CIVIL LIBERTIES AND THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

DONALD J. MUSCH

Fourteenth Volume, Second Series
Terrorism: Documents of International & Local Control

James Walsh
General Editor

OCEANA PUBLICATIONS, INC. DOBBS FERRY, NEW YORK

Library of Congress Control Number: 2003109185

Terrorism: Documents of International and Local Control, Second Series

ISSN 1064-9352

ISBN 0-379-21503-9

Manufactured in the United States of America on acid-free paper.

INTRODUCTION

It is well documented that government activities affecting personal rights escalate during times of crisis. Events since the attacks of 9/11 fit this practice. The Foreign Intelligence Surveillance Act (FISA) was enacted during the Cold War in the interest of national security to improve United States intelligence overseas and to provide better access to "foreign intelligence information." The FSIA specifically limits these surveillance activities within the United States. Passage of the FISA was a specific legislative pronouncement aimed at protecting against excessive government intrusion on personal liberties. Key to FISA was the creation of a Foreign Intelligence Surveillance Court (FISC), a secretive and specialized judicial tool which would ensure there was a check on the activities of the Executive Branch, most notably in the area of secret surveillance.

This work offers the reader an opportunity to revisit the actions and emotions which led to passage of the FISA, and the cataclysmic impact the attacks of 9/11 had on U.S. policy and its approach to the preservation of personal liberty. A distinct fear of a repeat of such attacks undoubtedly is driving the Administration to take very aggressive measures, not only to reconfigure the government's structure to cope with terrorism but to more closely align the legality of governmental actions with the concomitant dangers inherent in our 21st Century society. How far the pendulum swings towards the security argument will depend not so much on legislative oversight and initiative, but on the actual events which transpire in the near future. Put another way, relative quiet and peace from terrorists will likely precipitate increased pressure from the public to pull back from the more stringent authorities given the government. For example, freedom from violent acts will offer legislators a much easier opportunity to withdraw some of the Patriot Act authorities when the sunshine provisions come into effect in 2005.

To some extent, the public is still unaware of the degree of control and oversight which has been exercised by the FISC but, based on the required annual public reports submitted by the Attorney General to the Administrative Office of the U.S. Courts, there is clear evidence that the FISC has given virtually universal approval to the large number of government requests for electronic surveillance. The record for such applications shows:

1997	749 approved	0 disapproved
1998	796 approved	0 disapproved
1999	886 approved	0 disapproved
2000	1012 approved	0 disapproved
2001	934 approved	0 disapproved
2002	1228 approved	0 disapproved

Actions of the Executive Branch, and two fundamental decisions by the FISC and its Foreign Intelligence Review Court (FIRC) brought to the fore many resurgent concerns advanced, most notably, by civil rights groups in the United States and in the press. Those actions of the Executive Branch were led with:

- forcefully pushing through the USA Patriot Act of 2001 (with admittedly minimal evaluation and discussion in Congress);
- changes in the procedures followed by the Executive Branch in fighting terrorism through the legal system;
- the filing of new procedures with the FISC and appealing the FISC decision (which agreed to such changes only with amendments) to the FIRC, and;
- the more recent circulation of broader legislative proposals aimed at improving the government's ability to fight terrorism.

More detailed coverage is given to the actions and arguments surrounding the FISC decision of May 17, 2002 because it effectively represented the first time FISC had actually refused to go along with a governmental request and the FISC decision, at least in the eyes of civil libertarians, drew a line over which the Executive could not venture while it claimed to be enforcing the FISA as originally passed and intended. The FISC decision was appealed to the FIRC whose decision was equally momentous for it found the governmental approach to be sound, and it laid the groundwork for either "more effective" or "continued egregious" government conduct, depending on one's point of view.

The proposed "Patriot II" legislation represents an Administration initiative which is valuable because it shows the outer limits (for the moment) which the government wishes to reach in fighting terrorism. Some speculate the draft was leaked to gauge the public reaction to the proposals—offering the Administration an opportunity to tailor a final product acceptable to the American public, and its legislators. Whatever the reason, the draft elicited intense (and mostly critical) comments from the press, advocacy groups, and legal scholars. To those having a natural antagonism towards the current Administration it is living proof that this Department of Justice knows "no limits" on power. On the other hand, for those who are striving to ensure continued security for this democracy (and chances are this includes most of those who are directly connected with the "war on terrorism") most of what is being proposed is viewed as effective and warranted—even if some aspects are a bitter pill to swallow!

Some of the material presented in this work originates from an advocacy group which is well known throughout the world—the American Civil Liberties Union (ACLU). The ACLU's petition for a writ of Certiorari to the U.S. Supreme Court was a unique filing. The comments the ACLU provided on Patriot II represent one of the few explanations of those provisions—the Administration has circulated nothing on the subject. Countering the advocacy perspective contained in the ACLU materials is the equally slanted material in Document Number 11 giving the Executive's answers to questions posed by Congress on FISA and Patriot I. And, throughout this volume, the reader will find examples of the commentary from a broad range of media—each contribution with its own point of view to forward. What the reader should be left with is not confusion, but hopefully a starting point for further inquiry into what is being proposed, what is being done, and what should be changed.

Donald J. Musch

August 5, 2003

OVERALL TABLE OF CONTENTS

TABLE OF CONTENTS

THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA)

The Historical Perspective—The Church Hearings and Beyond

COMMENTARY

THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA)

The Historical Perspective—The Church Hearings and Beyond

Total disenchantment with governmental practices subsequent to Watergate led to the formation of the Senate Select Committee to Study Governmental Operations chaired by Senator Frank Church. The Committee was tasked "to conduct an investigation and study of governmental operations with respect to intelligence activities and of the extent, if any, to which illegal, improper, or unethical activities were engaged in by any agency of the Federal Government." Senate Resolution No. 21 included a comprehensive list of areas which the Committee was to address, and the ensuing 15-month investigation was perhaps the most comprehensive examination of intelligence operations conducted in the United States. In the area of civil liberties and the relationship of intelligence operations to domestic law enforcement agencies, the Committee confronted a broad range of issues dealing with electronic surveillance and other means for secretly obtaining information. As pointed out in the Committee Report issued on April 26, 1976:

> In the few years prior to the establishment of this Committee, however, the public's awareness of the need to examine intelligence issues was heightened. The series of allegations and partial exposure in the press and the congress provoked serious questions about the conduct of intelligence activities at home and abroad. The Watergate affair increased the public's concern about abuse of governmental power and caused greater attention to be paid to the need to follow and to strengthen the role of law to check such abuses . . . (Book I, page 11)

Addressing the question of warrantless electronic surveillance, the Committee reported:

> The courts have also not confronted intelligence issues. As the Supreme Court noted in 1972 in commenting on warrantless electronic surveillance, 'The practice has been permitted by successive presidents for more than a quarter of a century without 'guidance from the Congress or a definitive decision by the Court.' (Book I, page 11)

Though it was not a major topical area for consideration by the Committee, "coordination" of intelligence activities within the United States or involving American citizens (most particularly CIA-FBI coordination) was important and the Committee concluded: " . . . the Huston Plan episode illustrates the questions of propriety and legality which may arise in counterintelligence operations conducted in the United States or involving American citizens." (Book I, page 428). In the eyes of the Committee, Congress and the executive should pay more attention to this area of coordina-

tion because, among other reasons: " . . . counterintelligence has infringed on the rights and liberties of Americans." (Book I, page 440)

The Committee then issued as a "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 . . . " adding later that the legal standards and procedures regulating their use have been insufficient. (Book II, page 183)

The extensive criticisms of governmental policy and practices within the Committee Report triggered diverse views, even among those who served on the Committee. Senator Baker, referred to a comment by former Director of Central Intelligence William Colby (as quoted from the *New York Times* which said:

> . . . This year's excitement has made clear that the rule of law applies to all parts of the American Government, including intelligence. In fact, this will strengthen American intelligence. (Book I, page 595)

On the other hand, Senator Barry Goldwater stated in his separate comments to the Report:

> I have refused to sign the final report of the Select Committee on Intelligence Activities in the belief it will cause severe embarrassment, if not grave harm, to the Nation's foreign policy. (Book I, page 593)

But the balancing of acts which encroach on liberties to avoid other acts which can destroy the very fabric of our society permeates the hearings and the report, and the importance of its findings and deliberations were to focus attention on areas of immense importance which, heretofore, had been shielded by governmental secrecy, judicial inaction, and congressional complicity. And, in the end, in the relatively narrow field of laying down additional rules for domestic intelligence activities, the Report influenced the passage of the Foreign Intelligence Surveillance Act of 1978. The following excerpt from the Committee Report provides a valuable indication of the legal and executive branch actions which led up to the Watergate Hearings and the subsequent appointment and report of the Church Committee.

. . .

> 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 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 in 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 acquiesced 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 requirement of periodic reapproval by the Attorney General.[20] In the absence of any instruction to terminate them, some wiretraps 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 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 surveillance to protect the nation from domestic threats.[24] The Court pointedly refrained, however, from any "judgment on the scope of the President's 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 complied 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 antiwar 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 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 installa-

tions, continued until 1965, when the Justice Department began to apply the same criteria and procedures to both microphone and telephone surveillance.

Notes:

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

[14] *Nordone 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. 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 to 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 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).

[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 surveillance 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 Fourth 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 paralleled 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 NSA 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."

[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.

A full summary of the Report is included as a document in this volume.

FISA, affected by the events considered by the Church Committee and before, and as passed by Congress in 1978, was viewed as a major vehicle to control governmental activities which might impinge on private rights. As pointed out in the legislative history of the bill:

> As Attorney General Bell stated in testifying in favor of the bill:
>
> > I believe this bill is remarkable not only in the way it has been developed, but also in the fact that for the first time in our society the clandestine intelligence activities of our government shall be subject to the regulation and receive the positive authority of a public law for all to inspect. President Carter stated it very well in announcing this bill when he said that 'one of the most difficult tasks in a free society like our own is the correlation between adequate intelligence to guarantee our nation's security on the one hand, and the preservation of basic human rights on the other.' (P.S. 95-511, Legislative History, U.S. Cong. & Adm. News '78-30, page 3905).

Illustrating further what the Congress was trying to achieve, and the ills it was countering, the Legislative History points out that warrantless electronic surveillance abuses "illuminated in 1975 during the investigation of the Watergate break-in . . . ." and the subsequent conclusions of the Church Committee clearly identified numerous examples of illegal wiretaps without the benefit of judicial warrant.

Specific actions covered by FISA, and which were exempt from prior legislative restrictions, were electronic surveillance when done for "national security" but, as can be seen from governmental actions and judicial decisions post FISA, the FISA evolved (through amendments by the USA Patriot Act of 2001) into a valuable tool for governmental investigations, involving both criminal and foreign intelligence activities. The concern of many at the time FISA was enacted was that information would be circulated from electronic surveillance which did NOT involve foreign intelligence. As Ira R. Shapiro stated in the *Harvard Journal on Legislation* (Vol. 15, at page 202):

> But no similar qualms should block imposition of criminal penalties for improper retention or dissemination of information which is clearly not foreign intelligence information. Enactment of criminal sanctions would be a strong response to the revelations of the Church Committee. It would also allay public concern about the scope of the electronic surveillance permitted under the statute.

Mr. Shapiro concluded his note fully supporting passage of the FISA and stating:

> Every major provision of the bill has been written and reworked painstakingly, with careful attention to the concerns of both civil libertarians and the intelligence community. (at page 204)

FISA attempted to strike a balance between protecting the national security and protecting civil liberties by setting out a clear procedure for the use of electronic surveillance in gathering foreign intelligence. The law re-