

1 CINDY COHN (145997)
cindy@eff.org
2 LEE TIEN (148216)
KURT OPSAHL (191303)
3 JAMES S. TYRE (083117)
MARK RUMOLD (279060)
4 ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
5 San Francisco, CA 94110
Telephone: (415) 436-9333
6 Fax: (415) 436-9993

7 RICHARD R. WIEBE (121156)
wiebe@pacbell.net
8 LAW OFFICE OF RICHARD R. WIEBE
One California Street, Suite 900
9 San Francisco, CA 94111
Telephone: (415) 433-3200
10 Fax: (415) 433-6382

11
12
13 Attorneys for Plaintiffs

RACHAEL E. MENY (178514)
rmeny@kvn.com
PAULA L. BLIZZARD (207920)
MICHAEL S. KWUN (198945)
AUDREY WALTON-HADLOCK (250574)
KEKER & VAN NEST, LLP
710 Sansome Street
San Francisco, California 94111-1704
Telephone: (415) 391-5400
Fax: (415) 397-7188

THOMAS E. MOORE III (115107)
tmoore@moorelawteam.com
THE MOORE LAW GROUP
228 Hamilton Avenue, 3rd Floor
Palo Alto, CA 94301
Telephone: (650) 798-5352
Fax: (650) 798-5001

ARAM ANTARAMIAN (239070)
aram@eff.org
LAW OFFICE OF ARAM ANTARAMIAN
1714 Blake Street
Berkeley, CA 94703
Telephone: (510) 289-1626

14 **UNITED STATES DISTRICT COURT**
15 **FOR THE NORTHERN DISTRICT OF CALIFORNIA**

16
17 CAROLYN JEWEL, TASH HEPTING,
GREGORY HICKS, ERIK KNUTZEN and
18 JOICE WALTON, on behalf of themselves and
all others similarly situated,
19
20 Plaintiffs,
21
22 v.
NATIONAL SECURITY AGENCY, *et al.*,
23
24
25
26
27
28 Defendants.

) CASE NO. 08-CV-4373-JSW
)
)
) **DECLARATION OF**
) **CINDY A. COHN**
) **IN SUPPORT OF PLAINTIFFS'**
) **MOTION FOR PARTIAL SUMMARY**
) **JUDGMENT**
)
) Date: November 2, 2012
) Time: 9:00 a.m.
) Courtroom 11, 19th Floor
) The Honorable Jeffrey S. White

1 I, Cindy A. Cohn, do hereby declare:

2 1. I am a member in good standing of the Bar of the State of California and the bar of
3 this Court. I am counsel to plaintiffs in this action. I have personal knowledge of the facts set forth
4 below, except as may be otherwise noted, and if called as a witness I could and would testify
5 competently to them.

6 2. Attached hereto as Exhibit A is true and correct copy of excerpts from the Final
7 Report of the Senate Select Committee to Study Governmental Operations with Respect to
8 Intelligence Activities (the "Church Committee"), Book II: *Intelligence Activities and the Rights of*
9 *Americans*, S. Rep. No. 94-755 (1976).

10 3. Attached hereto as Exhibit B is a true and correct copy of the following newspaper
11 article: Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls*, USA Today (May
12 11, 2006), available at http://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm.

13 4. Attached hereto as Exhibit C is a true and correct copy of the following newspaper
14 article: James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. Times
15 (December 16, 2005), available at <http://www.nytimes.com/2005/12/16/politics/16program.html>.

16 5. Attached hereto as Exhibit D is a true and correct copy of the following newspaper
17 article: Matthew D. LaPlante, *Spies Like Us: NSA to Build Huge Facility in Utah*, Salt Lake
18 Tribune (July 2, 2009), available at http://www.sltrib.com/ci_12735293.

19 6. Attached hereto as Exhibit E are excerpts from S. Rep. No. 95-604 (1978), *reprinted*
20 *in* 1978 U.S.C.C.A.N. 3904.

21 7. Attached hereto as Exhibit F are excerpts from S. Rep. No. 94-1035 (1976).

22 8. Attached hereto as Exhibit G are excerpts from the House-Senate Conference
23 Committee on FISA, H.R. Rep. No. 95-1720 (1978), *reprinted in* 1978 U.S.C.C.A.N. 4048.

24 9. Attached hereto as Exhibit H are excerpts from H.R. Rep. No. 95-1283 (1978).

25 10. Attached hereto as Exhibit I are excerpts from S. Rep. No. 95-701 (1978), *reprinted*
26 *in* 1978 U.S.C.C.A.N. 3973.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

I declare under penalty of perjury of the laws of the United States that the foregoing is true and correct to the best of my knowledge and belief.

Executed June 29, 2012 at San Francisco, California.

s/ Cindy A. Cohn
Cindy A. Cohn

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

CERTIFICATE OF SERVICE

I hereby certify that on June 29, 2012, I electronically filed the foregoing document with the Clerk of the Court, using the CM/ECF system, which will send notification of such filing to the counsel of record in this matter who are registered on the CM/ECF system.

Executed on June 29, 2012, in San Francisco, California.

/s/ Cindy Cohn
Cindy Cohn

EXHIBIT A

94TH CONGRESS }
2d Session }

SENATE

{ REPORT
{ No. 94-755

INTELLIGENCE ACTIVITIES AND THE
RIGHTS OF AMERICANS

BOOK II

FINAL REPORT
OF THE
SELECT COMMITTEE
TO STUDY GOVERNMENTAL OPERATIONS
WITH RESPECT TO
INTELLIGENCE ACTIVITIES
UNITED STATES SENATE
TOGETHER WITH
ADDITIONAL, SUPPLEMENTAL, AND SEPARATE
VIEWS



APRIL 26 (legislative day, APRIL 14), 1976

U.S. GOVERNMENT PRINTING OFFICE

68-786 O

WASHINGTON : 1976

don his supposed 'obedience' to white liberal doctrines (non-violence)."⁷⁰ In short, a non-violent man was to be secretly attacked and destroyed as insurance against his abandoning non-violence.

(b) *Illegal or Improper Means.*—The surveillance which we investigated was not only vastly excessive in breadth and a basis for degrading counterintelligence actions, but was also often conducted by illegal or improper means. For example:

(1) For approximately 20 years the CIA carried out a program of indiscriminately opening citizens' first class mail. The Bureau also had a mail opening program, but cancelled it in 1966. The Bureau continued, however, to receive the illegal fruits of CIA's program. In 1970, the heads of both agencies signed a document for President Nixon, which correctly stated that mail opening was illegal, falsely stated that it had been discontinued, and proposed that the illegal opening of mail should be resumed because it would provide useful results. The President approved the program, but withdrew his approval five days later. The illegal opening continued nonetheless. Throughout this period CIA officials knew that mail opening was illegal, but expressed concern about the "flap potential" of exposure, not about the illegality of their activity.⁷¹

(2) From 1947 until May 1975, NSA received from international cable companies millions of cables which had been sent by American citizens in the reasonable expectation that they would be kept private.⁷²

(3) Since the early 1930's, intelligence agencies have frequently wiretapped and bugged American citizens without the benefit of judicial warrant. Recent court decisions have curtailed the use of these techniques against domestic targets. But past subjects of these surveillances have included a United States Congressman, a Congressional staff member, journalists and newsmen, and numerous individuals and groups who engaged in no criminal activity and who posed no genuine threat to the national security, such as two White House domestic affairs advisers and an anti-Vietnam War protest group. While the prior written approval of the Attorney General has been required for all warrantless wiretaps since 1940, the record is replete with instances where this requirement was ignored and the Attorney General gave only after-the-fact authorization.

Until 1965, microphone surveillance by intelligence agencies was wholly unregulated in certain classes of cases. Within weeks after a 1954 Supreme Court decision denouncing the FBI's installation of a microphone in a defendant's bedroom, the Attorney General informed the Bureau that he did not believe the decision applied to national security cases and

⁷⁰ Memorandum from FBI Headquarters to all SACs, 3/4/68.

⁷¹ See Mail Opening Report: Section II, "Legal Considerations and the 'Flap' Potential."

⁷² See NSA Report: Section I, "Introduction and Summary."

II. THE GROWTH OF DOMESTIC INTELLIGENCE: 1936 TO 1976

A. SUMMARY

1. *The Lesson: History Repeats Itself*

During and after the First World War, intelligence agencies, including the predecessor of the FBI, engaged in repressive activity.¹ A new Attorney General, Harlan Fiske Stone, sought to stop the investigation of "political or other opinions."² This restraint was embodied only in an executive pronouncement, however. No statutes were passed to prevent the kind of improper activity which had been exposed. Thereafter, as this narrative will show, the abuses returned in a new form. It is now the responsibility of all three branches of government to ensure that the pattern of abuse of domestic intelligence activity does not recur.

2. *The Pattern: Broadening Through Time*

Since the re-establishment of federal domestic intelligence programs in 1936, there has been a steady increase in the government's capability and willingness to pry into, and even disrupt, the political activities and personal lives of the people. The last forty years have witnessed a relentless expansion of domestic intelligence activity beyond investigation of criminal conduct toward the collection of political intelligence and the launching of secret offensive actions against Americans.

The initial incursions into the realm of ideas and associations were related to concerns about the influence of foreign totalitarian powers.

¹ Repressive practices during World War I included the formation of a volunteer auxiliary force, known as the American Protective League, which assisted the Justice Department and military intelligence in the investigation of "un-American activities" and in the mass round-up of 50,000 persons to discover draft evaders. These so-called "slacker raids" of 1918 involved warrantless arrests without sufficient probable cause to believe that crime had been or was about to be committed (FBI Intelligence Division memorandum, "An Analysis of FBI Domestic Security Intelligence Investigations," 10/28/75.)

The American Protective League also contributed to the pressures which resulted in nearly 2,000 prosecutions for disloyal utterances and activities during World War I, a policy described by John Lord O'Brien, Attorney General Gregory's Special Assistant, as one of "wholesale repression and restraint of public opinion." (Zechariah Chafee, *Free Speech in the United States* (Cambridge: Harvard University Press, 1941) p. 69.)

Shortly after the war the Justice Department and the Bureau of Investigation jointly planned the notorious "Palmer Raids", named for Attorney General A. Mitchell Palmer who ordered the overnight round-up and detention of some 10,000 persons who were thought to be "anarchist" or "revolutionary" aliens subject to deportation. (William Preston, *Aliens and Dissenters* (Cambridge: Harvard University Press, 1963), chs. 7-8; Stanley Cohen, *A. Mitchell Palmer: Politician* (New York: Columbia University Press, 1963), chs. 11-12.)

² See Attorney General Stone's full statement, p. 23.

Ultimately, however, intelligence activity was directed against domestic groups advocating change in America, particularly those who most vigorously opposed the Vietnam war or sought to improve the conditions of racial minorities. Similarly, the targets of intelligence investigations were broadened from groups perceived to be violence prone to include groups of ordinary protesters.

3. Three Periods of Growth for Domestic Intelligence

The expansion of domestic intelligence activity can usefully be divided into three broad periods: (a) the pre-war and World War II period; (b) the Cold War era; and (c) the period of domestic dissent beginning in the mid-sixties. The main developments in each of these stages in the evolution of domestic intelligence may be summarized as follows:

a. 1936-1945

By presidential directive—rather than statute—the FBI and military intelligence agencies were authorized to conduct domestic intelligence investigations. These investigations included a vaguely defined mission to collect intelligence about “subversive activities” which were sometimes unrelated to law enforcement. Wartime exigencies encouraged the unregulated use of intrusive intelligence techniques; and the FBI began to resist supervision by the Attorney General.

b. 1946-1963

Cold War fears and dangers nurtured the domestic intelligence programs of the FBI and military, and they became permanent features of government. Congress deferred to the executive branch in the oversight of these programs. The FBI became increasingly isolated from effective outside control, even from the Attorneys General. The scope of investigations of “subversion” widened greatly. Under the cloak of secrecy, the FBI instituted its COINTELPRO operations to “disrupt” and “neutralize” “subversives”. The National Security Agency, the FBI, and the CIA re-instituted intrusive wartime surveillance techniques in contravention of law.

c. 1964-1976

Intelligence techniques which previously had been concentrated upon foreign threats and domestic groups said to be under Communist influence were applied with increasing intensity to a wide range of domestic activity by American citizens. These techniques were utilized against peaceful civil rights and antiwar protest activity, and thereafter in reaction to civil unrest, often without regard for the consequences to American liberties. The intelligence agencies of the United States—sometimes abetted by public opinion and often in response to pressure from administration officials or the Congress—frequently disregarded the law in their conduct of massive surveillance and aggressive counterintelligence operations against American citizens. In the past few years, some of these activities were curtailed, partly in response to the moderation of the domestic crisis; but all too often improper programs were terminated only in response to exposure, the threat of exposure, or a change in the climate of public opinion, such as that triggered by the Watergate affair.

IV. CONCLUSIONS AND RECOMMENDATIONS

A. CONCLUSIONS

The findings which have emerged from our investigation convince us that the Government's domestic intelligence policies and practices require fundamental reform. We have attempted to set out the basic facts; now it is time for Congress to turn its attention to legislating restraints upon intelligence activities which may endanger the constitutional rights of Americans.

The Committee's fundamental conclusion is that intelligence activities have undermined the constitutional rights of citizens and that they have done so primarily because checks and balances designed by the framers of the Constitution to assure accountability have not been applied.

Before examining that conclusion, we make the following observations.

—While nearly all of our findings focus on excesses and things that went wrong, we do not question the need for lawful domestic intelligence. We recognize that certain intelligence activities serve perfectly proper and clearly necessary ends of government. Surely, catching spies and stopping crime, including acts of terrorism, is essential to insure “domestic tranquility” and to “provide for the common defense.” Therefore, the power of government to conduct *proper* domestic intelligence activities under effective restraints and controls must be preserved.

—We are aware that the few earlier efforts to limit domestic intelligence activities have proven ineffectual. This pattern reinforces the need for statutory restraints coupled with much more effective oversight from all branches of the Government.

—The crescendo of improper intelligence activity in the latter part of the 1960s and the early 1970s shows what we must watch out for: In time of crisis, the Government will exercise its power to conduct domestic intelligence activities to the fullest extent. The distinction between legal dissent and criminal conduct is easily forgotten. Our job is to recommend means to help ensure that the distinction will always be observed.

—In an era where the technological capability of Government relentlessly increases, we must be wary about the drift toward “big brother government.” The potential for abuse is awesome and requires special attention to fashioning restraints which not only cure past problems but anticipate and prevent the future misuse of technology.

—We cannot dismiss what we have found as isolated acts which were limited in time and confined to a few willful men. The failures to obey the law and, in the words of the oath of office, to “preserve, protect, and defend” the Constitution, have occurred repeatedly throughout administrations of both political parties going back four decades.

—We must acknowledge that the assignment which the Government has given to the intelligence community has, in many ways, been impossible to fulfill. It has been expected to predict or prevent every crisis, respond immediately with information on any question, act to meet all threats, and anticipate the special needs of Presidents. And then it is chastised for its zeal. Certainly, a fair assessment must place a major part of the blame upon the failures of senior executive officials and Congress.

In the final analysis, however, the purpose of this Committee's work is not to allocate blame among individuals. Indeed, to focus on personal culpability may divert attention from the underlying institutional causes and thus may become an excuse for inaction.

Before this investigation, domestic intelligence had never been systematically surveyed. For the first time, the Government's domestic surveillance programs, as they have developed over the past forty years, can be measured against the values which our Constitution seeks to preserve and protect. Based upon our full record, and the findings which we have set forth in Part III above, the Committee concludes that:

Domestic Intelligence Activity Has Threatened and Undermined The Constitutional Rights of Americans to Free Speech, Association and Privacy. It Has Done So Primarily Because The Constitutional System for Checking Abuse of Power Has Not Been Applied.

Our findings and the detailed reports which supplement this volume set forth a massive record of intelligence abuses over the years. Through a vast network of informants, and through the uncontrolled or illegal use of intrusive techniques—ranging from simple theft to sophisticated electronic surveillance—the Government has collected, and then used improperly, huge amounts of information about the private lives, political beliefs and associations of numerous Americans.

Affect Upon Constitutional Rights.—That these abuses have adversely affected the constitutional rights of particular Americans is beyond question. But we believe the harm extends far beyond the citizens directly affected.

Personal privacy is protected because it is essential to liberty and the pursuit of happiness. Our Constitution checks the power of Government for the purpose of protecting the rights of individuals, in order that all our citizens may live in a free and decent society. Unlike totalitarian states, we do not believe that any government has a monopoly on truth.

When Government infringes those rights instead of nurturing and protecting them, the injury spreads far beyond the particular citizens targeted to untold numbers of other Americans who may be intimidated.

Free government depends upon the ability of all its citizens to speak their minds without fear of official sanction. The ability of ordinary people to be heard by their leaders means that they must be free to join in groups in order more effectively to express their grievances. Constitutional safeguards are needed to protect the timid as well as the courageous, the weak as well as the strong. While many Americans have been willing to assert their beliefs in the face of possible govern-

mental reprisals, no citizen should have to weigh his or her desire to express an opinion, or join a group, against the risk of having lawful speech or association used against him.

Persons most intimidated may well not be those at the extremes of the political spectrum, but rather those nearer the middle. Yet voices of moderation are vital to balance public debate and avoid polarization of our society.

The federal government has recently been looked to for answers to nearly every problem. The result has been a vast centralization of power. Such power can be turned against the rights of the people. Many of the restraints imposed by the Constitution were designed to guard against such use of power by the government.

Since the end of World War II, governmental power has been increasingly exercised through a proliferation of federal intelligence programs. The very size of this intelligence system, multiplies the opportunities for misuse.

Exposure of the excesses of this huge structure has been necessary. Americans are now aware of the capability and proven willingness of their Government to collect intelligence about their lawful activities and associations. What some suspected and others feared has turned out to be largely true—vigorous expression of unpopular views, association with dissenting groups, participation in peaceful protest activities, have provoked both government surveillance and retaliation.

Over twenty years ago, Supreme Court Justice Robert Jackson, previously an Attorney General, warned against growth of a centralized power of investigation. Without clear limits, a federal investigative agency would “have enough on enough people” so that “even if it does not elect to prosecute them” the Government would, he wrote, still “find no opposition to its policies”. Jackson added, “Even those who are supposed to supervise [intelligence agencies] are likely to fear [them].” His advice speaks directly to our responsibilities today:

I believe that the safeguard of our liberty lies in limiting any national police or investigative organization, first of all to a small number of strictly federal offenses, and secondly to nonpolitical ones. The fact that we may have confidence in the administration of a federal investigative agency under its existing head does not mean that it may not revert again to the days when the Department of Justice was headed by men to whom the investigative power was a weapon to be used for their own purposes.¹

Failure to Apply Checks and Balances.—The natural tendency of Government is toward abuse of power. Men entrusted with power, even those aware of its dangers, tend, particularly when pressured, to slight liberty.

Our constitutional system guards against this tendency. It establishes many different checks upon power. It is those wise restraints which keep men free. In the field of intelligence those restraints have too often been ignored.

¹ Robert H. Jackson, *The Supreme Court in the American System of Government* (New York: Harper Torchbook, 1955, 1963), pp. 70-71.

The three main departures in the intelligence field from the constitutional plan for controlling abuse of power have been:

(a) *Excessive Executive Power.*—In a sense the growth of domestic intelligence activities mirrored the growth of presidential power generally. But more than any other activity, more even than exercise of the war power, intelligence activities have been left to the control of the Executive.

For decades Congress and the courts as well as the press and the public have accepted the notion that the control of intelligence activities was the exclusive prerogative of the Chief Executive and his surrogates. The exercise of this power was not questioned or even inquired into by outsiders. Indeed, at times the power was seen as flowing not from the law, but as inherent in the Presidency. Whatever the theory, the fact was that intelligence activities were essentially exempted from the normal system of checks and balances.

Such Executive power, not founded in law or checked by Congress or the courts, contained the seeds of abuse and its growth was to be expected.

(b) *Excessive Secrecy.*—Abuse thrives on secrecy. Obviously, public disclosure of matters such as the names of intelligence agents or the technological details of collection methods is inappropriate. But in the field of intelligence, secrecy has been extended to inhibit review of the basic programs and practices themselves.

Those within the Executive branch and the Congress who would exercise their responsibilities wisely must be fully informed. The American public, as well, should know enough about intelligence activities to be able to apply its good sense to the underlying issues of policy and morality.

Knowledge is the key to control. Secrecy should no longer be allowed to shield the existence of constitutional, legal and moral problems from the scrutiny of all three branches of government or from the American people themselves.

(c) *Avoidance of the Rule of Law.*—Lawlessness by Government breeds corrosive cynicism among the people and erodes the trust upon which government depends.

Here, there is no sovereign who stands above the law. Each of us, from presidents to the most disadvantaged citizen, must obey the law.

As intelligence operations developed, however, rationalizations were fashioned to immunize them from the restraints of the Bill of Rights and the specific prohibitions of the criminal code. The experience of our investigation leads us to conclude that such rationalizations are a dangerous delusion.

B. Principles Applied in Framing Recommendations and The Scope of the Recommendations.

Although our recommendations are numerous and detailed, they flow naturally from our basic conclusion. Excessive intelligence activity which undermines individual rights must end. The system for controlling intelligence must be brought back within the constitutional scheme.

Some of our proposals are stark and simple. Because certain domestic intelligence activities were clearly wrong, the obvious solution is to prohibit them altogether. Thus, we would ban tactics such as those used

in the FBI's COINTELPRO. But other activities present more complex problems. We see a clear need to safeguard the constitutional rights of speech, assembly, and privacy. At the same time, we do not want to prohibit or unduly restrict necessary and proper intelligence activity.

In seeking to accommodate those sometimes conflicting interests we have been guided by the earlier efforts of those who originally shaped our nation as a republic under law.

The Constitutional amendments protecting speech and assembly and individual privacy seek to preserve values at the core of our heritage and vital to our future. The Bill of Rights, and the Supreme Court's decisions interpreting it suggest three principles which we have followed:

(1) Governmental action which directly infringes the rights of free speech and association must be prohibited. The First Amendment recognizes that even if useful to a proper end, certain governmental actions are simply too dangerous to permit at all. It commands that "Congress shall make *no* law" abridging freedom of speech or assembly.

(2) The Supreme Court, in interpreting that command, has required that any governmental action which has a collateral (rather than direct) impact upon the rights of speech and assembly is permissible only if it meets two tests. First, the action must be undertaken only to fulfill a compelling governmental need, and second, the government must use the least restrictive means to meet that need. The effect upon protected interests must be minimized.²

(3) Procedural safeguards—"auxiliary precautions" as they were characterized in the Federalist Papers³—must be adopted along with substantive restraints. For example, while the Fourth Amendment prohibits only "unreasonable" searches and seizures, it requires a procedural check for reasonableness—the obtaining of a judicial warrant upon probable cause from a neutral magistrate. Our proposed procedural checks range from judicial review of intelligence activity before or after the fact, to formal and high level Executive branch approval, to greater disclosure and more effective Congressional oversight.

The Committee believes that its recommendations should be embodied in a comprehensive legislative charter defining and controlling the domestic security activities of the Federal Government. Accordingly, Part i of the recommendations provides that intelligence agencies must be made subject to the rule of law. In addition, Part i makes clear that no theory, of "inherent constitutional authority" or otherwise, can justify the violation of any statute.

Starting from the conclusion, based upon our record, that the Constitution and our fundamental values require a substantial curtailment

² *De Gregory v. New Hampshire*, 383 U.S. 825, 829 (1966); *NAACP v. Alabama*, 377 U.S. 288 (1964); *Gibson v. Florida Legislative Investigation Commission*, 372 U.S. 539, 546 (1962); *Shelton v. Tucker*, 364 U.S. 479, 488 (1960).

³ Madison, Federalist No. 51. Madison made the point with grace:

"If men were angels, no government would be necessary. If angels were to govern men, neither external nor internal controls on government would be necessary. In framing a government which is to be administered by men over men, the great difficulty lies in this: you must first enable the government to control the governed; and in the next place oblige it to control itself. A dependence on the people is, no doubt, the primary control on the government; but experience has taught mankind the necessity of auxiliary precautions."

of the scope of domestic surveillance, we deal after Part i with five basic questions:

1. Which agencies should conduct domestic security investigations?

The FBI should be primarily responsible for such investigations. Under the minimization principle, and to facilitate the control of domestic intelligence operations, only one agency should be involved in investigative activities which, even when limited as we propose, could give rise to abuse. Accordingly, Part ii of these recommendations reflects the Committee's position that foreign intelligence agencies (the CIA, NSA, and the military agencies) should be precluded from domestic security activity in the United States. Moreover, they should only become involved in matters involving the rights of Americans abroad where it is impractical to use the FBI, or where in the course of their lawful foreign intelligence operations⁴ they inadvertently collect information relevant to domestic security investigations. In Part iii the Committee recommends that non-intelligence agencies such as the Internal Revenue Service and the Post Office be required, in the course of any incidental involvement in domestic security investigations, to protect the privacy which citizens expect of first class mail and tax records entrusted to those agencies.

2. When should an American be the subject of an investigation at all; and when can particularly intrusive covert techniques, such as electronic surveillance or informants, be used?

In Part iv, which deals with the FBI, the Committee's recommendations seek to prevent the excessively broad, ill-defined and open ended investigations shown to have been conducted over the past four decades. We attempt to change the focus of investigations from constitutionally protected advocacy and association to dangerous conduct. Part iv also sets forth specific substantive standards for, and procedural controls on, particular intrusive techniques.

3. Who should be accountable within the Executive branch for ensuring that intelligence agencies comply with the law and for the investigation of alleged abuses by employees of those agencies?

In Parts v and vi, the Committee recommends that these responsibilities fall initially upon the agency heads, their general counsel and inspectors general, but ultimately upon the Attorney General. The information necessary for control must be made available to those responsible for control, oversight and review; and their responsibilities must be made clear, formal, and fixed.

4. What is the appropriate role of the courts?

In Part vii, the Committee recommends the enactment of a comprehensive civil remedy providing the courts with jurisdiction to entertain legitimate complaints by citizens injured by unconstitutional or illegal activities of intelligence agencies. Part viii suggests that criminal penalties should attach in cases of gross abuse. In addition, Part iv provides for judicial warrants before certain intrusive techniques can be used.

5. What is the appropriate role of Congress:

In Part xii the Committee reiterates its position that the Senate create a permanent intelligence oversight committee.

The recommendations deal with numerous other issues such as the proposed repeal or amendment of the Smith Act, the proposed mod-

⁴ Directed primarily at foreigners abroad.

ernization of the Espionage Act to cover modern forms of espionage seriously detrimental to the national interest, the use of the GAO to assist Congressional oversight of the intelligence community, and remedial measures for past victims of improper intelligence activity.

Scope of Recommendations.—The scope of our recommendations coincides with the scope of our investigation. We examined the FBI, which has been responsible for most domestic security investigations, as well as foreign and military intelligence agencies, the IRS, and the Post Office, to the extent they became involved incidentally in domestic intelligence functions. While there are undoubtedly activities of other agencies which might legitimately be addressed in these recommendations, the Committee simply did not have the time or resources to conduct a broader investigation. Furthermore, the mandate of Senate Resolution 21 required that the Committee exclude from the coverage of its recommendations those activities of the federal government which are directed at organized crime and narcotics.

The Committee believes that American citizens should not lose their constitutional rights to be free from improper intrusion by their Government when they travel overseas. Accordingly, the Committee proposes recommendations which apply to protect the rights of Americans abroad as well as at home.

1. Activities Covered

The Domestic Intelligence Recommendations pertain to: the domestic security activities of the federal government;⁵ and any activities of military or foreign intelligence agencies which affect the rights of Americans⁶ and any intelligence activities of any non-intelligence agency working in concert with intelligence agencies, which affect those rights.

2. Activities Not Covered

The recommendations are not designed to control federal investigative activities directed at organized crime, narcotics, or other law enforcement investigations unrelated to domestic security activities.

3. Agencies Covered

The agencies whose activities are specifically covered by the recommendations are:

- (i) the Federal Bureau of Investigation; (ii) the Central Intelligence Agency; (iii) the National Security Agency and other intelligence agencies of the Department of De-

⁵ "Domestic security activities" means federal governmental activities, directed against Americans or conducted within the United States or its territories, including enforcement of the criminal law, intended to (a) protect the United States from hostile foreign intelligence activity, including espionage; (b) protect the federal, state, and local governments from domestic violence or rioting; and (c) protect Americans and their government from terrorist activity. See Part xiii of the recommendations and conclusions for all the definitions used in the recommendations.

⁶ "Americans" means U.S. citizens, resident aliens and unincorporated associations, composed primarily of U.S. citizens or resident aliens; and corporations, incorporated or having their principal place of business in the United States or having majority ownership by U.S. citizens, or resident aliens, including foreign subsidiaries of such corporations, provided, however, Americans does not include corporations directed by foreign governments or organizations.

fense; (iv) the Internal Revenue Service; and (v) the United States Postal Service.

While it might be appropriate to provide similar detailed treatment to the activities of other agencies, such as the Secret Service, Customs Service, and Alcohol, Tobacco, and Firearms Division (Treasury Department), the Committee did not study these agencies intensively. A permanent oversight committee should investigate and study the intelligence functions of those agencies and the effect of their activities on the rights of Americans.

4. Indirect Prohibitions

Except as specifically provided herein, these Recommendations are intended to prohibit any agency from doing indirectly that which it would be prohibited from doing directly. Specifically, no agency covered by these Recommendations should request or induce any other agency, or any person, whether the agency or person is American or foreign, to engage in any activity which the requesting or inducing agency is prohibited from doing itself.

5. Individuals and Groups Not Covered

Except as specifically provided herein, these Recommendations do not apply to investigation of foreigners⁷ who are officers or employees of a foreign power, or foreigners who, pursuant to the direction of a foreign power, are engaged in or about to engage in "hostile foreign intelligence activity" or "terrorist activity".⁸

6. Geographic Scope

These Recommendations apply to intelligence activities which affect the rights of Americans whether at home or abroad, including all domestic security activities within the United States.

7. Legislative Enactment of Recommendations

Most of these Recommendations are designed to be implemented in the form of legislation and others in the form of regulations pursuant to statute. (Recommendations 85 and 90 are not proposed to be implemented by statute.)

C. Recommendations

Pursuant to the requirement of Senate Resolution 21, these recommendations set forth the new congressional legislation [the Committee] deems necessary to "safeguard the rights of American citizens."⁹ We believe these recommendations are the appropriate conclusion to a traumatic year of disclosures of abuses. We hope they will prevent such abuses in the future.

i. Intelligence Agencies Are Subject to the Rule of Law

Establishing a legal framework for agencies engaged in domestic security investigation is the most fundamental reform needed to end the long history of violating and ignoring the law set forth in Finding A. The legal framework can be created by a two-stage process of enabling legislation and administrative regulations promulgated to implement the legislation.

⁷ "Foreigners" means persons and organizations who are not Americans as defined above.

⁸ These terms, which cover the two areas in which the Committee recommends authorizing preventive intelligence investigations, are defined on pp. 340-341.

⁹ S. Res. 21, Sec. 5; 2(12).

However, the Committee proposes that the Congress, in developing this mix of legislative and administrative charters, make clear to the Executive branch that it will not condone, and does not accept, any theory of inherent or implied authority to violate the Constitution, the proposed new charters, or any other statutes. We do not believe the Executive has, or should have, the inherent constitutional authority to violate the law or infringe the legal rights of Americans, whether it be a warrantless break-in into the home or office of an American, warrantless electronic surveillance, or a President's authorization to the FBI to create a massive domestic security program based upon secret oral directives. Certainly, there would be no such authority after Congress has, as we propose it should, covered the field by enactment of a comprehensive legislative charter.¹⁰ Therefore statutes enacted pursuant to these recommendations should provide the exclusive legal authority for domestic security activities.

Recommendation 1.—There is no inherent constitutional authority for the President or any intelligence agency to violate the law.

Recommendation 2.—It is the intent of the Committee that statutes implementing these recommendations provide the exclusive legal authority for federal domestic security activities.

(a) No intelligence agency may engage in such activities unless authorized by statute, nor may it permit its employees, informants, or other covert human sources¹¹ to engage in such activities on its behalf.

(b) No executive directive or order may be issued which would conflict with such statutes.

Recommendation 3.—In authorizing intelligence agencies to engage in certain activities, it is not intended that such authority empower agencies, their informants, or covert human sources to violate any prohibition enacted pursuant to these Recommendations or contained in the Constitution or in any other law.

ii. United States Foreign and Military Agencies Should Be Precluded from Domestic Security Activities

Part iv of these Recommendations centralizes domestic security investigations within the FBI. Past abuses also make it necessary that the Central Intelligence Agency, the National Security Agency, the Defense Intelligence Agency, and the military departments be precluded expressly, except as specifically provided herein, from investigative activity which is conducted within the United States. Their activities abroad should also be controlled as provided herein to minimize their impact on the rights of Americans.

a. Central Intelligence Agency

The CIA is responsible for foreign intelligence and counterintelligence. These recommendations minimize the impact of CIA operations on Americans. They do not affect CIA investigations of foreigners outside of the United States. The main thrust is to prohibit past actions revealed as excessive, and to transfer to the FBI other activities which might involve the CIA in internal security or law enforce-

¹⁰ See, e.g., *Youngstown Sheet and Tube Company v. Sawyer*, 343 U.S. 579 (1952).

¹¹ "Covert human sources" means undercover agents or informants who are paid or otherwise controlled by an agency.

domestic communications, even for foreign intelligence purposes. Second, the Committee recommends that NSA should not select messages for monitoring, from those foreign communications it has intercepted, because the message is to or from or refers to a particular American, unless the Department of Justice has first obtained a search warrant, or the particular American has consented. Third, the Committee recommends that NSA be required to make every practicable effort to eliminate or minimize the extent to which the communications of Americans are intercepted, selected, or monitored. Fourth, for those communications of Americans which are nevertheless incidentally selected and monitored, the Committee recommends that NSA be prohibited from disseminating such communication, or information derived therefrom, which identifies an American, unless the communication indicates evidence of hostile foreign intelligence or terrorist activity, or felonious criminal conduct, or contains a threat of death or serious bodily harm. In these cases, the Committee recommends that the Attorney General approve any such dissemination as being consistent with these policies.

In summary, the Committee's recommendations reflect its belief that NSA should have no greater latitude to monitor the communications of Americans than any other intelligence agency. To the extent that other agencies are required to obtain a warrant before monitoring the communications of Americans, NSA should be required to obtain a warrant.³⁴

Recommendation 14.—NSA should not engage in domestic security activities. Its functions should be limited in a precisely drawn legislative charter to the collection of foreign intelligence from foreign communications.³⁵

Recommendation 15.—NSA should take all practicable measures consistent with its foreign intelligence mission to eliminate or minimize the interception, selection, and monitoring of communications of Americans from the foreign communications.³⁶

Recommendation 16.—NSA should not be permitted to select for monitoring any communication to, from, or about an American without his consent, except for the purpose of obtaining information about hostile foreign intelligence or terrorist activities, and then only if a warrant approving such monitoring is obtained in accordance with procedures similar³⁷ to those contained in Title III of the Omnibus Crime Control and Safe Streets Act of 1968.

³⁴ None of the Committee's recommendations pertaining to NSA should be construed as inhibiting or preventing NSA from protecting U.S. communications against interception or monitoring by foreign intelligence services.

³⁵ "Foreign communications," as used in this section, refers to a communication between or among two or more parties in which at least one party is outside the United States, or a communication transmitted between points within the United States only if transmitted over a facility which is under the control of, or exclusively used by, a foreign government.

³⁶ In order to ensure that this recommendation is implemented, both the Attorney General and the appropriate oversight committees of the Congress should be continuously apprised of, and periodically review, the measures taken by NSA pursuant to this recommendation.

³⁷ The Committee believes that in the case of interceptions authorized to obtain information about hostile foreign intelligence, there should be a presumption that notice to the subject of such intercepts, which would ordinarily be required under Title III (18 U.S.C. 2518(8)(d)), is not required, unless there is evidence of gross abuse.

vi. Administrative Rulemaking and Increased Disclosure Should Be Required

a. Administrative Rulemaking

Recommendation 86.—The Attorney General should approve all administrative regulations required to implement statutes created pursuant to these recommendations.

Recommendation 87.—Such regulations, except for regulations concerning investigations of hostile foreign intelligence activity or other matters which are properly classified, should be issued pursuant to the Administrative Procedures Act and should be subject to the approval of the Attorney General.

Recommendation 88.—The effective date of regulations pertaining to the following matters should be delayed ninety days, during which time Congress would have the opportunity to review such regulations:⁶⁵

- (a) Any CIA activities against Americans, as permitted in ii.a. above;
- (b) Military activities at the time of a civil disorder;
- (c) The authorized scope of domestic security investigations, authorized investigative techniques, maintenance and dissemination of information by the FBI; and
- (d) The termination of investigations and covert techniques as described in Part iv.

b. Disclosure

Recommendation 89.—Each year the FBI and other intelligence agencies affected by these recommendations should be required to seek annual statutory authorization for their programs.

Recommendation 90.—The Freedom of Information Act (5 U.S.C. 552(b)) and the Federal Privacy Act (5 U.S.C. 552(a)) provide important mechanisms by which individuals can gain access to information on intelligence activity directed against them. The Domestic Intelligence Recommendations assume that these statutes will continue to be vigorously enforced. In addition, the Department of Justice should notify all readily identifiable targets of past illegal surveillance techniques, and all COINTELPRO victims, and third parties who had received anonymous COINTELPRO communications, of the nature of the activities directed against them, or the source of the anonymous communication to them.^{65a}

vii. Civil Remedies Should Be Expanded

Recommendation 91 expresses the Committee's concern for establishing a legislative scheme which will afford effective redress to people who are injured by improper federal intelligence activity. The recommended provisions for civil remedies are also intended to deter improper intelligence activity without restricting the sound exercise of discretion by intelligence officers at headquarters or in the field.

As the Committee's investigation has shown, many Americans have suffered injuries from domestic intelligence activity, ranging from deprivation of constitutional rights of privacy and free speech to the loss of a job or professional standing, break-up of a marriage, and impairment of physical or mental health. But the extent, if any, to

⁶⁵ This review procedure would be similar to the procedure followed with respect to the promulgation of the Federal Rules of Criminal and Civil Procedure.

^{65a} It is not proposed that this recommendation be enacted as a statute.

which an injured citizen can seek relief—either monetary or injunctive—from the government or from an individual intelligence officer is far from clear under the present state of the law.

One major disparity in the current state of the law is that, under the Reconstruction era Civil Rights Act of 1871, the deprivation of constitutional rights by an officer or agent of a state government provides the basis for a suit to redress the injury incurred;⁶⁶ but there is no statute which extends the same remedies for identical injuries when they are caused by a federal officer.

In the landmark *Bivens* case, the Supreme Court held that a federal officer could be sued for money damages for violating a citizen's Fourth Amendment rights.⁶⁷ Whether monetary damages can be obtained for violation of other constitutional rights by federal officers remains unclear.

While we believe that any citizen with a substantial and specific claim to injury from intelligence activity should have standing to sue, the Committee is aware of the need for judicial protection against legal claims which amount to harassment or distraction of government officials, disruption of legitimate investigations, and wasteful expenditure of government resources. We also seek to ensure that the creation of a civil remedy for aggrieved persons does not impinge upon the proper exercise of discretion by federal officials.

Therefore, we recommend that where a government official—as opposed to the government itself—acted in good faith and with the reasonable belief that his conduct was lawful, he should have an affirmative defense to a suit for damages brought under the proposed statute. To tighten the system of accountability and control of domestic intelligence activity, the Committee proposes that this defense be structured to encourage intelligence officers to obtain written authorization for questionable activities and to seek legal advice about them.⁶⁸

To avoid penalizing federal officers and agents for the exercise of discretion, the Committee believes that the government should indemnify their attorney fees and reasonable litigation costs when they are held not to be liable. To avoid burdening the taxpayers for the deliberate misconduct of intelligence officers and agents, we believe the government should be able to seek reimbursement from those who willfully and knowingly violate statutory charters or the Constitution.

Furthermore, we believe that the courts will be able to fashion discovery procedures, including inspection of material in chambers, and to issue orders as the interests of justice require, to allow plaintiffs with substantial claims to uncover enough factual material to argue their case, while protecting the secrecy of governmental information in which there is a legitimate security interest.

The Committee recommends that a legislative scheme of civil remedies for the victims of intelligence activity be established along the

⁶⁶ 42 U.S.C. 1983.

⁶⁷ *Bivens v. Six Unknown Fed. Narcotics Agents*, 403 U.S. 388 (1971).

⁶⁸ One means of structuring such a defense would be to create a rebuttable presumption that an individual defendant acted so as to avail himself of this defense when he proves that he acted in good faith reliance upon: (1) a written order or directive by a government officer empowered to authorize him to take action; or (2) a written assurance by an appropriate legal officer that his action is lawful.

following lines to clarify the state of the law, to encourage the responsible execution of duties created by the statutes recommended herein to regulate intelligence agencies, and to provide relief for the victims of illegal intelligence activity.

Recommendation 91.—Congress should enact a comprehensive civil remedies statute which would accomplish the following:⁶⁹

(a) Any American with a substantial and specific claim⁷⁰ to an actual or threatened injury by a violation of the Constitution by federal intelligence officers or agents⁷¹ acting under color of law should have a federal cause of action against the government and the individual federal intelligence officer or agent responsible for the violation, without regard to the monetary amount in controversy. If actual injury is proven in court, the Committee believes that the injured person should be entitled to equitable relief, actual, general, and punitive damages, and recovery of the costs of litigation.⁷² If threatened injury is proven in court, the Committee believes that equitable relief and recovery of the costs of litigation should be available.

(b) Any American with a substantial and specific claim to actual or threatened injury by violation of the statutory charter for intelligence activity (as proposed by these Domestic Intelligence Recommendations) should have a cause of action for relief as in (a) above.

(c) Because of the secrecy that surrounds intelligence programs, the Committee believes that a plaintiff should have two years from the date upon which he discovers, or reasonably should have discovered, the facts which give rise to a cause of action for relief from a constitutional or statutory violation.

(d) Whatever statutory provision may be made to permit an individual defendant to raise an affirmative defense that he acted within the scope of his official duties, in good faith, and with a reasonable belief that the action he took was lawful, the Committee believes that to ensure relief to persons injured by governmental intelligence activity, this defense should be available solely to individual defendants and should not extend to the government. Moreover, the defense should not be available to bar injunctions against individual defendants.

viii. Criminal Penalties Should Be Enacted

Recommendation 92.—The Committee believes that criminal penalties should apply, where appropriate, to willful and knowing

⁶⁹ Due to the scope of the Committee's mandate, we have taken evidence only on constitutional violations by intelligence officers and agents. However, the anomalies and lack of clarity in the present state of the law (as discussed above) and the breadth of constitutional violations revealed by our record, suggest to us that a general civil remedy would be appropriate. Thus, we urge consideration of a statutory civil remedy for constitutional violations by any federal officer; and we encourage the appropriate committees of the Congress to take testimony on this subject.

⁷⁰ The requirement of a substantial and specific claim is intended to allow a judge to screen out frivolous claims where a plaintiff cannot allege specific facts which indicate that he was the target of illegal intelligence activity.

⁷¹ "Federal intelligence officers or agents" should include a person who was an intelligence officer, employee, or agent at the time a cause of action arose. "Agent" should include anyone acting with actual, implied, or apparent authority.

⁷² The right to recover "costs of litigation" is intended to include recovery of reasonable attorney fees as well as other litigation costs reasonably incurred.

EXHIBIT B

Search

How do I find it?

Subscribe to paper



Home

News

Travel

Money

Sports

Life

Tech

Weather

Washington/Politics

Inside News

Cars Event tickets Jobs Real estate Shop Online degrees

NSA has massive database of Americans' phone calls

Updated 5/11/2006 10:38 AM ET

E-mail | Print | Reprints & Permissions |

By Leslie Cauley, USA TODAY



Enlarge By Roger Wollenberg, Getty Images

Gen. Michael Hayden, nominated by President Bush to become the director of the CIA, headed the NSA from March 1999 to April 2005. In that post, Hayden would have overseen the agency's domestic phone record collection program.

The National Security Agency has been secretly collecting the phone call records of tens of millions of Americans, using data provided by AT&T, Verizon and BellSouth, people with direct knowledge of the arrangement told USA TODAY.

The NSA program reaches into homes and businesses across the nation by amassing information about the calls of ordinary Americans — most of whom aren't suspected of any crime. This program does not involve the NSA listening to or recording conversations. But the spy agency is using the data to analyze calling patterns in an effort to detect terrorist activity, sources said in separate interviews.

QUESTIONS AND ANSWERS: The NSA record collection program

"It's the largest database ever assembled in the world," said one person, who, like the others who agreed to talk about the NSA's activities, declined to be identified by name or affiliation. The agency's goal is "to create a database of every call ever made" within the nation's borders, this person added.

For the customers of these companies, it means that the government has detailed records of calls they made — across town or across the country — to family members, co-workers, business contacts and others.

The three telecommunications companies are working under contract with the NSA, which launched the program in 2001 shortly after the Sept. 11 terrorist attacks, the sources said. The program is aimed at identifying and tracking suspected terrorists, they said.

The sources would talk only under a guarantee of anonymity because the NSA program is secret.

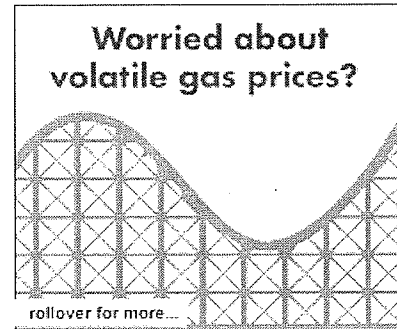
Air Force Gen. Michael Hayden, nominated Monday by President Bush to become the director of the CIA, headed the NSA from March 1999 to April 2005. In that post, Hayden would have overseen the agency's domestic call-tracking program. Hayden declined to comment about the program.

The NSA's domestic program, as described by sources, is far more expansive than what the White House has acknowledged. Last year, Bush said he had authorized the NSA to eavesdrop — without warrants — on international calls and international e-mails of people suspected of having links to terrorists when one party to the communication is in the USA. Warrants have also not been used in the NSA's efforts to create a national call database.

In defending the previously disclosed program, Bush insisted that the NSA was focused exclusively on international calls. "In other words," Bush explained, "one end of the communication must be outside the United States."

As a result, domestic call records — those of calls that originate and terminate within U.S. borders — were believed to be private.

Sources, however, say that is not the case. With access to



REACTION

From the White House:

The White House defended its overall eavesdropping program and said no domestic surveillance is conducted without court approval.

"The intelligence activities undertaken by the United States government are lawful, necessary and required to protect Americans from terrorist attacks," said Dana Perino, the deputy White House press secretary, who added that appropriate members of Congress have been briefed on intelligence activities.

From Capitol Hill:

Sen. Arlen Specter, R-Pa., the chairman of the Senate Judiciary Committee, said he would call the phone companies to appear before the panel "to find out exactly what is going on."

Sen. Patrick Leahy of Vermont, the ranking Democrat on the panel, sounded incredulous about the latest report and railed against what he called a lack of congressional oversight. He argued that the media was doing the job of Congress.

"Are you telling me that tens of millions of Americans are involved with al Qaeda?" Leahy asked. "These are tens of millions of Americans who are not suspected of anything ... Where does it stop?"

The Democrat, who at one point held up a copy of the newspaper, added: "Shame on us for being so far behind and being so willing to rubber stamp anything this administration does. We ought to fold our tents."

The report came as the former NSA director, Gen. Michael Hayden - Bush's choice to take over leadership of the CIA - had been scheduled to visit lawmakers on Capitol Hill Thursday. However, the meetings with Republican Sens. Rick Santorum of Pennsylvania and Lisa Murkowski of Alaska were postponed at the request of the White House, said congressional aides in the two Senate offices.

Source: *The Associated Press*

NSA SURVEILLANCE

Opinion: Congress in the dark
| Specter: My bill would
provide light



ACLU, NSA to head to court

VP pressured panel, Specter
says



Senators won't grill phone companies

FCC: NSA probe impossible

Pre-9/11 records help flag
suspicious calling



More

records of billions of domestic calls, the NSA has gained a secret window into the communications habits of millions of Americans. Customers' names, street addresses and other personal information are not being handed over as part of NSA's domestic program, the sources said. But the phone numbers the NSA collects can easily be cross-checked with other databases to obtain that information.

Don Weber, a senior spokesman for the NSA, declined to discuss the agency's operations. "Given the nature of the work we do, it would be irresponsible to comment on actual or alleged operational issues; therefore, we have no information to provide," he said. "However, it is important to note that NSA takes its legal responsibilities seriously and operates within the law."

The White House would not discuss the domestic call-tracking program. "There is no domestic surveillance without court approval," said Dana Perino, deputy press secretary, referring to actual eavesdropping.

She added that all national intelligence activities undertaken by the federal government "are lawful, necessary and required for the pursuit of al-Qaeda and affiliated terrorists." All government-sponsored intelligence activities "are carefully reviewed and monitored," Perino said. She also noted that "all appropriate members of Congress have been briefed on the intelligence efforts of the United States."

The government is collecting "external" data on domestic phone calls but is not intercepting "internals," a term for the actual content of the communication, according to a U.S. intelligence official familiar with the program. This kind of data collection from phone companies is not uncommon; it's been done before, though never on this large a scale, the official said. The data are used for "social network analysis," the official said, meaning to study how terrorist networks contact each other and how they are tied together.

Carriers uniquely positioned

AT&T recently merged with SBC and kept the AT&T name. Verizon, BellSouth and AT&T are the nation's three biggest telecommunications companies; they provide local and wireless phone service to more than 200 million customers.

The three carriers control vast networks with the latest communications technologies. They provide an array of services: local and long-distance calling, wireless and high-speed broadband, including video. Their direct access to millions of homes and businesses has them uniquely positioned to help the government keep tabs on the calling habits of Americans.

Among the big telecommunications companies, only Qwest has refused to help the NSA, the sources said. According to multiple sources, Qwest declined to participate because it was uneasy about the legal implications of handing over customer information to the government without warrants.

Qwest's refusal to participate has left the NSA with a hole in its database. Based in Denver, Qwest provides local phone service to 14 million customers in 14 states in the West and Northwest. But AT&T and Verizon also provide some services — primarily long-distance and wireless — to people who live in Qwest's region. Therefore, they can provide the NSA with at least some access in that area.

Created by President Truman in 1952, during the Korean War, the NSA is charged with protecting the United States from foreign security threats. The agency was considered so secret that for years the government refused to even confirm its existence. Government insiders used to joke that NSA stood for "No Such Agency."

In 1975, a congressional investigation revealed that the NSA had been intercepting, without warrants, international communications for more than 20 years at the behest of the CIA and other agencies. The spy campaign, code-named "Shamrock," led to the Foreign Intelligence Surveillance Act (FISA), which was designed to protect Americans from illegal eavesdropping.

Enacted in 1978, FISA lays out procedures that the U.S. government must follow to conduct electronic surveillance and

TIMELINE

OFFICIAL WORDS ON SURVEILLANCE

Bush administration officials have said repeatedly that the warrantless surveillance program authorized by President Bush after the Sept. 11 terrorist attacks is carefully targeted to include only international calls and e-mails into or out of the USA, and only those that involve at least one party suspected of being a member or ally of al-Qaeda or a related terror group.

Some comments related to what the administration calls the "Terrorist Surveillance

Program," and surveillance in general:

Gen. Michael Hayden, principal deputy director of national intelligence, and now Bush's nominee to head the CIA, at the National Press Club, Jan. 23, 2006:

"The program ... is not a drift net over (U.S. cities such as) Dearborn or Lackawanna or Fremont, grabbing conversations that we then sort out by these alleged keyword searches or data-mining tools or other devices that so-called experts keep talking about.

"This is targeted and focused. This is not about intercepting conversations between people in the United States. This is not pursuit of communications entering or leaving America involving someone we believe is associated with al-Qaeda. ... This is focused. It's targeted. It's very carefully done. You shouldn't worry."

Senate Judiciary Committee hearing, Feb. 6, 2006:

Attorney General Alberto Gonzales: "Only international communications are authorized for interception under this program. That is, communications between a foreign country and this country. ...

"To protect the privacy of Americans still further, the NSA employs safeguards to minimize the unnecessary collection and dissemination of information about U.S. persons."

Sen. Joseph Biden, D-Del.: "I don't understand why you would limit your eavesdropping only to foreign conversations. ..."

Gonzales: "I believe it's because of trying to balance concerns that might arise that, in fact, the NSA was engaged in electronic surveillance with respect to domestic calls."

physical searches of people believed to be engaged in espionage or international terrorism against the United States. A special court, which has 11 members, is responsible for adjudicating requests under FISA.

Over the years, NSA code-cracking techniques have continued to improve along with technology. The agency today is considered expert in the practice of "data mining" — sifting through reams of information in search of patterns. Data mining is just one of many tools NSA analysts and mathematicians use to crack codes and track international communications.

Paul Butler, a former U.S. prosecutor who specialized in terrorism crimes, said FISA approval generally isn't necessary for government data-mining operations. "FISA does not prohibit the government from doing data mining," said Butler, now a partner with the law firm Akin Gump Strauss Hauer & Feld in Washington, D.C.

The caveat, he said, is that "personal identifiers" — such as names, Social Security numbers and street addresses — can't be included as part of the search. "That requires an additional level of probable cause," he said.

The usefulness of the NSA's domestic phone-call database as a counterterrorism tool is unclear. Also unclear is whether the database has been used for other purposes.

The NSA's domestic program raises legal questions. Historically, AT&T and the regional phone companies have required law enforcement agencies to present a court order before they would even consider turning over a customer's calling data. Part of that owed to the personality of the old Bell Telephone System, out of which those companies grew.

Ma Bell's bedrock principle — protection of the customer — guided the company for decades, said Gene Kimmelman, senior public policy director of Consumers Union. "No court order, no customer information — period. That's how it was for decades," he said.

The concern for the customer was also based on law: Under Section 222 of the Communications Act, first passed in 1934, telephone companies are prohibited from giving out information regarding their customers' calling habits: whom a person calls, how often and what routes those calls take to reach their final destination. Inbound calls, as well as wireless calls, also are covered.

The financial penalties for violating Section 222, one of many privacy reinforcements that have been added to the law over the years, can be stiff. The Federal Communications Commission, the nation's top telecommunications regulatory agency, can levy fines of up to \$130,000 per day per violation, with a cap of \$1.325 million per violation. The FCC has no hard definition of "violation." In practice, that means a single "violation" could cover one customer or 1 million.

In the case of the NSA's international call-tracking program, Bush signed an executive order allowing the NSA to engage in eavesdropping without a warrant. The president and his representatives have since argued that an executive order was sufficient for the agency to proceed. Some civil liberties groups, including the American Civil Liberties Union, disagree.

Companies approached

The NSA's domestic program began soon after the Sept. 11 attacks, according to the sources. Right around that time, they said, NSA representatives approached the nation's biggest telecommunications companies. The agency made an urgent pitch: National security is at risk, and we need your help to protect the country from attacks.

The agency told the companies that it wanted them to turn over their "call-detail records," a complete listing of the calling histories of their millions of customers. In addition, the NSA wanted the carriers to provide updates, which would enable the agency to keep tabs on the nation's calling habits.

The sources said the NSA made clear that it was willing to pay for the cooperation. AT&T, which at the time was headed by C. Michael Armstrong, agreed to help the NSA. So did BellSouth, headed by F. Duane Ackerman; SBC, headed by Ed Whitacre; and Verizon, headed by Ivan Seidenberg.

With that, the NSA's domestic program began in earnest.

AT&T, when asked about the program, replied with a comment prepared for USA TODAY: "We do not comment on matters of national security, except to say that we only assist law enforcement and government agencies charged with protecting national security in strict accordance with the law."

In another prepared comment, BellSouth said: "BellSouth does not provide any confidential customer information to the NSA or any governmental agency without proper legal authority."

Verizon, the USA's No. 2 telecommunications company behind AT&T, gave this statement: "We do not comment on national security matters, we act in full compliance with the law and we are committed to safeguarding our customers' privacy."

Qwest spokesman Robert Charton said: "We can't talk about this. It's a classified situation."

In December, *The New York Times* revealed that Bush had authorized the NSA to wiretap, without warrants, international phone calls and e-mails that travel to or from the USA. The following month, the Electronic Frontier Foundation, a civil liberties group, filed a class-action lawsuit against AT&T. The lawsuit accuses the company of helping the NSA spy on U.S. phone customers.

Last month, U.S. Attorney General Alberto Gonzales alluded to that possibility. Appearing at a House Judiciary Committee hearing, Gonzales was asked whether he thought the White House has the legal authority to monitor domestic traffic without a warrant. Gonzales' reply: "I wouldn't rule it out." His comment marked the first time a Bush appointee publicly asserted that the White House might have that authority.

Similarities in programs

The domestic and international call-tracking programs have things in common, according to the sources. Both are being conducted without warrants and without the approval of the FISA court. The Bush administration has argued that FISA's procedures are too slow in some cases. Officials, including Gonzales, also make the case that the USA Patriot Act gives them broad authority to protect the safety of the nation's citizens.

The chairman of the Senate Intelligence Committee, Sen. Pat Roberts, R-Kan., would not confirm the existence of the program. In a statement, he said, "I can say generally, however, that our subcommittee has been fully briefed on all aspects of the Terrorist Surveillance Program. ... I remain convinced that the program authorized by the president is lawful and absolutely necessary to protect this nation from future attacks."

The chairman of the House Intelligence Committee, Rep. Pete Hoekstra, R-Mich., declined to comment.

One company differs

One major telecommunications company declined to participate in the program: Qwest.

According to sources familiar with the events, Qwest's CEO at the time, Joe Nacchio, was deeply troubled by the NSA's assertion that Qwest didn't need a court order — or approval under FISA — to proceed. Adding to the tension, Qwest was unclear about who, exactly, would have access to its customers' information and how that information might be used.

Financial implications were also a concern, the sources said. Carriers that illegally divulge calling information can be subjected to heavy fines. The NSA was asking Qwest to turn over millions of records. The fines, in the aggregate, could have been substantial.

The NSA told Qwest that other government agencies, including the FBI, CIA and DEA, also might have access to the database, the sources said. As a matter of practice, the NSA regularly shares its information — known as "product" in intelligence circles — with other intelligence groups. Even so, Qwest's lawyers were troubled by the expansiveness of the NSA request, the sources said.

The NSA, which needed Qwest's participation to completely cover the country, pushed back hard.

Trying to put pressure on Qwest, NSA representatives pointedly told Qwest that it was the lone holdout among the big telecommunications companies. It also tried appealing to Qwest's patriotic side: In one meeting, an NSA representative suggested that Qwest's refusal to contribute to the database could compromise national security, one person recalled.

In addition, the agency suggested that Qwest's foot-dragging might affect its ability to get future classified work with the government. Like other big telecommunications companies, Qwest already had classified contracts and hoped to get more.

Unable to get comfortable with what NSA was proposing, Qwest's lawyers asked NSA to take its proposal to the FISA court. According to the sources, the agency refused.

The NSA's explanation did little to satisfy Qwest's lawyers. "They told (Qwest) they didn't want to do that because FISA might not agree with them," one person recalled. For similar reasons, this person said, NSA rejected Qwest's suggestion of getting a letter of authorization from the U.S. attorney general's office. A second person confirmed this version of events.


In June 2002, Nacchio resigned amid allegations that he had misled investors about Qwest's financial health. But Qwest's legal questions about the NSA request remained.

Unable to reach agreement, Nacchio's successor, Richard Notebaert, finally pulled the plug on the NSA talks in late 2004, the sources said.

Contributing: John Diamond

Posted 5/10/2006 11:16 PM ET

Updated 5/11/2006 10:38 AM ET

E-mail | Print | Reprints & Permissions | 

Newspaper Home Delivery - Subscribe Today

Home • News • Travel • Money • Sports • Life • Tech • Weather

About USATODAY.com: Site Map | FAQ | Contact Us | Jobs with Us | Terms of Service
 Privacy Policy/Your California Privacy Right | Advertise | Press Room | Developer | Media Lounge | Reprints and Permissions

News Your Way: Mobile News | Email News | Add USATODAY.com RSS feeds | Twitter | Podcasts | Widgets

Partners: USA WEEKEND | Sports Weekly | Education | Space.com | Travel Tips

EXHIBIT C

The New York Times
nytimes.com



December 16, 2005

Bush Lets U.S. Spy on Callers Without Courts

By JAMES RISEN and ERIC LICHTBLAU

Correction Appended

WASHINGTON, Dec. 15 - Months after the Sept. 11 attacks, President Bush secretly authorized the National Security Agency to eavesdrop on Americans and others inside the United States to search for evidence of terrorist activity without the court-approved warrants ordinarily required for domestic spying, according to government officials.

Under a presidential order signed in 2002, the intelligence agency has monitored the international telephone calls and international e-mail messages of hundreds, perhaps thousands, of people inside the United States without warrants over the past three years in an effort to track possible "dirty numbers" linked to Al Qaeda, the officials said. The agency, they said, still seeks warrants to monitor entirely domestic communications.

The previously undisclosed decision to permit some eavesdropping inside the country without court approval was a major shift in American intelligence-gathering practices, particularly for the National Security Agency, whose mission is to spy on communications abroad. As a result, some officials familiar with the continuing operation have questioned whether the surveillance has stretched, if not crossed, constitutional limits on legal searches.

"This is really a sea change," said a former senior official who specializes in national security law. "It's almost a mainstay of this country that the N.S.A. only does foreign searches."

Nearly a dozen current and former officials, who were granted anonymity because of the classified nature of the program, discussed it with reporters for The New York Times because of their concerns about the operation's legality and oversight.

According to those officials and others, reservations about aspects of the program have also been expressed by Senator John D. Rockefeller IV, the West Virginia Democrat who is the vice chairman of the Senate Intelligence Committee, and a judge presiding over a secret court that oversees intelligence matters. Some of the questions about the agency's new powers led the administration to temporarily suspend the operation last year and impose more restrictions, the officials said.

The Bush administration views the operation as necessary so that the agency can move quickly to monitor communications that may disclose threats to the United States, the officials said. Defenders of the program say it has been a critical tool in helping disrupt terrorist plots and prevent attacks inside the United States.

Administration officials are confident that existing safeguards are sufficient to protect the privacy and civil liberties of Americans, the officials say. In some cases, they said, the Justice Department eventually seeks warrants if it wants to expand the eavesdropping to include communications confined within the United States. The officials said the administration had briefed Congressional leaders about the program and notified the judge in charge of the Foreign Intelligence Surveillance Court, the secret Washington court that deals with national security issues.

The White House asked The New York Times not to publish this article, arguing that it could jeopardize continuing investigations and alert would-be terrorists that they might be under scrutiny. After meeting with senior administration officials to hear their concerns, the newspaper delayed publication for a year to conduct additional reporting. Some information that administration officials argued could be useful to terrorists has been omitted.

Dealing With a New Threat

While many details about the program remain secret, officials familiar with it say the N.S.A. eavesdrops without warrants on up to 500 people in the United States at any given time. The list changes as some names are added and others dropped, so the number monitored in this country may have reached into the thousands since the program began, several officials said. Overseas, about 5,000 to 7,000 people suspected of terrorist ties are monitored at one time, according to those officials.

Several officials said the eavesdropping program had helped uncover a plot by Lyman Faris, an Ohio trucker and naturalized citizen who pleaded guilty in 2003 to supporting Al Qaeda by planning to bring down the Brooklyn Bridge with blowtorches. What appeared to be another Qaeda plot, involving fertilizer bomb attacks on British pubs and train stations, was exposed last year in part through the program, the officials said. But they said most people targeted for N.S.A. monitoring have never been charged with a crime, including an Iranian-American doctor in the South who came under suspicion because of what one official described as dubious ties to [Osama bin Laden](#).

The eavesdropping program grew out of concerns after the Sept. 11 attacks that the nation's intelligence agencies were not poised to deal effectively with the new threat of Al Qaeda and that they were handcuffed by legal and bureaucratic restrictions better suited to peacetime than war, according to officials. In response, President Bush significantly eased limits on American intelligence and law enforcement agencies and the

military.

But some of the administration's antiterrorism initiatives have provoked an outcry from members of Congress, watchdog groups, immigrants and others who argue that the measures erode protections for civil liberties and intrude on Americans' privacy.

Opponents have challenged provisions of the USA Patriot Act, the focus of contentious debate on Capitol Hill this week, that expand domestic surveillance by giving the Federal Bureau of Investigation more power to collect information like library lending lists or Internet use. Military and F.B.I. officials have drawn criticism for monitoring what were largely peaceful antiwar protests. The Pentagon and the Department of Homeland Security were forced to retreat on plans to use public and private databases to hunt for possible terrorists. And last year, the Supreme Court rejected the administration's claim that those labeled "enemy combatants" were not entitled to judicial review of their open-ended detention.

Mr. Bush's executive order allowing some warrantless eavesdropping on those inside the United States - including American citizens, permanent legal residents, tourists and other foreigners - is based on classified legal opinions that assert that the president has broad powers to order such searches, derived in part from the September 2001 Congressional resolution authorizing him to wage war on Al Qaeda and other terrorist groups, according to the officials familiar with the N.S.A. operation.

The National Security Agency, which is based at Fort Meade, Md., is the nation's largest and most secretive intelligence agency, so intent on remaining out of public view that it has long been nicknamed "No Such Agency." It breaks codes and maintains listening posts around the world to eavesdrop on foreign governments, diplomats and trade negotiators as well as drug lords and terrorists. But the agency ordinarily operates under tight restrictions on any spying on Americans, even if they are overseas, or disseminating information about them.

What the agency calls a "special collection program" began soon after the Sept. 11 attacks, as it looked for new tools to attack terrorism. The program accelerated in early 2002 after the Central Intelligence Agency started capturing top Qaeda operatives overseas, including Abu Zubaydah, who was arrested in Pakistan in March 2002. The C.I.A. seized the terrorists' computers, cellphones and personal phone directories, said the officials familiar with the program. The N.S.A. surveillance was intended to exploit those numbers and addresses as quickly as possible, they said.

In addition to eavesdropping on those numbers and reading e-mail messages to and from the Qaeda figures, the N.S.A. began monitoring others linked to them, creating an expanding chain. While most of the numbers and addresses were overseas, hundreds were in the United States, the officials said.

Under the agency's longstanding rules, the N.S.A. can target for interception phone calls or e-mail messages on foreign soil, even if the recipients of those communications are in the United States. Usually, though, the government can only target phones and e-mail messages in the United States by first obtaining a court order from the Foreign Intelligence Surveillance Court, which holds its closed sessions at the Justice Department.

Traditionally, the F.B.I., not the N.S.A., seeks such warrants and conducts most domestic eavesdropping. Until the new program began, the N.S.A. typically limited its domestic surveillance to foreign embassies and missions in Washington, New York and other cities, and obtained court orders to do so.

Since 2002, the agency has been conducting some warrantless eavesdropping on people in the United States who are linked, even if indirectly, to suspected terrorists through the chain of phone numbers and e-mail addresses, according to several officials who know of the operation. Under the special program, the agency monitors their international communications, the officials said. The agency, for example, can target phone calls from someone in New York to someone in Afghanistan.

Warrants are still required for eavesdropping on entirely domestic-to-domestic communications, those officials say, meaning that calls from that New Yorker to someone in California could not be monitored without first going to the Federal Intelligence Surveillance Court.

A White House Briefing

After the special program started, Congressional leaders from both political parties were brought to Vice President Dick Cheney's office in the White House. The leaders, who included the chairmen and ranking members of the Senate and House intelligence committees, learned of the N.S.A. operation from Mr. Cheney. Lt. Gen. Michael V. Hayden of the Air Force, who was then the agency's director and is now a full general and the principal deputy director of national intelligence, and George J. Tenet, then the director of the C.I.A., officials said.

It is not clear how much the members of Congress were told about the presidential order and the eavesdropping program. Some of them declined to comment about the matter, while others did not return phone calls.

Later briefings were held for members of Congress as they assumed leadership roles on the intelligence committees, officials familiar with the program said. After a 2003 briefing, Senator Rockefeller, the West Virginia Democrat who became vice chairman of the Senate Intelligence Committee that year, wrote a letter to Mr. Cheney expressing concerns about the program, officials knowledgeable about the letter said. It could not be determined if he received a reply. Mr. Rockefeller declined to comment. Aside from the Congressional leaders, only a small group of people, including several cabinet members and officials at the N.S.A., the C.I.A. and the Justice Department, know of the program.

Some officials familiar with it say they consider warrantless eavesdropping inside the United States to be unlawful and possibly unconstitutional, amounting to an improper search. One government official involved in the operation said he privately complained to a Congressional official about his doubts about the program's legality. But nothing came of his inquiry. "People just looked the other way because they didn't want to know what was going on," he said.

A senior government official recalled that he was taken aback when he first learned of the operation. "My first reaction was, 'We're doing what?'"

he said. While he said he eventually felt that adequate safeguards were put in place, he added that questions about the program's legitimacy were understandable.

Some of those who object to the operation argue that is unnecessary. By getting warrants through the foreign intelligence court, the N.S.A. and F.B.I. could eavesdrop on people inside the United States who might be tied to terrorist groups without skirting longstanding rules, they say.

The standard of proof required to obtain a warrant from the Foreign Intelligence Surveillance Court is generally considered lower than that required for a criminal warrant - intelligence officials only have to show probable cause that someone may be "an agent of a foreign power," which includes international terrorist groups - and the secret court has turned down only a small number of requests over the years. In 2004, according to the Justice Department, 1,754 warrants were approved. And the Foreign Intelligence Surveillance Court can grant emergency approval for wiretaps within hours, officials say.

Administration officials counter that they sometimes need to move more urgently, the officials said. Those involved in the program also said that the N.S.A.'s eavesdroppers might need to start monitoring large batches of numbers all at once, and that it would be impractical to seek permission from the Foreign Intelligence Surveillance Court first, according to the officials.

The N.S.A. domestic spying operation has stirred such controversy among some national security officials in part because of the agency's cautious culture and longstanding rules.

Widespread abuses - including eavesdropping on Vietnam War protesters and civil rights activists - by American intelligence agencies became public in the 1970's and led to passage of the Foreign Intelligence Surveillance Act, which imposed strict limits on intelligence gathering on American soil. Among other things, the law required search warrants, approved by the secret F.I.S.A. court, for wiretaps in national security cases. The agency, deeply scarred by the scandals, adopted additional rules that all but ended domestic spying on its part.

After the Sept. 11 attacks, though, the United States intelligence community was criticized for being too risk-averse. The National Security Agency was even cited by the independent 9/11 Commission for adhering to self-imposed rules that were stricter than those set by federal law.

Concerns and Revisions

Several senior government officials say that when the special operation began, there were few controls on it and little formal oversight outside the N.S.A. The agency can choose its eavesdropping targets and does not have to seek approval from Justice Department or other Bush administration officials. Some agency officials wanted nothing to do with the program, apparently fearful of participating in an illegal operation, a former senior Bush administration official said. Before the 2004 election, the official said, some N.S.A. personnel worried that the program might come under scrutiny by Congressional or criminal investigators if Senator John Kerry, the Democratic nominee, was elected president.

In mid-2004, concerns about the program expressed by national security officials, government lawyers and a judge prompted the Bush administration to suspend elements of the program and revamp it.

For the first time, the Justice Department audited the N.S.A. program, several officials said. And to provide more guidance, the Justice Department and the agency expanded and refined a checklist to follow in deciding whether probable cause existed to start monitoring someone's communications, several officials said.

A complaint from Judge Colleen Kollar-Kotelly, the federal judge who oversees the Federal Intelligence Surveillance Court, helped spur the suspension, officials said. The judge questioned whether information obtained under the N.S.A. program was being improperly used as the basis for F.I.S.A. wiretap warrant requests from the Justice Department, according to senior government officials. While not knowing all the details of the exchange, several government lawyers said there appeared to be concerns that the Justice Department, by trying to shield the existence of the N.S.A. program, was in danger of misleading the court about the origins of the information cited to justify the warrants.

One official familiar with the episode said the judge insisted to Justice Department lawyers at one point that any material gathered under the special N.S.A. program not be used in seeking wiretap warrants from her court. Judge Kollar-Kotelly did not return calls for comment.

A related issue arose in a case in which the F.B.I. was monitoring the communications of a terrorist suspect under a F.I.S.A.-approved warrant, even though the National Security Agency was already conducting warrantless eavesdropping.

According to officials, F.B.I. surveillance of Mr. Faris, the Brooklyn Bridge plotter, was dropped for a short time because of technical problems. At the time, senior Justice Department officials worried what would happen if the N.S.A. picked up information that needed to be presented in court. The government would then either have to disclose the N.S.A. program or mislead a criminal court about how it had gotten the information.

Several national security officials say the powers granted the N.S.A. by President Bush go far beyond the expanded counterterrorism powers granted by Congress under the USA Patriot Act, which is up for renewal. The House on Wednesday approved a plan to reauthorize crucial parts of the law. But final passage has been delayed under the threat of a Senate filibuster because of concerns from both parties over possible intrusions on Americans' civil liberties and privacy.

Under the act, law enforcement and intelligence officials are still required to seek a F.I.S.A. warrant every time they want to eavesdrop within the United States. A recent agreement reached by Republican leaders and the Bush administration would modify the standard for F.B.I. wiretap warrants, requiring, for instance, a description of a specific target. Critics say the bar would remain too low to prevent abuses.

Bush administration officials argue that the civil liberties concerns are unfounded, and they say pointedly that the Patriot Act has not freed the

N.S.A. to target Americans. "Nothing could be further from the truth," wrote John Yoo, a former official in the Justice Department's Office of Legal Counsel, and his co-author in a Wall Street Journal opinion article in December 2003. Mr. Yoo worked on a classified legal opinion on the N.S.A.'s domestic eavesdropping program.

At an April hearing on the Patriot Act renewal, Senator Barbara A. Mikulski, Democrat of Maryland, asked Attorney General Alberto R. Gonzales and Robert S. Mueller III, the director of the F.B.I., "Can the National Security Agency, the great electronic snooper, spy on the American people?"

"Generally," Mr. Mueller said, "I would say generally, they are not allowed to spy or to gather information on American citizens."

President Bush did not ask Congress to include provisions for the N.S.A. domestic surveillance program as part of the Patriot Act and has not sought any other laws to authorize the operation. Bush administration lawyers argued that such new laws were unnecessary, because they believed that the Congressional resolution on the campaign against terrorism provided ample authorization, officials said.

The Legal Line Shifts

Seeking Congressional approval was also viewed as politically risky because the proposal would be certain to face intense opposition on civil liberties grounds. The administration also feared that by publicly disclosing the existence of the operation, its usefulness in tracking terrorists would end, officials said.

The legal opinions that support the N.S.A. operation remain classified, but they appear to have followed private discussions among senior administration lawyers and other officials about the need to pursue aggressive strategies that once may have been seen as crossing a legal line, according to senior officials who participated in the discussions.

For example, just days after the Sept. 11, 2001, attacks on New York and the Pentagon, Mr. Yoo, the Justice Department lawyer, wrote an internal memorandum that argued that the government might use "electronic surveillance techniques and equipment that are more powerful and sophisticated than those available to law enforcement agencies in order to intercept telephonic communications and observe the movement of persons but without obtaining warrants for such uses."

Mr. Yoo noted that while such actions could raise constitutional issues, in the face of devastating terrorist attacks "the government may be justified in taking measures which in less troubled conditions could be seen as infringements of individual liberties."

The next year, Justice Department lawyers disclosed their thinking on the issue of warrantless wiretaps in national security cases in a little-noticed brief in an unrelated court case. In that 2002 brief, the government said that "the Constitution vests in the President inherent authority to conduct warrantless intelligence surveillance (electronic or otherwise) of foreign powers or their agents, and Congress cannot by statute extinguish that constitutional authority."

Administration officials were also encouraged by a November 2002 appeals court decision in an unrelated matter. The decision by the Foreign Intelligence Surveillance Court of Review, which sided with the administration in dismantling a bureaucratic "wall" limiting cooperation between prosecutors and intelligence officers, cited "the president's inherent constitutional authority to conduct warrantless foreign intelligence surveillance."

But the same court suggested that national security interests should not be grounds "to jettison the Fourth Amendment requirements" protecting the rights of Americans against undue searches. The dividing line, the court acknowledged, "is a very difficult one to administer."

Barclay Walsh contributed research for this article.

Correction: Dec. 28, 2005, Wednesday:

Because of an editing error, a front-page article on Dec. 16 about a decision by President Bush to authorize the National Security Agency to eavesdrop on Americans and others inside the United States to search for evidence of terrorist activity without warrants ordinarily required for domestic spying misstated the name of the court that would normally issue those warrants. It is the Foreign - not Federal - Intelligence Surveillance Court.

EXHIBIT D

What can we help you find?

Salt Lake City 91° Partly Cloudy | Traffic

Thursday, June 21, 2012 | Last Updated: 07:00 pm

News Sports Blogs Opinion Money Lifestyle Entertainment Obituaries Jobs Homes Cars Classifieds Shopping Subscribe
Utah | Nation + World | Neighborhood | Politics | Justice | Polygamy | LDS Church | Education | Weather | UtahsRight.com | McEntee | Rolly | Online Today



Spies like us: NSA to build huge facility in Utah

Civilian jobs » The facility could offer more than 1,000 high-tech jobs for the state.

Article Tools



E-mail this story

Print Friendly

Photos



BY MATTHEW D. LAPLANTE

THE SALT LAKE TRIBUNE

PUBLISHED JULY 1, 2009 7:13 PM

This is an archived article that was published on sltrib.com in 2009, and information in the article may be outdated. It is provided only for personal research purposes and may not be reprinted.

Hoping to protect its top-secret operations by decentralizing its massive computer hubs, the National Security Agency will build a 1-million-square-foot data center at Utah's Camp Williams.

The years-in-the-making project, which may cost billions over time, got a \$181 million start last week when President Obama signed a war spending bill in which Congress agreed to pay for primary construction, power access and security infrastructure. The enormous building, which will have a footprint about three times the size of the Utah State Capitol building, will be constructed on a 200-acre site near the Utah National Guard facility's runway.

Congressional records show that initial construction -- which may begin this year -- will include tens of millions in electrical work and utility construction, a \$9.3 million vehicle inspection facility, and \$6.8 million in perimeter security fencing. The budget also allots \$6.5 million for the relocation of an existing access road, communications building and training area.

Officials familiar with the project say it may bring as many as 1,200 high-tech jobs to Camp Williams, which borders Salt Lake, Utah and Tooele counties.

It will also require at least 65 megawatts of power -- about the same amount used by every home in Salt Lake City combined. A separate power substation will have to be built at Camp Williams to sustain that demand, said Col. Scott Olson, the Utah National Guard's legislative liaison. He noted that there were two significant power corridors that ran through Camp Williams -- a chief factor in the NSA's desire to build there.

The NSA bills itself as the home of America's codemakers and codebreakers, but the Department of Defense agency is perhaps better known for its signals intelligence program, which is reported to have the capacity to tap into a significant amount of the world's communications. The agency also has been the subject of significant criticism by civil libertarians, who have accused it of unwarranted monitoring of the communications of U.S. citizens.

The NSA's heavily automated computerized operations have for years been based at Fort Meade, Maryland, but the agency began looking to decentralize its efforts following the terrorist attacks of Sept. 11, 2001.

Propelling that desire was the insatiable energy appetite of the agency's computers. In 2006, the Baltimore Sun reported that the NSA -- Baltimore Gas & Electric's biggest customer -- had maxed out the local grid and could not bring online several supercomputers it needed to expand its operations.

About the same time, NSA officials, who have a long-standing relationship with Utah based on the state Guard's unique linguist units, approached state officials about finding land in the state on which to build an additional data center.

UTAH
ARTS
FESTIVAL

HERE.

ROLLOVER
FOR VIDEO

OPENS TODAY! LIBRARY SQUARE

Olson said NSA officials also seemed drawn to Utah's increasing reputation as a center of technical industry and the area's more traditional role as a transportation hub.

"They were looking at secure sites, where there could be a natural nexus between organizations and where space was available," he said. "The stars just kind of came into alignment. We could provide them everything they need."

The agency is building a similar center in San Antonio at the site of a former Sony microchip plant.

Sen. Orrin Hatch, the longest-serving member of the Senate Select Committee on Intelligence, refused to answer questions about the project. Officials from Hatch's office said they were not at liberty to discuss a classified matter, though it is referenced in several public documents and has been spoken about openly by state officials for the past week.

NSA officials also declined to comment immediately on the project, but pledged to answer questions later this week.

Tribune reporter Matt Canham contributed to this story

© Copyright 2012 The Salt Lake Tribune. All rights reserved. This material may not be published, broadcast, rewritten or redistributed.



1500 COUNT
EGYPTIAN COTTON
SHEETS
\$79

Find us on Facebook



The Salt Lake Tribune

Like

11,786 people like The Salt Lake Tribune.



Barbara Rudolfina Annela Matthew Annette

Facebook social plugin

Recent Activity

Sign Up

Create an account or log in to see what your friends are doing.



Sex also awesome | The Salt Lake Tribune
467 people recommend this.

Facebook social plugin

UT H A TS FESTIVAL **HERE.** ROLLOVER FOR VIDEO **OPENS TODAY!** LIBRARY SQUARE

EXHIBIT E



LEGISLATIVE HISTORY
P.L. 95-511

FOREIGN INTELLIGENCE SURVEILLANCE
ACT OF 1978

P.L. 95-511, see page 92 Stat. 1783

Senate Report (Judiciary Committee) No. 95-604 (I and II),
Nov. 15, 22, 1977 [To accompany S. 1566]

Senate Report (Intelligence Committee) No. 95-701,
Mar. 14, 1978 [To accompany S. 1566]

House Report [Intelligence Committee] No. 95-1283,
June 8, 1978 [To accompany H.R. 7308]

House Conference Report No. 95-1720, Oct. 5, 1978
[To accompany S. 1566]

Cong. Record Vol. 124 (1978)

DATES OF CONSIDERATION AND PASSAGE

Senate April 20, October 9, 1978

House September 7, October 12, 1978

The Senate bill was passed in lieu of the House bill. The Senate
Reports (this page, p. 3970, p. 3973) and the House Con-
ference Report (p. 4048) are set out.

SENATE REPORT NO. 95-604—PART 1

[page 1]

The Committee on the Judiciary, to which was referred the bill
(S. 1566) to amend title 18, United States Code, to authorize appli-
cations for a court order approving the use of electronic surveillance
to obtain foreign intelligence information, having considered the same,
reports favorably thereon with amendments and recommends that the
bill, as amended, do pass.

* * * * *

[page 3]

PURPOSE OF AMENDMENTS

The amendments to S. 1566 are designed to clarify and make more
explicit the statutory intent, as well as to provide further safeguards
for individuals subjected to electronic surveillance pursuant to this
new chapter. Certain amendments are also designed to provide a de-
tailed procedure for challenging such surveillance, and any evidence
derived therefrom, during the course of a formal proceeding.

Finally, the reported bill adds an amendment to Chapter 119 of
title 18, United States Code (Title III of the Omnibus Crime Control
and Safe Streets Act of 1968, Public Law 90-351, section 802). This
latter amendment is technical and conforming in nature and is de-
signed to integrate certain provisions of Chapters 119 and 120. A
more detailed explanation of the individual amendments is contained
in the section-by-section analysis of this report.

T
intr
pro
pro
info
Bay
Nels
Cor
S.
veill
also
inch
hear
of t
telli

by a
the
S.
of ti
on (C
the
num
reco
Dire
genc
Bro
Mor
B:
with
S.
resp
ited
comm
omm

Th
supp
testi

LEGISLATIVE HISTORY

P.L. 95-511

or lawful resident alien is the target of an electronic surveillance, the judge is required to review the Executive Branch certification to determine if it is clearly erroneous. No review of the certification was allowed in S. 3197. Finally, S. 1566 spells out that the Executive cannot engage in electronic surveillance within the United States without a prior judicial warrant. This is accomplished by repealing the so-called executive "inherent power" disclaimer clause currently found in section 2511(3) of Title 18, United States Code. S. 1566 provides instead that its statutory procedures (and those found in chapter 119 of title 18) "shall be the exclusive means" for conducting electronic surveillance, as defined in the legislation, in the United States. The highly controversial disclaimer has often been cited as evidence of a congressional ratification of the President's inherent constitutional power to engage in electronic surveillance in order to obtain foreign intelligence information essential to the national security. Despite the admonition of the Supreme Court that the language of the disclaimer was "neutral" and did not reflect any such congressional recognition of inherent power, the section has been a major source of controversy. By repeal-

[page 7]

ing section 2511(3) and expressly stating that the statutory warrant procedures spelled out in the law must be followed in conducting electronic surveillance in the United States, this legislation ends the eight-year debate over the meaning and scope of the inherent power disclaimer clause.

II. STATEMENT OF NEED

The Federal Government has never enacted legislation to regulate the use of electronic surveillance within the United States for foreign intelligence purposes. Although efforts have been made in recent years by Senator Kennedy, Senator Nelson, Senator Mathias, and former Senator Philip A. Hart to circumscribe the power of the executive branch to engage in such surveillance, and the Senate came very close to enacting such legislation during the 94th Congress, the fact remains that such efforts have never been successful.² The hearings held this year on S. 1566 were the sixth set of hearings on warrantless wiretapping in as many years.³ The Committee believes that S. 1566 is a measure which can successfully break this impasse and provide effective, reasonable safeguards to ensure accountability and prevent improper surveillance. S. 1566 goes a long way in striking a fair and just balance between protection of national security and protection of personal liberties. It is a recognition by both the Executive Branch and the Congress that the statutory rule of law must prevail in the area of foreign intelligence surveillance.

The need for such statutory safeguards has become apparent in recent years. This legislation is in large measure a response to the revelations that warrantless electronic surveillance in the name of national security has been seriously abused. These abuses were initially illuminated in 1973 during the investigation of the Watergate break-in. Since that time, however, the Senate Select Committee to Study Government Operations with Respect to Intelligence Activities, chaired by Senator Church (hereafter referred to as the Church Committee); has concluded that every President since Franklin D. Roosevelt asserted the authority to authorize warrantless electronic surveillance and exercised that authority. While the number of illegal or improper

R
t
V
-
S
S
S
C
P
S
A
T
B
R
S
tr
W
th
gr
wi

cc
D:

wh
tio
per
tial
inf
acti
exe
und

FOREIGN INTELLIGENCE

P.L. 95-511

national security taps and bugs conducted during the Nixon administration may have exceeded those in previous administrations, the surveillances were regrettably by no means atypical. In summarizing its

² See, e.g., S. 3197, *Foreign Intelligence Surveillance Act of 1976*, 94th Cong., 2d sess. (1976); S. 743, *National Security Surveillance Act of 1975*, 94th Cong., 1st sess. (1975); S. 2820, *Surveillance Practices and Procedures Act of 1973*, 93rd Cong., 1st sess. (1973); S. 4062, *Freedom from Surveillance Act of 1974*, 93rd Cong., 2d sess. (1974).

³ See, e.g., Hearings before the Subcommittee on Criminal Laws and Procedures of the Senate Committee on the Judiciary, *Foreign Intelligence Surveillance Act of 1976*, 94th Cong., 2d sess. (1976); Senate Select Committee on Intelligence, *Foreign Intelligence Surveillance Act of 1976*, 94th Cong., 2d sess. (1976); Subcommittee on Surveillance of the Senate Committee on Foreign Relations and the Subcommittee on Administrative Practice and Procedure of the Senate Committee on the Judiciary, *Warrantless Wiretapping and Electronic Surveillance*, 94th Cong., 1st sess. (1975); Joint Hearings before the Subcommittee on Administrative Practice and Procedure and the Subcommittee on Constitutional Rights of the Senate Committee on the Judiciary, *Warrantless Wiretapping and Electronic Surveillance*, 93d Cong., 2d sess. (1974); Hearings before the Subcommittee on Administrative Practice and Procedure of the Senate Committee on the Judiciary, *Warrantless Wiretapping*, 92d Cong., 2d sess. (1972). In the joint report of the Subcommittees on Surveillance and Administrative Practice and Procedure issued in 1975, findings were made that "there are not adequate written standards or criteria within the executive branch to govern the warrantless electronic surveillance of either Americans or foreigners. There is a gap in the statutes, the case, and in administrative regulation on the use of warrantless wiretaps or bugs by executive branch agencies for alleged 'national security' purposes."

[page 8]

conclusion that surveillance was "often conducted by illegal or improper means," the Church committee wrote:

Since the 1930's, intelligence agencies have frequently wire-tapped and bugged American citizens without the benefit of judicial warrant. . . . [P]ast subjects of these surveillances have included a United States Congressman, Congressional staff member, journalists and newsmen, and numerous individuals and groups who engaged in no criminal activity and who posed no genuine threat to the national security, such as two White House domestic affairs advisers and an anti-Vietnam War protest group. (vol. 2, p. 12)

* * * * *

The application of vague and elastic standards for wire-tapping and bugging has resulted in electronic surveillances which, by any objective measure, were improper and seriously infringed the Fourth Amendment Rights of both the targets and those with whom the targets communicated. The inherently intrusive nature of electronic surveillance, moreover, has enabled the Government to generate vast amounts of information—unrelated to any legitimate government interest—about the personal and political lives of American citizens. The collection of this type of information has, in turn, raised the danger of its use for partisan political and other improper ends by senior administration officials. (vol. 3, p. 32.)

Also formidable—although incalculable—is the "chilling effect" which warrantless electronic surveillance may have on the constitutional rights of those who were not targets of the surveillance, but who perceived themselves, whether reasonably or unreasonably, as potential targets. Our Bill of Rights is concerned not only with direct infringements on constitutional rights, but also with government activities which effectively inhibit the exercise of these rights. The exercise of political freedom depends in large measure on citizens' understanding that they will be able to be publicly active and dissent



LEGISLATIVE HISTORY

P.L. 95-511

from official policy, within lawful limits, without having to sacrifice the expectation of privacy that they rightfully hold. Arbitrary or uncontrolled use of warrantless electronic surveillance can violate that understanding and impair that public confidence so necessary to an uninhibited political life.

S. 1566 is designed, therefore, to curb the practice by which the Executive Branch may conduct warrantless electronic surveillance on its own unilateral determination that national security justifies it. At the same time, however, this legislation does not prohibit the legitimate use of electronic surveillance to obtain foreign intelligence information. As the Church committee pointed out:

Electronic surveillance techniques have understandably enabled these agencies to obtain valuable information relevant to their legitimate intelligence missions. Use of these techniques has provided the Government with vital intelligence, which would be difficult to acquire through other means, about the activities and intentions of foreign powers and has

[page 9]

provided important leads in counterespionage cases. (vol. 2, p. 274)

Safeguarding national security against the intelligence activities of foreign agents remains a vitally important Government purpose. Few would dispute the fact that we live in a dangerous world in which hostile intelligence activities in this country are still carried on to our detriment.

Striking a sound balance between the need for such surveillance and the protection of civil liberties lies at the heart of S. 1566. As Senator Kennedy stated in introducing S. 1566:

The complexity of the problem must not be underestimated. Electronic surveillance can be a useful tool for the Government's gathering of certain kinds of information; yet, if abused, it can also constitute a particularly indiscriminate and penetrating invasion of the privacy of our citizens. My objective over the past six years has been to reach some kind of fair balance that will protect the security of the United States without infringing on our citizens' human liberties and rights.

The committee believes that the Executive Branch of Government should have, under proper circumstances and with appropriate safeguards, authority to acquire important foreign intelligence information by means of electronic surveillance. The committee also believes that the past record and the state of the law in the area make it desirable that the Executive Branch not be the sole or final arbiter of when such proper circumstances exist. S. 1566 is designed to permit the Government to gather necessary foreign intelligence information by means of electronic surveillance but under limitations and according to procedural guidelines which will better safeguard the rights of individuals.

III. BACKGROUND

The bipartisan congressional support for S. 1566 and the constructive cooperation of the Executive Branch toward the legislation signifies a constructive change in the ongoing debate over electronic sur-

v
to
co
su
de
to
fo
Pr
ar
of
fo

be
ch

wi
—

T
te
sy
su
an
wi
gu
an
fo

Co
ini
mu
to
tio
we
int
as
oni
era
De
tar
]
Ge
unc
nat
Att
at]
sub
incl
limi
ther
T
Attc
form

EXHIBIT F

Calendar No. 977

94TH CONGRESS }
2d Session }

SENATE

REPORT
No. 94-1035

FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1976

JULY 15, 1976.—Ordered to be printed
Filed under authority of the order of the Senate of July 1, 1976

Mr. KENNEDY, from the Committee on the Judiciary,
submitted the following

REPORT

together with

ADDITIONAL AND MINORITY VIEWS

[To accompany S. 3197]

The Committee on the Judiciary, to which was referred the bill (S. 3197) to amend title 18, United States Code, to authorize applications for a court order approving the use of electronic surveillance to obtain foreign intelligence information, having considered the same, reports favorably thereon with amendments and recommends that the bill, as amended, do pass.

AMENDMENTS

On page 2, line 16, strike out "assists" and insert after the second "or", the word "knowingly".

On page 2, line 16, strike out "and" and insert in lieu thereof "or".

On page 2, line 20, insert the word "surveillance", after the word "other".

On page 3, line 2, insert the word "surveillance" after the word "other".

On page 3, line 3, strike out "transmission", and insert in lieu thereof "communication".

On page 3, lines 4 and 5, strike out "with a reasonable expectation of privacy", and insert in lieu thereof "under circumstances where a person has a constitutionally protected right of privacy and".

On page 3, line 5, strike out "point of origin", and insert in lieu thereof "sender".

Jer-
anner

At the same time, however, this legislation does not prohibit the use of electronic surveillance to obtain foreign intelligence information. As the Church committee pointed out:

Electronic surveillance techniques have understandably enabled these agencies to obtain valuable information relevant to their legitimate intelligence missions. Use of these techniques has provided the Government with vital intelligence, which would be difficult to acquire through other means, about the activities and intentions of foreign powers and has provided important leads in counter espionage cases. (vol. 2, p. 274.)

Safeguarding national security against the intelligence activities of foreign agents remains a vitally important Government purpose. Few would dispute the fact that we live in a dangerous world in which hostile intelligence activities in this country are still carried on to our detriment.

Striking this balance between the need for such surveillance and the protection of civil liberties lies at the heart of S. 3197. As Senator Kennedy stated in introducing the legislation:

The complexity of the problem must not be underestimated. Electronic surveillance can be a useful tool for the Government's gathering of certain kinds of information; yet, if abused, it can also constitute a particularly indiscriminate and penetrating invasion of the privacy of our citizens. Our objective has been to reach some kind of balance that will protect the security of the United States without infringing on our citizens' human liberties and rights.*

The committee believes that the executive branch of Government should have, under proper circumstances, authority to acquire important foreign intelligence information by means of electronic surveillance. The committee also believes that the past record establishes clearly that the executive branch cannot be the sole or final arbiter of when such proper circumstances exist. S. 3197 is designed to permit the Government to gather foreign intelligence information by means of electronic surveillance but under substantive limitations and according to procedural guidelines which will better safeguard the rights of individuals and prevent the reoccurrence of abuses which have occurred.

III. BACKGROUND

Bipartisan congressional support for S. 3197 and the constructive cooperation of the executive branch toward the legislation cannot mask the fact that substantial differences continue to exist among members of the Congress and the executive branch concerning the constitutionality of warrantless wiretapping. This is not surprising since the United States Supreme Court has never expressly decided the issue of whether the President has constitutional authority to authorize warrantless electronic surveillance in cases concerning the national security. Whether or not the President has a so-called "inherent power" to engage in or authorize warrantless electronic sur-

* 122 Cong. Rec. S4025 (daily ed., Mar. 23, 1976).

Study Governmental Operations with Respect to Intelligence Activities, chaired by Senator Church (hereafter referred to as the Church committee), has concluded that every President since Franklin D. Roosevelt asserted the authority to authorize warrantless electronic surveillance and exercised that authority. While the number of illegal or improper national security taps and bugs conducted during the Nixon administration may have exceeded those in previous administrations, the surveillances were regrettably by no means atypical. In summarizing its conclusion that surveillance investigation was "often conducted by illegal or improper means," the Church committee wrote:

Since the 1980's, intelligence agencies have frequently wiretapped and bugged American citizens without the benefit of judicial warrant. . . . [P]ast subjects of these surveillances have included a United States Congressman, a Congressional staff member, journalists and newsmen, and numerous individuals and groups who engaged in no criminal activity and who posed no genuine threat to the national security, such as two White House domestic affairs advisers and an anti-Vietnam War protest group. (vol. 2, p. 12.)

* * * * * The application of vague and elastic standards for wiretapping and bugging has resulted in electronic surveillances which, by any objective measure, were improper and seriously infringed the Fourth Amendment Rights of both the targets and those with whom the targets communicated. The inherently intrusive nature of electronic surveillance, moreover, has enabled the Government to generate vast amounts of information—unrelated to any legitimate government interest—about the personal and political lives of American citizens. The collection of this type of information has, in turn, raised the danger of its use for partisan political and other improper ends by senior administration officials. (vol. 3, p. 32.)

Also formidable—although incalculable—is the "chilling effect" which warrantless electronic surveillance may have on the constitutional rights of those who were not targets of the surveillance, but who perceived themselves, whether reasonably or unreasonably, as potential targets. Our Bill of Rights prevents not only direct infringements on constitutional rights; it also prevents government activities which effectively chill the exercise of these rights. The exercise of political freedom depends in large measure on citizens' understanding that they will be able to be publicly active and dissent from official policy, within lawful limits, without having to sacrifice the expectation of privacy that they rightfully hold. Arbitrary or uncontrolled use of warrantless electronic surveillance can violate that understanding and impair that public confidence so necessary to an uninhibited political life.

S. 3197 is designed, therefore, to curb the practice by which the executive branch may conduct warrantless electronic surveillance on its own unilateral determination that national security justifies it.

S. 3197 is based on the premise (supported by history) that executive self-restraint, in the area of national security electronic surveillance, is neither feasible nor wise. The determination of when "national security" is in jeopardy is necessarily subjective. This determination can lead to electronic surveillance of those perceived as a threat when, in fact, no such threat exists. S. 3197 is designed to provide both external and internal checks on such subjective determinations.

But establishing statutory limits in the area of foreign intelligence electronic surveillance has proven a difficult task. Perhaps the most difficult issue posed during committee deliberations was whether such surveillance should be limited to situations involving the commission of a crime.

The committee has made a limited exception in this bill for electronic surveillance when an American acting under the control of a foreign power engages in certain clandestine intelligence gathering which is not presently a violation of federal criminal statutes.

Although there are precedents for departing from a strict criminal standard in the issuance of search warrants deemed compatible with the fourth amendment, see e.g., *Camara v. Municipal Court*, 387 U.S. 523 (1967); *Ameida-Sanchez v. United States*, 413 U.S. 266 (1973); cf. *United States v. Martinez-Fuerte*, ___ U.S. ___ (1976) (No. 74-1560, decided July 6, 1976) (no warrant required), those decisions did not involve national security intelligence, with its recognized potential for abuse. It should also be noted, however, that in the *Keith* case, *supra*, the Supreme Court noted that the reasons for domestic security surveillance may differ from those justifying surveillance for ordinary crimes and that, accordingly, "Different standards may be compatible with the fourth amendment if they are reasonable both in relation to the legitimate needs of Government for intelligence information and the protected rights of our citizens. For the warrant application may vary according to the governmental interest to be enforced and the nature of citizens rights deserving protection." (407 U.S. at 322.) (See also, *Zweibon v. Mitchell, supra*, at 669.) As indicated in the section-by-section analysis, this departure from the general principle that such surveillance must be linked to criminal activity is intended to be a narrow, circumscribed one, reflecting the deep concern of the committee. This bill authorizes electronic surveillance in a limited number of noncriminal situations only under the twin safeguards of an independent review by a neutral judge and his application of the "probable cause standard."

It is important to note that the committee's favorable recommendation of this legislation in no way reflects any judgment that it would also be appropriate to depart from the standard of criminal activity as the basis for using other intrusive investigative techniques. The bill does not impliedly authorize departure from the standard of criminality in other aspects of national security investigations or intelligence collection directed at Americans without the safeguards of judicial review and probable cause. It remains to determine, in fashioning a charter for the use of informants, physical surveillance and other investigative procedures, whether the departure from a criminal standard is an acceptable basis for investigating Americans on grounds of national security.

SECTION-BY-SECTION ANALYSIS

Section 1 of the bill provides that the Act may be cited as the "Foreign Intelligence Surveillance Act of 1976".

Section 2 of the bill amends the Omnibus Crime Control and Safe Streets Act of 1968 (Pub. L. 90-351, Title III, section 802) by adding a new chapter 120 and items 2521-2528:

Section 2521

Subsection (a) provides that except for those terms specifically defined in this section the definitions of Chapter 119, relating to the interception of wire and oral communications, apply to this chapter as well.

Subsection (b) (1) defines an "agent of a foreign power" in two separate ways. Subparagraph (i) includes officers and employees of foreign powers who are not United States citizens or aliens lawfully admitted for permanent residence. The definition is framed in this way because it is presumed that nonresident aliens who are indeed officers or employees of a foreign power are likely sources of foreign intelligence information. Given a foreign officer or employee's tenuous relationship with the United States and their close relationship with a foreign power, this standard is considered by the committee to be reasonable in light of the Government's legitimate need for foreign intelligence information and the nature of the interests upon which the search would intrude. Employees of a foreign power are meant to include those persons who have a normal employee-employer relationship.²⁰

Subparagraph (ii) offers a second definition of "agent of a foreign power," which encompasses two different types of persons. The first is a person who, pursuant to the direction of a foreign power, is engaged in clandestine intelligence activities, sabotage, or terrorist activities. The second is a person who conspires with or knowingly aids or abets another person who is acting pursuant to the direction of a foreign power and is engaged in such activities.

It should be noted at the outset that the definition of "agent of a foreign power" would only include American citizens and aliens lawfully admitted for permanent residence who are engaged in clandestine intelligence activities, sabotage, or terrorist activities pursuant to the direction of a foreign power or who consciously conspire with or knowingly aid or abet persons who engage in these activities.

Thus the two constituent elements of the definition of such an agent are his relationship with a foreign power or an agent of a foreign power and, secondly, the nature of the activities in which he engages.

A. "PURSUANT TO THE DIRECTION OF A FOREIGN POWER"

"Pursuant to the direction" of a foreign power means that a person must be acting under the direction and control of such power. There

²⁰ This bill is not intended, of course, to repeal or abrogate the Vienna Convention on Diplomatic Relations, which was ratified by the Senate and came into effect in the United States on December 13, 1972. This Convention provides that diplomatic agents, their residences (Article 30(1)), and their missions (Article 22(1) and (3)), as well as their official correspondence (Article 27(2) and 30(2)), are "inviolable." The obligations of the Convention are reciprocal; when another nation has failed to maintain the inviolability of American diplomatic communications, this country is free under international law to act similarly towards representatives of that nation (Article 47(2a)).

EXHIBIT G

LEGISLATIVE HISTORY
P.L. 95-511

question of how many "cutouts" are enough to exempt an American acting on behalf of or in conjunction with a Communist regime from lawful electronic surveillance? Most Americans would probably agree that in such cases it would be better to err on the side of caution and tell the intelligence agencies to survey anyone working with such regimes. The bill ought to reflect this.

Finally, the very complexity of the standards must be judged a drawback. Even if they provided the Nation sufficient protection in peacetime, they would surely be too cumbersome to do so in time of war. In time of war, then, a new bill would have to be hastily enacted to provide for emergency powers. But emergency legislation is generally bad legislation. While we have the time we ought to enact a bill workable in bad times as well as in good times.

MALCOLM WALLOP.

HOUSE CONFERENCE REPORT NO. 95-1720

* * * * *

[page 19]

JOINT EXPLANATORY STATEMENT OF THE COMMITTEE OF CONFERENCE

The managers on the part of the House and the Senate at the conference on the disagreeing votes of the two Houses on the amendments of the House to the bill (S. 1566) to amend title 18, United States Code, to authorize applications for a court order approving the use of electronic surveillance to obtain foreign intelligence information, submit the explanation of the effect of the action agreed upon by the managers and recommended in the accompanying conference report.

The managers recommend that the Senate agree to the amendments of the House, with an amendment. That amendment will be referred to here as the "conference substitute." Except for certain clarifying, clerical, conforming, and other technical changes, there follows an issue by issue summary of the Senate bill, the House amendments, and the conference substitute.

TITLE

The Senate bill amended Title 18 (Crimes and Criminal Procedures) of the United States Code, to authorize applications for a court order approving the use of electronic surveillance to obtain foreign intelligence information.

The House amendments provided for an uncodified title, to authorize electronic surveillance to obtain foreign intelligence information.

The conference substitute adopts the House provision. The conferees agree that this change is not intended to affect in any way the jurisdiction of Congressional Committees with respect to electronic surveillance for foreign intelligence purposes. Rather, the purpose of the change is solely to allow the placement of Title I of the Foreign Intelligence Surveillance Act in that portion of the United States Code (Title 50) which most directly relates to its subject matter.

DEFINITION OF "FOREIGN POWER"

The Senate bill defined "foreign power", with respect to terrorist groups, to mean a foreign-based terrorist group.

T
eng
T
fere
essa
arat

T
pers

Uni
pers
clan
Stat
bill
who
rori
with
acti
T
resp
in t
pow
pow
Uni
spec
defi
kno
inte
sons
acti
T
defi
men
acti
pow
act
The
will
Stat
inst
sho
of a
tion
on
iden
indi
furt
ratic
ratic
acts
train
natic

LEGISLATIVE HISTORY

P.L. 95-511

[page 31]

NOTICE OF USE OF INFORMATION IN LEGAL PROCEEDINGS

The Senate bill provided for notification to the court when information derived from electronic surveillance is to be used in legal proceedings.

The House amendments contained a comparable provision and also a provision, not contained in the Senate bill, requiring notice to the aggrieved person. The House amendments also contained a separate section relating to use by State or local authorities requiring notice to the Attorney General.

The conference substitute adopts the House provisions. The conferees agree that notice should be given to the aggrieved person as soon as possible, so as to allow for the disposition of any motions concerning evidence derived from electronic surveillance. The conferees also agree that the Attorney General should at all times be able to assess whether and to what extent the use of information made available by the Government to a State or local authority will be used.

SUPPRESSION MOTIONS

The Senate bill provided for motions to suppress the contents of any communication acquired by electronic surveillance, or evidence derived therefrom.

The House amendments provided for motions to suppress the evidence obtained or derived from electronic surveillance.

The conference substitute adopts the House provision. The conferees agree that the broader term "evidence" should be used because it includes both the contents of communications and other information obtained or derived from electronic surveillance.

IN CAMERA PROCEDURE FOR DETERMINING LEGALITY

The Senate bill provided a single procedure for determining the legality of electronic surveillance in a subsequent in camera and ex parte proceeding, if the Government by affidavit asserts that disclosure or an adversary hearing would harm the national security of the United States. The Senate bill also provided that, in making this determination, the court should disclose to the aggrieved person materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance.

The House amendments provided two separate procedures for determining the legality of electronic surveillance, if the Attorney General files an affidavit under oath that disclosure would harm the national security of the United States or compromise foreign intelligence sources and methods. In criminal cases, there would be an in camera proceeding; and the court might disclose to the aggrieved person, under appropriate security procedures and protective orders, materials relating to the surveillance if there were a reasonable question as to the legality of the surveillance and if disclosure would likely promote a more accurate determination of such legality, or if disclosure would not harm the national security. In civil suits, there would be an in camera and ex parte proceeding before a court of appeals; and the court would disclose, under appropriate security procedures and protective orders, to the aggrieved person or his attorney materials relat-

ing to
aggri
regar
The
with
and e
affida
be fir
Gover
The
the pr
the in
The c
view o
is nec
sider
ment
that t
sary
The
appro
in bo
stand
of the
and p
intere

The
acquir
pectat
ment
or seri
The
except
bodily
The
the wo
dicatic

The
torney
commit
the act.
The
deemed
commit
they ma
The
intellig
version.
Sectio
Commit

FOREIGN INTELLIGENCE

P.L. 95-511

[page 32]

ing to the surveillance only if necessary to afford due process to the aggrieved person. The House amendments also provided that orders regarding legality or disclosure would be final and binding.

The conference substitute essentially adopts the Senate provisions, with technical changes and the following modifications. The in camera and ex parte proceeding is invoked if the Attorney General files an affidavit under oath. All orders regarding legality and disclosure shall be final and binding only where the rulings are against the Government.

The conference substitute adds the words "requiring review or" to the provision making orders final and binding. This change clarifies the intent of the House provision in conformity with section 102(a). The conferees intend that a determination by a district court that review of a certification by the Attorney General under section 102(a) is necessary to determine the legality of the surveillance shall be considered a final and binding order and thus appealable by the Government before the court reviews the certification. The court may order that the certification be unsealed for review if such review is necessary to determine the legality of the surveillance.

The conferees agree that an in camera and ex parte proceeding is appropriate for determining the lawfulness of electronic surveillance in both criminal and civil cases. The conferees also agree that the standard for disclosure in the Senate bill adequately protects the rights of the aggrieved person, and that the provision for security measures and protective orders ensures adequate protection of national security interests.

UNINTENTIONAL RADIO ACQUISITION

The Senate bill prohibited any use of the contents of unintentionally acquired domestic radio communications, if there is a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, except where the contents indicate a threat of death or serious bodily harm to any person.

The House amendments contained a comparable provision, with an exception if the contents may indicate a threat of death or serious bodily harm to any person.

The conference substitute adopts the Senate provision which omits the word "may." The conferees agree that an exception for any indication of such a threat is sufficient.

CONGRESSIONAL OVERSIGHT

The Senate bill and the House amendments both require the Attorney General, on a semiannual basis, to fully inform the intelligence committees of each House concerning all electronic surveillance under the act.

The Senate bill also stated that "nothing in this chapter shall be deemed to limit the authority and responsibility of the appropriate committees of each House of Congress to obtain such information as they may need to carry out their respective functions and duties."

The House amendments limited this reservation to the respective intelligence committees. The conference substitute adopts the Senate version.

Section 2528(b) of the Senate bill required the Senate Intelligence Committee to report annually to the Senate on the implementation of

men in-
n legal

and also
e to the
separate
notice to

The con-
n as soon
concern-
rees also
to assess
ilable by

ts of any
e derived

s the evi-
conferees
ause it in-
nation ob-

mining the
era and ex
t disclosure
city of the
g this deter-
n materials
necessary to
eillance.
es for deter-
ney General
the national
intelligence
in in camera
person, under
aterials relat-
ion as to the
ly promote a
losure would
uld be an in-
eals; and the
ures and pro-
aterials relat-

EXHIBIT H

95TH CONGRESS } HOUSE OF REPRESENTATIVES { REPORT 95-
 2d Session } { 1283, Pt. I

FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978

JUNE 8, 1978.—Ordered to be printed

Mr. BOLAND, from the Permanent Select Committee on Intelligence,
 submitted the following

REPORT

together with

SUPPLEMENTAL, ADDITIONAL, AND DISSENTING VIEWS

[To accompany H.R. 7308 which on November 4, 1977, was referred jointly to the
 Committee on the Judiciary and the Permanent Select Committee on Intelli-
 gence]

The Permanent Select Committee on Intelligence, to whom was
 referred the bill (H.R. 7308) to amend title 18, United States Code, to
 authorize applications for a court order approving the use of elec-
 tronic surveillance to obtain foreign intelligence information, having
 considered the same, report favorably thereon with amendments and
 recommend that the bill as amended do pass.

AMENDMENTS

Strike all after the enacting clause and insert in lieu thereof:

That this act may be cited as the "Foreign Intelligence Surveillance Act of
 1978".

TABLE OF CONTENTS

TITLE I—ELECTRONIC SURVEILLANCE WITHIN THE UNITED STATES FOR FOREIGN INTELLIGENCE PURPOSES	
Sec. 101.	Definitions.
Sec. 102.	Authorization for electronic surveillance for foreign intelligence purposes.
Sec. 103.	Special courts.
Sec. 104.	Application for an order.
Sec. 105.	Issuance of an order.
Sec. 106.	Use of information.
Sec. 107.	Report of electronic surveillance.
Sec. 108.	Congressional oversight.
Sec. 109.	Penalties.
Sec. 110.	Civil liability.
TITLE II—CONFORMING AMENDMENTS	
Sec. 201.	Amendments to chapter 119 of title 18, United States Code.
TITLE III—EFFECTIVE DATE	
Sec. 301.	Effective date.

person. The effect of this is to require a tap on the wire, an induction coil or like device to acquire the communication from the wire furnished by the common carrier for the activity to be electronic surveillance under section 101(f)(2). Interception of microwave communications carried by common carriers, by intercepting the radio signal, is electronic surveillance under section 101(f)(3), not section 101(f)(2), involving acquisition of a radio communication, not a wire communication. A radio signal is not within the term, a "like connection," in this definition.

(m) *Person*

Section 101(m) defines "person" in the broadest sense possible. It is intended to make explicit that entities can be persons, where the term "person" is used. For example, while it is expected that most entities would be targeted under the "foreign power" standard (which cannot be applied to individuals), it is possible that entities could be targeted under certain of the "agent of a foreign power" standards, see section 101(b)(2)(A)-(D). Where it is intended that only natural persons are referred to, the term "individual" U.S. person or "individual" person is used.

(n) *Contents*

Section 101(n) defines the term "contents", when used with respect to any communication, in broad terms. Specifically, it includes any information concerning the identities of the parties or the existence, substance, purport, or meaning of a communication. This broad phrasing is meant to assure that the scope of the bill is sufficient to protect legitimate privacy interests. Inasmuch as three of the four subdivisions of electronic surveillance, which in fact define the coverage of the bill, turn on the acquisition of "contents" it is necessary to assure that devices such as pen registers are included.

In a recent decision,³² the Supreme Court suggested that a pen register did not acquire "contents" of a "wire communication" as those terms are defined in chapter 119 of title 18, United States Code.³³ It is the intent of this committee that pen registers do acquire "contents" of "wire communications" as those terms are defined in this bill. The term "contents" specifically mentions the identity of parties and "identity" includes a person's phone number, which can as effectively identify him as the mention of his name. Moreover, the definition of "contents" includes information concerning the "existence" of a communication. When a person dials another person's telephone number, whether or not the other person answers the phone, this is a communication under this bill. This is especially true in the intelligence field where signals to a spy may be conveyed merely by having the phone ring a designated number of times. The fact that the target of the pen registers has attempted to communicate with another person at a particular phone is information concerning the "existence" of the communication.

Of course, acquiring knowledge of the "existence" of communications in general, as opposed to acquiring knowledge of the "existence" of a particular communication or communications is not within the

³² *United States v. N.Y. Telephone Co.*, ___ U.S. ___ (1977).

³³ This aspect of the decision seems gratuitous because the Court noted that pen registers do not result in the "aural acquisition" of anything, which would be required, to bring them under chapter 119.

in West Berlin) are not under the territorial sovereignty of the United States.

In the bill terms such as "foreign-based" and "foreign territory" refer to places outside the "United States," as defined here.

(k) *Aggrieved person*

Section 101(k) defines the term "aggrieved person" as a person who has been the target of an electronic surveillance or any other person who, although not a target, has been incidentally subjected to electronic surveillance. As defined, the term is intended to be coextensive, but no broader than, those persons who have standing to raise claims under the Fourth Amendment with respect to electronic surveillance. See *Alderman v. United States*, 394 U.S. 316 (1968).

The term specifically does not include persons, not parties to a communication, who may be mentioned or talked about by others. The Supreme Court has specifically held in *Alderman* that such persons have no fourth amendment privacy right in communications about them which the Government may intercept. While under this bill minimization procedures require minimization of communications about U.S. persons, even though they are not parties to the communication, there is no intent to create a statutory right in such persons which they may enforce. Suppression of relevant criminal evidence and civil suit are particularly inappropriate tools to insure compliance with this part of minimization. Review by judges pursuant to section 105(d), Executive oversight and congressional oversight by the Senate and House Intelligence Committees are intended to be the exclusive means by which compliance with minimization procedures governing minimization of "mentions of" U.S. persons is to be monitored under this or any other law.

(l) *Wire communication*

Section 101(l) defines "wire communication" to mean any communication (whether oral, verbal, or otherwise) while it is being carried by a wire, cable, or other like connection furnished or operated by a communications common carrier. This definition of wire communication differs from the definition of the same term in chapter 119 of title 18, United States Code. There the term is defined to include any communication carried in whole or in part by a wire furnished by a common carrier. This has led to anomalous results such as where a woman listening to an ordinary FM radio has intercepted radio-telephone communications and thereby technically violated chapter 119. See *United States v. Hall*, 488 F. 2d 193 (9th Cir. 1973). Also, ordinary marine band communications, which do not have a reasonable expectation of privacy or require a warrant for law enforcement interception, can be "patched into" telephone systems, becoming a "wire communication" under chapter 119.

The definition here makes clear that communications are "wire communications" under the bill only while they are carried by a wire furnished or operated by a common carrier. The term "common carrier" means a U.S. common carrier and not a common carrier in a foreign country. Moreover, the word "furnished" means furnished in the ordinary course of the common carrier's provision of communications facilities. It does not refer to equipment sold outright to a

EXHIBIT I

FOREIGN INTELLIGENCE
P.L. 95-511

guise that he is an agent of a refugee terrorist leader and then to target these recruited persons against the FBI, the Dade County Police, and the CIA, the ultimate goal being to infiltrate these agencies. F is to keep the intelligence officer informed as to his progress in this regard but his reports are to be made by mail, because the U.S. Government cannot open the mail unless a crime is being committed.

Comment.—As in case No. 4, no tap would be permitted under S. 1566. This is not the kind of information contemplated under the act. A tap would not be permitted under section 794 of title 18 as well. If F is to report in "by mail" is F going to do his recruitment by telephone? Does the Government plan to read S. 1566 to permit the refugee organizations to be wiretapped to find out if they are infiltrated? These are dangerous readings of S. 1566. The proper action is to allow the FBI, having this much information, to foil F's scheme.

In sum, the Justice Department is "reaching" for the exceptional case to establish the need for a deviation from the criminal standard. Contrary to all experience with judicial warrants in the wiretapping area, the Department presumes "strict construction" by judges will hamper legitimate intelligence. The Justice Department should be reminded that only seven judges, picked by the Chief Justice of the U.S. Supreme Court, will review these warrant requests. Of course, this does not give the Justice Department any certainty that all applications will be approved. But the criminal standard does not appreciably make the process more risky for the Government. On the other hand, the noncriminal standard is a dangerous precedent for abuse.

SENATE REPORT NO. 95-701

[page 1]

The Select Committee on Intelligence, to which was referred the bill (S. 1566) to amend title 18, United States Code, to authorize applications for a court order approving the use of electronic surveillance to obtain foreign intelligence information, having considered the same, reports favorably thereon with amendments and recommends that the bill, as amended, do pass.

* * * * *

[page 5]

PURPOSE OF AMENDMENTS

The Committee on the Judiciary adopted several amendments to S. 1566 designed to clarify and make more explicit the statutory intent, to provide further safeguards for individuals subjected to electronic surveillance pursuant to this new chapter, and to provide a detailed procedure for challenging such surveillance, and any evidence derived therefrom, during the course of a formal proceeding.

which
n, but
when
ments

f "na-
laws.
hat is
urt's
com-
vered
) (B)
iracy

rant,
ighly
) has
rass-
to a
The
d in
le to

794
for-
18.
kind
art-
ards
tap
ped
be
with

t to
ious
the
s in

s do
Na-
ould
ary.
lary

ited
has
His
the



LEGISLATIVE HISTORY

P.L. 95-511

[page 63]

sequent trial testimony, a Government witness provides evidence that the electronic surveillance may have been authorized or conducted in violation of the court order. The most common circumstance in which such a motion might be appropriate would be a situation in which a defendant queries the Government under 18 U.S.C. 3504 and discovers that he has been intercepted by electronic surveillance even before the Government has decided whether evidence derived from that surveillance will be used in the presentation of its case. In this instance, under the appropriate factual circumstances, the defendant might move to suppress such evidence under this subsection even without having seen any of the underlying documentation.

A motion under this subsection shall be made before the trial, hearing, or proceeding unless there was no opportunity to make such motion or the movant was not aware of the grounds for the motion. The only change in subsection (d) from S. 3197 is to remove as a separate, independent basis for suppression the fact that the order was insufficient on its face. This is not a substantive change, however, since communications acquired pursuant to an order insufficient on its face would be unlawfully acquired and therefore subject to suppression under paragraph (1).

Subsection (e) states in detail the procedure the court shall follow when it receives a notification under subsection (c) or a suppression motion is filed under subsection (d). This procedure applies, for example, whenever an individual makes a motion pursuant to subsection (d) or 18 U.S.C. 3504, or any other statute or rule of the United States to discover, obtain or suppress evidence or information obtained or derived from electronic surveillance conducted pursuant to this chapter (for example, Rule 12 of the Federal Rules of Criminal Procedure). Although a number of different procedures might be used to attack the legality of the surveillance, it is this procedure "notwithstanding any other law" that must be used to resolve the question. The committee wishes to make very clear that the procedures set out in subsection (e) apply whatever the underlying rule or statute referred to in the motion. This is necessary to prevent the carefully drawn procedures in subsection (e) from being bypassed by the inventive litigant using a new statute, rule or judicial construction.

The special procedures in subsection (e) cannot be invoked until they are triggered by a Government affidavit that disclosure or an adversary hearing would harm the national security of the United States. If no such assertion is made, the committee envisions that mandatory disclosure of the application and order, and discretionary disclosure of other surveillance materials, would be available to the defendant, as is required under title III. When the procedure is so triggered, however, the Government must make available to the court a copy of the court order and accompanying application upon which the surveillance was based.

The court must then conduct an ex parte, in camera inspection of these materials as well as any other documents relation to the surveillance which the Government may be ordered to provide, to determine whether the surveillance was authorized and conducted in a manner which did not violate any constitutional or statutory right of the person against whom the evidence is sought to be introduced. The sub-

secti
cour
to be
tions
it fir
natic
Th
veilla
decid
curri

394 I
U.S.
subse
came
abilit
occas
tellig
Th
is for
and c
noted
Cour:
the d
ancin

t
s
t
b
v
f
is
t
a
a

The
legali
In otl
for ex
identi
which
tion, c
contai
the co
whole
rate de

4. 89
33 Cf. A
Taghianer