private documents.

(ii) Scientific and technological advances have rendered obsolete traditional controls on electronic surveillance obsolete and have made it more difficult to limit intrusions. Because of the nature of wiretaps, microphones, and other sophisticated electronic techniques, it has not always been possible to restrict the monitoring of communications to the persons being investigated.

a. The Intrusive Nature of the Intelligence Informant Technique

The FBI employs two types of informants: (1) "intelligence informants" who are used to report on groups and individuals in the course of intelligence investigations, and (2) "criminal informants," who are used in connection with investigations of specific criminal activity. FBI intelligence informants are administered by the FBI Intelligence Division at Bureau headquarters through a centralized system that is separate from the administrative system for FBI criminal informants. For example, the FBI's large-scale Ghetto Informant Program was administered by the FBI Intelligence Division. The Committee's investigation centered on the use of FBI intelligence informants. The FBI's criminal informant program fell outside the scope of the Committee's mandate, and accordingly it was not examined.

The Committee recognizes that FBI intelligence informants in violent groups have sometimes played a key role in the enforcement of

---

[42] Letter from Acting Assistant Attorney General John C. Keeny to Hugh E. Kline, Clerk of the U.S. Court of Appeals for the District of Columbia, 5/9/75.

[43] The Supreme Court's decision in *United States* v. *United States District Court*, 407 U.S. 297 (1972), clearly established the principle that such warrantless invasions of the privacy of Americans are unconstitutional.

the criminal law. The Committee examined a number of such cases,[44] and in public hearings on the use of FBI intelligence informants included the testimony of a former informant in the Ku Klux Klan whose reporting and court room testimony was essential to the arrest and conviction of the murderers of Mrs. Viola Liuzzo, a civil rights worker killed in 1965.[45] Former Attorney General Katzenbach testified that informants were vital to the solution of the murders of three civil rights workers killed in Mississippi in 1964.[46]

FBI informant coverage of the Women's Liberation Movement resulted in intensive reporting on the identities and opinions of women who attended WLM meetings. For example, the FBI's New York Field Office summarized one informant's report in a memorandum to FBI Headquarters:

> Informant advised that a WLM meeting was held on ----------.[47] Each woman at this meeting stated why she had come to the meeting and how she felt oppressed, sexually or otherwise.
>
> According to this informant, these women are mostly concerned with liberating women from this "oppressive society." They are mostly against marriage, children, and other states of oppression caused by men. Few of them, according to the informant, have had political backgrounds.[48]

Individual women who attended WLM meetings at midwestern universities were identified by FBI intelligence informants. A report by the Kansas City FBI Field Office stated:

> Informant indicates members of Women's Liberation campus group who are now enrolled as students at University of Missouri, Kansas City, are ---------, ---------, ---------, ---------, ---------.[49] Informant noted that ---------, and ---------,[50] not currently students on the UMKC campus are reportedly roommates at ----------.[51]

---

[44] In one case, an FBI informant involved in an intelligence investigation of the Detroit Black Panther Party furnished advance information regarding a planned ambush of Detroit police officers which enabled the Detroit Police Department to take necessary action to prevent injury or death to the officers and resulted in the arrest of eight persons and the seizure of a cache of weapons. The informant also furnished information resulting in the location and confiscation by Bureau agents of approximately fifty sticks of dynamite available to the Black Panther Party which likely resulted in the saving of lives and the prevention of property damage. (Joseph Deegan testimony, 2/13/76, p. 54)

[45] Rowe, 12/2/75, Hearings, Vol. 6, p. 115.

[46] Katzenbach testified that the case "could not have been solved without acquiring informants who were highly placed members of the Klan." (Katzenbach, 12/3/75, Hearings, Vol. 6, p. 215.)

[47] Date and address deleted at FBI request so as not to reveal informant's identity.

[48] Memorandum, from New York Field Office to FBI Headquarters, re: Women's Liberation Movement, 5/28/69, p. 2.

[49] Names deleted for security reasons.

[50] Names deleted for security reasons.

[51] Names and addresses deleted for security reasons.

Informants were instructed to report "everything" they knew about a group to the FBI.

> . . . to go to meetings, write up reports . . . on what happened, who was there . . . to try to totally identify the background of every person there, what their relationships were, who they were living with, who they were sleeping with, to try to get some sense of the local structure and the local relationships among the people in the organization.[52]

Another intelligence informant described his mission as "total reporting." Rowe testified that he reported "anything and everything I observed or heard" pertaining to any member of the group he infiltrated.[53]

Even where intelligence informants are used to infiltrate groups where some members are suspected of violent activity, the nature of the intelligence mission results in governmental intrusion into matters irrelevant to that inquiry. The FBI Special Agents who directed an intelligence informant in the Ku Klux Klan testified that the informant

> . . . furnished us information on the meetings and the thoughts and feelings, intentions and ambitions, as best he knew them, of other members of the Klan, both the rank and file and the leadership.[54]

Intelligence informants also report on other groups—not the subject of intelligence investigations—which merely associate with, or are even opposed to, the targeted group. For example, an FBI informant in the VVAW had the following exchange with a member of the Committee:

> Senator HART (Mich.). . . . did you report also on groups and individuals outside the [VVAW], such as other peace groups or individuals who were opposed to the war whom you came in contact with because they were cooperating with the [VVAW] in connection with protest demonstrations and petitions?
>
> Ms. COOK. . . . I ended up reporting on groups like the United Church of Christ, American Civil Liberties Union, the National Lawyers Guild, liberal church organizations [which] quite often went into coalition with the VVAW.[55]

This informant reported the identities of an estimated 1,000 individuals to the FBI, although the local chapter to which she was assigned had only 55 regular members.[56] Similarly, an FBI informant in the Ku Klux Klan reported on the activities of civil rights and black groups that he observed in the course of his work in the Klan.[57]

In short, the intelligence informant technique is not a precise instrument. By its nature, it extends far beyond the sphere of proper govern-

[52] Cook, 12/2/75, Hearings, Vol. 6, p. 111.
[53] Rowe, 12/2/75, Hearings, Vol. 6, p. 116.
[54] Special Agent, 11/21/75, p. 7.
[55] Cook, 12/2/75, Hearings, Vol. 6, pp. 119, 120.
[56] Cook, 12/2/75, Hearings, Vol. 6, p. 120.
[57] Rowe, 12/2/75, Hearings, Vol. 6, p. 116.

mental interest and risks governmental monitoring of the private lives and the constitutionally-protected activity of Americans. Nor is the intelligence informant technique used infrequently. As reflected in the statistics described above, FBI intelligence investigations are in large part conducted through the use of informants; and FBI agents are instructed to "develop reliable informants at all levels and in all segments" of groups under investigation.[58]

b. Other Dangers in the Intelligence Informant Technique

In the absence of clear guidelines for informant conduct, FBI paid and directed intelligence informants have participated in violence and other illegal activities and have taken membership lists and other private documents.

1. Participation in Violence and Other Illegal Activity

The Committee's investigation has revealed that there is often a fundamental dilemma in the use of intelligence informants in violent organizations. The Committee recognizes that intelligence informants in such groups have sometimes played essential roles in the enforcement of the criminal law. At the same time, however, the Committee has found that the intelligence informant technique carries with it the substantial danger that informants will participate in, or provoke, violence or illegal activity. Intelligence informants are frequently infiltrated into groups for long-term reporting rather than to collect evidence for use in prosecutions. Consequently, intelligence informants must participate in the activity of the group they penetrate to preserve their cover for extended periods. Where the group is involved in violence or illegal activity, there is a substantial risk that the informant must also become involved in this activity. As an FBI Special Agent who handled an intelligence informant in the Ku Klux Klan testified: "[you] couldn't be an angel and be a good informant."[59]

FBI officials testified that it is Bureau practice to instruct informants that they are not to engage in violence or unlawful activity and, if they do so, they may be prosecuted. FBI Deputy Associate Director Adams testified:

> . . . we have informants who have gotten involved in the violation of the law, and we have immediately converted their status from an informant to the subject, and have prosecuted, I would say, offhand . . . around 20 informants.[60]

The Committee finds, however, that the existing guidelines dealing with informant conduct do not adequately ensure that intelligence informants stay within the law in carrying out their assignments. The FBI Manual of Instructions contain no provisions governing informant conduct. While FBI employee conduct regulations prohibit an FBI agent from directing informants to engage in violent or other illegal activity, informants themselves are not governed by these regulations since the FBI does not consider them as FBI employees.

[58] FBI Manual, Section 107 c(3).
[59] Special Agent, 11/21/75, p. 12.
[60] Adams, 12/2/75, Hearings, Vol. 6, p. 150.

In the absence of clear and precise written provisions directly applicable to informants, FBI intelligence informants have engaged in violent and other illegal activity. For example, an FBI intelligence informant who penetrated the Ku Klux Klan and reported on its activities for over five years testified that on a number of occassions he and other Klansmen had "beaten people severely, had boarded buses and kicked people off; had went in restaurants and beaten them with blackjacks, chains, pistols." [61] This informant described how he had taken part in Klan attacks on Freedom Riders at the Birmingham, Alabama, bus depot, where "baseball bats, clubs, chains and pistols" were used in beatings.[62]

Although the FBI Special Agents who directed this informant instructed him that he was not to engage in violence, it was recognized that there was a substantial risk that he would become a participant in violent activity.

As one of the Agents testified:

> . . . it is kind of difficult to tell him that we would like you to be there on deck, observing, be able to give us information and still keep yourself detached and uninvolved and clean, and that was the problem that we constantly had.[63]

In another example, an FBI intelligence informant penetrated "right wing" groups operating in California under the names "The Minutemen" and "The Secret Army Oroganization." The informant reported on the activities of these "right wing" paramilitary groups for a period of five years but was also involved in acts of violence or destruction. In addition, the informant actually rose to a position of leadership in the SAO and became an innovator of various harassment actions. For example, he admittedly participated in firebombing of an automobile and was present, conducting a "surveillance" of a professor at San Diego State University, when his associate and subordinate in the SAO took out a gun and fired into the home of the professor, wounding a young woman.[64]

An FBI intelligence informant in a group of antiwar protesters planning to break into a draft board claimed to have provided technical instruction and materials that were essential to the illegal break- testified to the committee:

> Everything they learned about breaking into a building or climbing a wall or cutting glass or destroying lockers, I taught them. I got sample equipment, the type of windows that we would go through, I picked up off the job and taught them how to cut the glass, how to drill holes in the glass so you cannot hear it and stuff like that, and the FBI supplied me with the equipment needed. The stuff I did not have, the [the FBI] got off their own agents.[65]

The Committee finds that where informants are paid and directed by a government agency, the government has a responsibility to

[61] Rowe deposition, 10/17/75, p. 12.
[62] Rowe, 12/2/75, Hearings, Vol. 6, p. 118.
[63] Special Agent, 11/21/75, pp. 16–17.
[64] Memorandum from the FBI to Senate Select Committee, 2/26/76, with enclosures.
[65] Hardy, 9/29/75, pp. 16–17.

impose clear restrictions on their conduct. Unwritten practice or general provisions aimed at persons other than the informants themselves are not sufficient. In the investigation of violence or illegal activity, it is essential that the government not be implicated in such activity.

2. Membership Lists and Other Private Documents Obtained by the Government Through Intelligence Informants

The Committee finds that there are inadequate guidelines to regulate the conduct of intelligence informants with respect to private and confidential documents, such as membership lists, mailing lists and papers relating to legal matters. The Fourth Amendment provides that citizens shall be "secure in their . . . papers and effects, against unreasonable searches and seizures" and requires probable cause to believe there has been a violation of law before a search warrant may issue. Moreover the Supreme Court, in *NAACP* v. *Alabama*,[66] held that the First Amendment's protections of speech, assembly and group association did not permit a state to compel the production of the membership list of a group engaged in lawful activity. The Court distinguished the case where a state was able to demonstrate a "controlling justification" for such lists by showing a group's activities involved "acts of unlawful intimidation and violence." [66a]

There are no provisions in the FBI Manual which preclude the FBI from obtaining private and confidential documents through intelligence informants. The Manual does prohibit informant reporting of "any information pertaining to defense plans or strategy," but the FBI interprets this as applying only to privileged communications between an attorney and client in connection with a specific court proceeding.[67]

The Committee's investigation has shown that, the FBI, through its intelligence informants and sources, has sought to obtain membership lists and other confidential documents of groups and individuals.[68] For example, one FBI Special Agent testified:

> I remember one evening . . . [an informant] called my home and said I will meet you in a half an hour . . . I have a complete list of everybody that I have just taken out of the files, but I have to have it back within such a length of time.
>
> Well, naturally I left home and met him and had the list duplicated forthwith, and back in his possession and back in the files with nobody suspecting." [69]

Similarly, the FBI Special Agent who handled an intelligence informant in an antiwar group testified that he obtained confidential papers of the group which related to legal defense matters:

> "She brought back several things . . . various position papers taken by various legal defense groups, general statements of . . . the VVAW, legal thoughts on various trials, the

---

[66] 357 U.S. 449 (1958). Similarly, in *Bates* v. *City of Little Rock*, 361 U.S. 516 (1960), the Supreme Court held compulsory disclosure of group membership lists was an unjustified interference with members' freedom of association.

[66a] 361 U.S. at 465.

[67] FBI Manual of Instructions, Section 107.

[68] Surreptitious entry has also provided a means for the obtaining of such lists and other confidential documents.

[69] Special Agent, 11/19/75, pp. 10–11.

Gainesville (Florida) 8 . . . the Camden (New Jersey) 9 . . . various documents from all of these groups." [70]

This informant also testified that she took the confidential mailing list of the group she had penetrated and gave it to the FBI.[71]

She also gave the FBI a legal manual prepared by the group's attorneys to guide lawyers in defending the group's members should they be arrested in connection with antiwar demonstrations or other political activity.[72] Since this document was prepared as a general legal reference manual rather than in connection with a specific trial the FBI considered it outside the attorney-client privilege and not barred by the FBI Manual provision with respect to legal defense and strategy matters.

For the government to obtain membership lists and other private documents pertaining to lawful and protected activities covertly through intelligence informants risks infringing rights guaranteed by the Constitution. The Committee finds that there is a need for new guidelines for informant conduct with respect to the private papers of groups and individuals.

c. Electronic Surveillance

In the absence of judicial warrant, both the "traditional" forms of electronic surveillance practiced by the FBI—wiretapping and bugging—and the highly sophisticated form of electronic monitoring practiced by NSA have been used to collect too much information about too many people.

1. Wiretapping and Bugging

Wiretaps and bugs are considered by FBI officials to be one of the most valuable techniques for the collection of information relevant to the Bureau's legitimate foreign counterintelligence mandate. W. Raymond Wannall, the former Assistant Director in charge of the FBI's Intelligence Division, stated that electronic surveillance assisted Bureau officials in making "decisions" as to operations against foreigners engaged in espionage. "It gives us leads as to persons . . . hostile intelligence services are trying to subvert or utilize in the United States, so certainly it is a valuable technique." [73]

Despite its stated value in foreign counterintelligence cases, however, the dangers inherent in its use imply a clear need for rigorous controls. By their nature, wiretaps and bugs are incapable of a surgical precision that would permit intelligence agencies to overhear only the target's conversations. Since wiretaps are placed on particular telephones, anyone who uses a tapped phone—including members of the target's family—can be overheard. So, too, can everyone with whom the target (or anyone else using the target's telephone) communicates.[74] Microphones planted in the target's room or office inevitably intercept all conversations in a particular area: anyone conferring in the room or office, not just the target, is overheard.

---

[70] Special Agent, 11/20/75, pp. 15–16.

[71] Cook, 12/2/75, Hearings, Vol. 6, p. 112.

[72] *Cook deposition*, 10/14/75, p. 36.

[73] W. Raymond Wannall testimony, 10/21/75, p. 21.

[74] Under the Justice Department's procedures for Title III (court-ordered) wiretaps, however, the monitoring agent is obligated to turn off the recording equipment when certain privileged communications begin. Manual for conduct of Electronic Surveillance under Title III of Public Law 90–351, Sec. 8.1.

The intrusiveness of these techniques has a second aspect as well. It is extremely difficult, if not impossible, to limit the interception to conversations that are relevant to the purposes for which the surveillance is placed. Virtually all conversations are overheard, no matter how trivial, personal, or political they might be. When the electronic surveillance target is a political figure who is likely to discuss political affairs, or a lawyer, who confers with his clients, the possibilities for abuse are obviously heightened.

The dangers of indiscriminate interception are perhaps most acute in the case of microphones planted in locations such as bedrooms. When Attorney General Herbert Brownell gave the FBI sweeping authority to engage in microphone surveillances for intelligence purposes in 1954, he expressly permitted the Bureau to plant microphones in such locations if, in the sole discretion of the FBI, the facts warranted the installation.[75] Acting under this general authority, for example, the Bureau installed no fewer than twelve bugs in hotel rooms occupied by Dr. Martin Luther King, Jr.[76]

The King surveillances which occurred between January 1964 and October 1965, were ostensibly approved within the FBI for internal security reasons, but they produced vast amounts of personal information that were totally unrelated to any legitimate governmental interest; indeed, a single hotel room bug alone yielded twenty reels of tape that subsequently provided the basis for the dissemination of personal information about Dr. King throughout the Federal establishment.[76a] Significantly, FBI internal memoranda with respect to some of the installations make clear that they were planted in Dr. King's hotel rooms for the express purpose of obtaining personal information about him.[77]

Extremely personal information about the target, his family, and his friends, is easily obtained from wiretaps as well as microphones. This fact is clearly illustrated by the warrantless electronic surveillance of an American citizen who was suspected of leaking classified data to the press. A wiretap on this individual produced no evidence that he had in fact leaked any stories or documents, but among the items of information that the FBI did obtain from the tap (and delivered in utmost secrecy to the White House) were the following: that "meat was ordered [by the target's family] from a grocer;" that the target's daughter had a toothache; that the target needed grass clippings for a compost heap he was building; and that during a telephone conversation between the target's wife and a friend the "matters discussed were milk bills, hair, soap operas, and church." [78]

---

[75] Memorandum from the Attorney General to the Director, FBI, 5/20/54.

[76] Three additional bugs were planted in Dr. King's hotel rooms in 1965 after the standards for wiretapping and microphone surveillance became identical. According to FBI memoranda, apparently initiated by Katzenbach, Attorney General Nicholas Katzenbach was given after the fact notification that these three surveillances of Dr. King had occurred. See p. 273, and the King Report, Sec. IV, for further details.

[76a] Memorandum from F. J. Baumgardener to W. C. Sullivan, 3/26/64.

[77] For example, memorandum from Baumgardner to W. C. Sullivan, 2/4/64.

[78] FBI memoranda. Identifying details are being withheld by the Select Committee because of privacy considerations. Even the FBI realized that this type of information was unrelated to criminal activity or national security: for the last four months of this surveillance, most of the summaries that were disseminated to the White House began, "The following is a summary of nonpertinent information concerning captioned individual as of . . ."

The so-called "seventeen" wiretaps on journalists and government employees, which collectively lasted from May 1969 to February 1971, also illustrate the intrusiveness of electronic surveillance. According to former President Nixon, these taps produced "just gobs of material: gossip and bull." [79] FBI summaries of information obtained from the wiretaps and disseminated to the White House, suggest that the former President's private evaluation of them was correct. This wiretapping program did not reveal the source of any leaks of classified data, which was its ostensible purpose, but it did generate a wealth of information about the personal lives of the targets—their social contacts, their vacation plans, their employment satisfactions and dissatisfaction, their marital problems, their drinking habits, and even their sex lives.[80]

Among those who were incidentally overheard on one of these wiretaps was a currently sitting Associate Justice of the Supreme Court of the United States, who made plans to review a manuscript written by one of the targets.[81] Vast amounts of political information were also obtained from these wiretaps.[82]

The "seventeen" wiretaps also exemplify the particularly acute problems of wiretapping when the targeted individuals are involved in the domestic political process. These wiretaps produced vast amounts of purely political information,[82] much of which was obtained from the home telephones of two consultants to Senator Edmund Muskie and other Democratic politicians.

The incidental collection of political information from electronic surveillance is also shown by a series of telephone and microphone surveillances conducted during the Kennedy administration. In an investigation of the possibly unlawful attempts of representatives of a foreign country to influence congressional deliberations about sugar quota legislation in the early 1960s, Attorney General Robert Kennedy authorized a total of twelve warrantless wiretaps on foreign and domestic targets. Among the wiretaps of American citizens were two on American lobbyists, three on executive branch officials, and two on a staff member of a House of Representatives' Committee.[83] A bug was also planted in the hotel room of a United States Congressman, the Chairman of the House Agriculture Committee, Harold D. Cooley.[84]

Although this investigation was apparently initiated because of the Government's concern about future relations with the foreign country involved and the possibility of bribery,[85] it is clear that the Ken-

[79] Transcript of Presidential Tapes, 2/28/73 (House Judiciary Committee Statement of Information, Book VII, Part 4, p. 1754).

[80] For example, letters from Hoover to the Attorney General, 7/25/69, and 7/31/69; letters from Hoover to H. R. Haldeman, 6/25/70.

[81] Letter from Hoover to Haldeman, 6/25/70.

[82] Examples of such information are listed in the finding on Political Abuse, "The '17' wiretaps."

[83] Memorandum from J. Edgar Hoover to the Attorney General, 2/14/61; Memorandum from J. Edgar Hoover to the Attorney General, 2/16/61; Memorandum from J. Edgar Hoover to the Attorney General, 6/26/62; Memorandum from Wannall to W. C. Sullivan, 12/22/66.

[84] Memorandum from D. E. Moore to A. H. Belmont, 2/16/61.

[85] Memorandum from W. R. Wannall to W. C. Sullivan, 12/22/66; Memorandum from A. H. Belmont to Mr. Parsons, 2/14/61. This investigation did discover that representatives of a foreign nation were attempting to influence Congressional deliberations, but it did not reveal that money was being passed to any member of Congress or Congressional staff aide.

nedy administration was politically interested in the outcome of the sugar quota legislation as well.[86] Given the nature of the techniques used and of the targets they were directed against, it is not surprising that a great deal of potentially useful political information was generated from these "Sugar Lobby" surveillances.[87]

The highly intrusive nature of electronic surveillance also raises special problems when the targets are lawyers and journalists. Over the past two decades there have been a number of wiretaps placed on the office telephones of lawyers.[88] In the Sugar Lobby investigation, for example, Robert Kennedy authorized wiretaps on ten telephone lines of a single law firm.[90] All of these lines were apparently used by the one lawyer who was a target and presumably by other attorneys in the firm as well. Such wiretaps represent a serious threat to the attorney-client privilege, because once they are instituted they are capable of detecting all conversations between a lawyer and his clients, even those relating to pending criminal cases.

Since 1960, at least six American journalists and newsmen have also been the targets of warrantless wiretaps or bugs.[91] These surveillances were all rationalized as necessary to discover the source of leaks of classified information, but, since wiretaps and bugs are indiscriminate in the types of information collected, some of these taps revealed the attitudes of various newsmen toward certain politicians and supplied advance notice of forthcoming newspaper and magazine articles dealing with administration policies. The collection of information such as this, and the precedent set by wiretapping of newsmen, generally, inevitably tends to undermine the constitutional guarantee of a free and independent press.

2. NSA Monitoring

The National Security Agency (NSA) has the capability to monitor almost any electronic communication which travels through the air. This means that NSA is capable of intercepting a telephone call or even a telegram, if such call or telegram is transmitted at least partially through the air. Radio transmissions, *a fortiori*, are also within NSA's reach.

Since most communications today—to an increasing extent even domestic communications—are, at some point, transmitted through the air, NSA's potential to violate the privacy of American citizens is unmatched by any other intelligence agency. Furthermore, since the interception of electronic signals entails neither the installation of electronic surveillance devices nor the cooperation of private communications companies, the possibility that such interceptions will be undetected is enhanced.

NSA has never turned its monitoring apparatus upon entirely domestic communications, but from the early 1960s until 1973, it did inter-

[86] Memorandum from Wannall to W. C. Sullivan, 12/22/66.

[87] See Finding on Political Abuse, p. 233.

[88] Electronic Surveillance Report: Sec. II, "Presidential and Attorney General Authorization."

[90] Memorandum from J. Edgar Hoover to the Attorney General, 6/26/62.

[91] Memorandum from J. Edgar Hoover to the Attorney General 6/29/61; memorandum from J. Edgar Hoover to the Attorney General 7/31/62; memorandum from J. Edgar Hoover to the Attorney General 4/19/65; memorandum from J. Edgar Hoover to the Attorney General 6/4/69; memorandum from J. Edgar Hoover to the Attorney General 9/10/69; letter from W. C. Sullivan to J. Edgar Hoover 7/2/69.

cept the international communications of American citizens, without a warrant, at the request of other federal agencies.

Under current practice, NSA does not target any American citizen or firm for the purpose of intercepting their foreign communications. As a result of monitoring international links of communication, however, it does acquire an enormous number of communications to, from, or about American citizens and firms.[93]

As a practical matter, most of the communications of American citizens or firms acquired by NSA as incidental to its foreign intelligence-gathering process are destroyed upon recognition as a communication to or from an American citizen. But other such communications, which bear upon NSA's foreign intelligence requirements, are processed, and information obtained from them are used in NSA's reports to other intelligence agencies. Current practice precludes NSA from identifying American citizens and firms by name in such reports. Nonetheless, the practice does result in NSA's disseminating information derived from the international communications of American citizens and firms to the intelligence agencies and policymakers in the federal government.

In his dissent in *Olmstead* v. *United States*,[94] which held that the Fourth Amendment warrant requirement did not apply to the seizure of conversations by means of wiretapping, Justice Louis D. Brandeis expressed grave concern that new technologies might outstrip the ability of the Constitution to protect American citizens. He wrote:

> Subtler and more far-reaching means of invading privacy have become available to the government . . . (and) the progress of science in furnishing the Government with means of espionage is not likely to stop with wiretapping. Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home . . . . Can it be that the Constitution affords no protection against such invasions of individual security?

The question posed by Justice Brandeis applies with obvious force to the technological developments that allow NSA to monitor an enormous number of communications each year. His fears were firmly based, for in fact no warrant was ever obtained for the inclusion of 1200 American citizens on NSA's "Watch List" between the early 1960s and 1973, and none is obtained today for the dissemination within the intelligence community of information derived from the international communications of American citizens and firms. In the face of this new technology, it is well to remember the answer Justice Brandeis gave to his own question. Quoting from *Boyd* v. *United States*, 116 U.S. 616, he wrote:

> It is not the breaking of his doors, and the rummaging of his drawers that constitutes the essense of the offense; but it is the invasion of his indefeasible right of personal security, personal liberty, and private property . . .[94a]

[93] NSA has long asserted that it had the authority to do this so long as one of the parties to such communication was located in a foreign country.

[94] 277 U.S. 438, 473–474 (1928).

[94a] 277 U.S. at 474–475.

D. Mail Opening

By ignoring the legal prohibitions against warrantless mail opening, the CIA and the FBI were able to obtain access to the written communications of hundreds of thousands of individuals, a large proportion of whom were American citizens. The intercepted letters were presumably sealed with the expectation that they would only be opened by the party to whom they were addressed, but intelligence agents in ten cities throughout the United States surreptitiously opened the seal and photographed the entire contents for inclusion in their intelligence files.

Mail opening is an imprecise technique. In addition to relying on a "Watch List" of names, the CIA opened vast numbers of letters on an entirely random basis; as one agent who opened mail in the CIA's New York project testified, "You never knew what you would hit." [95] Given the imprecision of the technique and the large quantity of correspondence that was opened, it is perhaps not surprising that during the twenty year course of the Agency's New York project, the mail that was randomly opened included that of at least three United States Senators and a Congressman, one Presidential Candidate, and numerous educational, business, and civil rights leaders.[96]

Several of the FBI programs utilized as selection criteria certain "indicators" on the outside of envelopes that suggested that the communication might be to or from a foreign espionage agent. These "indicators" were more refined than the "shotgun approach" [97] which characterized the CIA's New York project, and they did lead to the identification of three foreign spies.[98] But even by the Bureau's own accounting, it is clear that the mail of hundreds of innocent American citizens was opened and read for every successful counterintelligence lead that was obtained by means of "indicators." [99]

Large volumes of mail were also intercepted and opened in other FBI mail programs that were based not on indicators but on far less precise criteria. Two programs that involved the opening of mail to and from an Asian country, for example, used "letters to or from a university, scientific, or technical facility" as one selection criterion.[100] According to FBI memoranda, an average of 50 to 100 letters per day was opened and photographed during the ten years in which one of these two programs operated.[101]

[95] "CIA Officer" testimony, 9/30/75, p. 15.

[96] Staff summary of "Master Index." review, 9/5/75.

[97] James Angelton testimony, 9/17/75, p. 28.

[98] Wannall, 10/21/75, p. 5.

[99] In one of the programs based on "indicators" a participating agent testified that he opened 30 to 60 letters each day. (FBI agent statement, 9/10/75, p. 23.) In a second such program, a total of 1,011 letters were opened in one of the six cities in which it operated; statistics on the number of letters opened in the other five cities cannot be reconstructed. (W. Raymond Wannall testimony, 10/21/75, p. 5.) In a third such project, 2,350 letters were opened in one city and statistics for the other two cities in which it operated are unavailable. (Memorandum from W. A. Branigan to W. C. Sullivan, 8/31/61; Memorandum from Mr. Branigan to Mr. Sullivan, 12/21/61; memorandum from New York Field Office to FBI Headquarters, 3/5/62.)

[100] Letter from the FBI to the Senate Select Committee, 10/29/75. Six other criteria were used in these programs. See Mail Opening Report, Sec. IV.

[101] Memorandum from S. B. Donohoe to A. H. Belmont, 2/23/61: Memorandum from San Francisco Field Office to FBI Headquarters, 3/11/60. Statistics relating to the number of letters opened in the other program which used this criterion cannot be reconstructed.

E. Surreptitious Entries

Surreptitious entries, conducted in violation of the law, have also permitted intelligence agencies to gather a wide range of information about American citizens and domestic organization as well as foreign targets.[102] By definition this technique involves a physical entry into the private premises of individuals and groups. Once intelligence agents are inside, no "papers or effects" are secure. As the Huston Plan recommendations stated in 1970, "It amounts to burglary."[103]

The most private documents are rendered vulnerable by the use of surreptitious entries. According to a 1966 internal FBI memorandum, which discusses the use of this technique against domestic organizations:

> [The FBI has] on numerous occasions been able to obtain material held highly secret and closely guarded by subversive groups and organizations which consisted of membership lists and mailing lists of these organizations.[104]

A specific example cited in this memorandum also reveals the types of information that this technique can collect and the uses to which the information thus collected may be put:

> Through a "black bag" job, we obtained the records in the possession of three high-ranking officials of a Klan organization. . . . These records gave us the complete membership and financial information concerning the Klan's operation which we have been using most effectively to disrupt the organization and, in fact, to bring about its near disintegration.[105]

Unlike techniques such as electronic surveillance, government entries into private premises were familiar to the Founding Fathers. "Indeed," Judge Gesell wrote in the *Ehrlichman* case, "the American Revolution was sparked in part by the complaints of the colonists against the issuance of writs of assistance, pursuant to which the King's revenue officers conducted unrestricted, indiscriminate searches of persons and homes to uncover contraband."[106] Recognition of the intrusiveness of government break-ins was one of the primary reasons

---

[102] According to the FBI, "there were at least 239 surreptitious entries (for purposes other than microphone installation) conducted against at least fifteen domestic subversive targets from 1942 to April 1968. . . . In addition, at least three domestic subversive targets were the subject of numerous entries from October 1952 to June 1966." (FBI memorandum to the Senate Select Committee, 10/13/76.) One target, the Socialist Workers Party, was the subject of possibly as many as 92 break-ins by the FBI, between 1960 and 1966 alone. The home of at least one SWP member was also apparently broken into. (Sixth Supplementary Response to Requests for Production of Documents of Defendant, Director of the FBI, *Socialist Workers Party* v. *Attorney General*, 73 Civ. 3160, (SDNY), 3/24/76.) An entry against one "white hate group" was also reported by the FBI. (Memorandum from FBI Headquarters to the Senate Select Committee, 10/13/75.)

[103] Memorandum from Tom Huston to H. R. Haldeman, 7/70, p. 3.

[104] Memorandum from W. C. Sullivan to C. D. DeLoach, 7/19/66.

[105] Ibid.

[106] *United States* v. *Ehrlichman*, 376 F. Supp. 29, 32 (D.D.C. 1974).

for the subsequent adoption of the Fourth Amendment in 1791,[107] and this technique is certainly no less intrusive today.

Subfunding (c)

The imprecision and manipulation of labels such as "national security," "domestic security," "subversive activities" and "foreign intelligence" have led to unjustified use of these techniques.

Using labels such as "national security" and "foreign intelligence", intelligence agencies have directed these highly intrusive techniques against individuals and organizations who were suspected of no criminal activity and who posed no genuine threat to the national security. In the absence of precise standards and effective outside control, the selection of American citizens as targets has at times been predicated on grounds no more substantial than their lawful protests or their non-conformist philosophies. Almost any connection with any perceived danger to the country has sufficed.

The application of the "national security" rationale to cases lacking a substantial national security basis has been most apparent in the area of warrantless electronic surveillance. Indeed, the unjustified use of wiretaps and bugs under this and related labels has a long history. Among the wiretaps approved by Attorney General Francis Biddle under the standard of "persons suspected of subversive activities," for example, was one on the Los Angeles Chamber of Commerce in 1941.[108] This was approved in spite of his comment to J. Edgar Hoover that the target organization had "no record of espionage at this time." [109] In 1945, Attorney General Tom Clark authorized a wiretap on a former aide to President Roosevelt.[110] According to a memorandum by J. Edgar Hoover, Clark stated that President Truman wanted "a very thorough investigation" of the activities of the former official so that "steps might be taken, if possible, to see that [his] activities did not interfere with the proper administration of government." [111] The memorandum makes no reference to "subversive activities" or any other national security considerations.

The "Sugar Lobby" and Martin Luther King, Jr., wiretaps in the early 1960s both show the elasticity of the "domestic security" standard which supplemented President Roosevelt's "subversive activities" formulation. Among those wiretapped in the Sugar Lobby investigation, as noted above, was a Congressional staff aide. Yet the documentary record of this investigation reveals no evidence indicating that the target herself represented any threat to the "domestic security." Similarly, while the FBI may properly have been concerned with the activities of certain advisors to Dr. King, the direct wiretapping of Dr. King shows that the "domestic security" standard could be stretched to unjustified lengths.

The microphone surveillances of Congressman Cooley and Dr. King under the "national interest" standard established by Attorney General Brownell in 1954 also reveal the relative ease with which electronic bugging devices could be used against American citizens who

[107] See, e.g., *Olmstead* v. *United States*, 277 U.S. 438, (1928).

[108] Memorandum from Francis Biddle to Mr. Hoover, 11/19/41.

[109] Ibid.

[110] Unaddressed Memorandum from J. Edgar Hoover, 11/15/45, found in Director Hoover's "Official and Confidential" files.

[111] Ibid.

posed no genuine "national security" threat. Neither of these targets advocated or engaged in any conduct that was damaging to the security of the United States.

In April, 1964, Attorney General Robert Kennedy approved "technical coverage (electronic surveillance)" of a black nationalist leader after the FBI advised Kennedy that he was "forming a new group" which would be "more aggressive" and would "participate in racial demonstrations and civil rights activities." The only indication of possible danger noted in the FBI's request for the wiretaps, however, was that this leader had "recommended the possession of firearms by members for their self-protection.[112]

One year later, Attorney General Nicholas Katzenbach approved a wiretap on the offices of the Student Non-Violent Coordinating Committee on the basis of *potential* communist infiltration into that organization. The request which was sent to the Attorney General noted that "confidential informants" described SNCC as "the principal target for Communist Party infiltration among the various civil rights organizations" and stated that some of its leaders had "made public appearances with leaders of communist-front organizations" and had "subversive backgrounds." [113] The FBI presented no substantial evidence however, that SNCC was in fact infiltrated by communists—only that the organization was apparently a target for such infiltration in the future.

After the Justice Department adopted new criteria for the institution of warrantless electronic surveillance in 1968, the unjustified use of wiretaps continued. In November 1969, Attorney General John Mitchell approved a series of three wiretaps on organizations involved in planning the antiwar "March on Washington." The FBI's request for coverage of the first group made no claim that its members engaged or were likely to engage in violent activity; the request was simply based on the statement that the anticipated size of the demonstration was cause for "concern should violence of any type break out." [114]

The only additional justification given for the wiretap on one of the other groups, the Vietnam Moratorium Committee, was that it "has recently endorsed fully the activities of the [first group] concerning the upcoming antiwar demonstrations." [115]

In 1970, approval for a wiretap on a "New Left oriented campus group" was granted by Attorney General Mitchell on the basis of an FBI request which included, among other factors deemed relevant to the necessity for the wiretap, evidence that the group was attempting "to develop strong ties with the cafeteria, maintenance and other workers on campus" and wanted to "go into industry and factories and . . . take the radical politics they learned on the campus and spread them among factory workers." [116]

---

[112] Memorandum from J. Edgar Hoover to the Attorney General, 4/1/64.

[113] Memorandum from J. Edgar Hoover to the Attorney General, 6/15/65.

[114] Memorandum from J. Edgar Hoover to the Attorney General, 11/5/69.

[115] Memorandum from J. Edgar Hoover to Attorney General Mitchell, 11/7/69.

[116] Memorandum from J. Edgar Hoover to the Attorney General, 3/16/70. The strongest evidence that this group's conduct was inimical to the national security was reported as follows:

"The [group] is dominated and controlled by the pro-Chinese Marxist Leninist (excised). . . .

"In carrying out the Marxist-Leninist ideology of the (excised) members have repeatedly sought to become involved in labor disputes on the side of labor, join

This approval was renewed three months later despite the fact that the request for renewal made no mention of violent or illegal activity by the group. The value of the wiretap was shown, according to the FBI, by such results as obtaining "the identities of over 600 persons either in touch with the national headquarters or associated with" it during the preceding three months.[117] Six months after the original authorization the number of persons so identified had increased to 1,428; and approval was granted for a third three-month period."[118]

The "seventeen wiretaps" also show how the term "national security" as a justification for wiretapping can obscure improper use of this technique. Shortly after these wiretaps were revealed publicly, President Nixon stated they had been justified by the need to prevent leaks of classified information harmful to the national security.[119]

Wiretaps for this purpose had, in fact, been authorized under the Kennedy and Johnson administrations. President Nixon learned of these and other prior taps and, at a news conference, sought to justify the taps he had authorized by referring to past precedent. He stated that in the:

> period of 1961 to '63 there were wiretaps on news organizations, on news people, on civil rights leaders and on other people. And I think they were perfectly justified and I'm sure that President Kennedy and his brother, Robert Kennedy, would never have authorized them, unless he thought they were in the national interest. (Presidential News Conference, 8/22/73.)

Thus, questionable electronic surveillances by earlier administrations were put forward as a defense for improper surveillances exposed in 1973. In fact, however, two of these wiretaps were placed on domestic affairs advisers at the White House who had no foreign affairs responsibilities and apparently no access to classified foreign policy materials.[121] A third target was a White House speech writer who had been overheard on an existing tap agreeing to provide a reporter with background information on a Presidential speech con-

---

picket lines and engage in disruptive and sometimes violent tactics against industry recruiters on college campuses. . . .

"This faction is currently very active in many of the major demonstrations and student violence on college campuses. . . ." (Memorandum from J. Edgar Hoover to the Attorney General, 3/16/70. The excised words have been deleted by the FBI.)

[117] Memorandum from J. Edgar Hoover to the Attorney General, 6/16/70. The only other results noted by Hoover related to the fact that the wiretap had "obtained information concerning the activities of the national headquarters of [the group and] plans for [the group's] support and participation in demonstrations supporting antiwar groups and the (excised)." It was also noted that the wiretap "revealed . . . contacts with Canadian student elements".

[119] Memorandum from J. Edgar Hoover to the Attorney General, 9/16/70. The only other results noted by Hoover again related to obtaining information about the "plans and activities" of the group. Specifically mentioned were the "plans for the National Interim Committee (ruling body of [excised]) meeting which took place in New York and Chicago", and the plans "for demonstrations at San Francisco, Detroit, Salt Lake City, Minneapolis, and Chicago." There was no indication that these demonstrations were expected to be violent. (The excised words have been deleted by the FBI).

[119] Public statement of President Nixon, 5/22/73.

[121] Memorandum from J. Edgar Hoover to the Attorney General 7/23/69; memorandum from J. Edgar Hoover to the Attorney General 12/14/70.

cerning domestic revenue sharing and welfare reform.[122] The reinstatement of another wiretap in this series was requested by H. R. Haldeman simply because "they may have a bad apple and have to get him out of the basket." [123] The last four requests in this series that were sent to the Attorney General (including the requests for a tap on the "bad apple") did not mention any national security justification at all. As former Deputy Attorney General William Ruckelshaus has testified:

> I think some of the individuals who were tapped, at least to the extent I have reviewed the record, had very little, if any, relationship to any claim of national security . . . I think that as the program proceeded and it became clear to those who could sign off on taps how easy it was to institute a wiretap under the present procedure that these kinds of considerations [i.e., genuine national security justifications] were considerably relaxed as the program went on.[124]

None of the "seventeen" wiretaps was ever reauthorized by the Attorney General, although 10 of them remained in operation for periods longer than 90 days and although President Nixon himself stated privately that "[t]he tapping was a very, very unproductive thing . . . it's never been useful to any operation I've conducted . . ." [125]

In short, warrantless electronic surveillance has been defended on the ground that it was essential for the national security, but the history of the use of this technique clearly shows that the imprecision and manipulation of this and similar labels, coupled with the absence of any outside scrutiny, has led to its improper use against American citizens who posed no criminal or national security threat to the country.[126]

Similarly, the terms "foreign intelligence" and "counterespionage" were used by the CIA and the FBI to justify their cooperation in the CIA's New York mail opening project, but this project was also used to target entirely innocent American citizens.

As noted above, the CIA compiled a "Watch List" of names of persons and organizations whose mail was to be opened if it passed through the New York facility. In the early days of the project, the names on this list—which then numbered fewer than twenty—might reason-

---

[122] Memorandum from W. C. Sullivan to C. D. DeLoach, 8/1/69.

[123] Memorandum from J. Edgar Hoover to Messrs. Tolson, Sullivan and D. C. Brennan, 10/15/70.

[124] Ruckelshaus testimony before the Senate Subcommittee on Administrative Practice and Procedure, 5/9/74, pp. 311–12.

[125] Transcript of the Presidential Tapes, 2/28/73 (House Judiciary Committee Statement of Information Book VII, Part W, p. 1754.)

[126] The term "national security" was also used by John Ehrlichman and Charles Colson to justify their roles in the break-in of Dr. Fielding's office in 1971. A March 21, 1973 tape recording of a meeting between President Nixon, John Dean, and H. R. Haldeman suggests, however, that the national security "justification" may have been developed long after the event for the purpose of obscuring its impropriety. When the President asked what could be done if the break-in was revealed publicly, John Dean suggested, "You might put it on a national security grounds basis." Later in the conversation, President Nixon stated "With the bombing thing coming out and everything coming out, the whole thing was national security," and Dean said, "I think we could get by on that." (Transcript of Presidential tapes, 3/21/73.)

ably have been expected to lead to genuine foreign intelligence or counterintelligence information. But as the project developed, the Watch List grew and its focus changed. By the late 1960s there were approximately 600 names on the list, many of them American citizens and organizations who were engaged in purely lawful and constitutionally protected forms of protest against governmental policies. Among the domestic organizations on the Watch List, which was supplemented by submissions from the FBI, were: Clergy and Laymen Concerned about Vietnam, the National Mobilization Committee to End the War in Vietnam, *Ramparts*, the Student Non-Violent Coordinating Committee, the Center for the Study of Public Policy, and the American Friends Service Committee.[127]

The FBI levied more general requirements on the CIA's project as well. The focus of the original categories of correspondence in which the FBI expressed an interest was clearly foreign counterespionage, but subsequent requirements became progressively more domestic in their focus and progressively broader in their scope. The requirements that were levied by the FBI in 1972, one year before the termination of the project, included the following:

> "... [p]ersons on the Watch List; known communists, New Left activists, extremists, and other subversives ...
>
> Communist party and front organizations ... extremist and New Left organizations.
>
> Protest and peace organizations, such as People's Coalition for Peace and Justice, National Peace Action Committee, and Women's Strike for Peace.
>
> Communists, Trotskyites and members of other Marxist-Leninist, subversive and extremist groups, such as the Black Nationalists and Liberation groups ... Students for a Democratic Society ... and other New Left groups.
>
> Traffic to and from Puerto Rico and the Virgin Islands showing anti-U.S. or subversive sympathies." [128]

This final set of requirements evidently reflected the domestic turmoil of the late 1960s and early 1970s. The mail opening program that began as a means of collecting foreign intelligence information and discovering Soviet intelligence efforts in the United States had expanded to encompass detection of the activities of domestic dissidents of all types.

. . . . . .

In the absence of effective outside control, highly intrusive techniques have been used to gather vast amounts of information about the entirely lawful activities—and privately held beliefs—of large numbers of American citizens. The very intrusiveness of these techniques demands the utmost circumspection in their use. But with vague or non-existent standards to guide them, and with labels such as "national security" and "foreign intelligence" to shield them, executive branch officials have been all too willing to unleash these techniques against American citizens with little or no legitimate justification.

---

[127] Staff summary of Watch List review, 9/5/75.

[128] Routing slip from J. Edgar Hoover to James Angelton (attachment), 3/10/72.