

AMERICAN BAR ASSOCIATION
SECTION OF INDIVIDUAL RIGHTS AND RESPONSIBILITIES
REPORT TO THE HOUSE OF DELEGATES

RECOMMENDATION

1 RESOLVED, That the American Bar Association urges the Congress to conduct
2 regular and timely oversight, including public hearings, where appropriate, to
3 ensure that government investigations undertaken pursuant to the Foreign
4 Intelligence Surveillance Act, 50 U.S.C. 1801 et seq. ("FISA" or "the Act")
5 comply with the First, Fourth, and Fifth Amendments to the Constitution and
6 adhere to the Act's purposes of accommodating and advancing both the
7 government's interest in pursuing legitimate intelligence activity and the
8 individual's interest in being free from improper government intrusion.

9 FURTHER RESOLVED, That the American Bar Association urges the Congress
10 to consider amendments to the Act to:

11 (1) Clarify that the procedures adopted by the Attorney General to protect
12 United States persons, as required by the Act, should ensure that FISA is used
13 only for bona fide foreign intelligence-gathering purposes, as contemplated by the
14 Act, and not to circumvent the Fourth Amendment requirements applicable to
15 domestic law enforcement investigations; and

16 (2) Make available to the public an annual statistical report on FISA
17 investigations, comparable to the reports prepared for the Administrative Office
18 of the United States Courts, pursuant to 18 U.S.C. sec. 2519, regarding the use of
19 Federal wiretap authority.
20

REPORT

Introduction

On November 18, 2002, the Foreign Intelligence Surveillance Court of Review significantly altered the legal landscape for intelligence gathering when it issued a groundbreaking decision concerning the scope and application of the Foreign Intelligence Surveillance Act of 1978 (FISA).¹

Enacted in response to severe and highly publicized abuses of foreign intelligence-gathering authority in the decades since World War II, FISA created a special legal regime for approval of counter-intelligence search and surveillance orders that would accommodate "the government's interest in pursuing legitimate intelligence activity" while preserving "the individual's interest in freedom from improper government intrusion."² Specifically, the statute requires the government to apply to a special Foreign Intelligence Surveillance Court (FISC) and to meet legal requirements that are far less demanding than those applicable to electronic surveillance conducted in criminal investigations. It also requires the Attorney General to develop "minimization" procedures to protect innocent U. S. persons from improper surveillance.

In the wake of the terrorist attacks of September 11, 2001, the Administration sought a number of changes to the statute to remove some of the restrictions that the government must satisfy before conducting foreign intelligence surveillance. In October 2001, Congress enacted the USA Patriot Act³, which included significant amendments to FISA. Among the amendments was a change from the requirement that a FISA investigation have as its "primary purpose" the collection of foreign intelligence information to the requirement that foreign intelligence gathering need only be a "significant purpose."⁴

In March 2002, the U. S. Department of Justice (DOJ) proposed new information-sharing procedures that would supersede previous restrictions on the involvement of prosecutors and other law enforcement officials in FISA searches and surveillances.

In May 2002, the FISC, which never before had ruled against the government, rejected the proposed new procedures. The court held that the procedures would permit

¹ 50 U.S.C. § 1801 et seq ("FISA").

² *United States v. Cavanagh*, 807 F. 2d 787, 789 (9th Cir. 1987).

³ ("Patriot Act"), Pub. L. No. 107-56, 115 Stat. 272 (Oct. 26, 2001).

⁴ Prior to enactment of the PATRIOT Act, the statute required the Attorney General or certain other high officials to certify that the purpose of the wiretap or search is to obtain foreign intelligence information. This requirement had been judicially construed to mean that foreign intelligence-gathering must be the *primary* purpose of the application, although that phrase does not occur in the statute.

the use of FISA in criminal investigations that are properly subject to the more stringent Fourth Amendment warrant requirements for Title III wiretaps.⁵

On November 18, 2002, the Foreign Intelligence Surveillance Court of Review reversed.⁶ That court, which was established to consider FISA appeals but never had been called upon to do so, upheld the DOJ's proposed new powers, ruling that the earlier rules ordered by the FISC were required by neither the statute nor the Constitution. Indeed, the Court of Review went so far as to say that the DOJ's own pre-Patriot Act procedures requiring the separation of foreign intelligence-gathering activities from criminal investigations had misinterpreted the statute and placed unnecessary restrictions upon the government's investigative powers.⁷

Following the decision of the Court of Review, the Attorney General stated that the decision "allows the Department of Justice to free immediately our agents and prosecutors in the field to work together more closely and cooperatively" and announced that the DOJ would double the number of attorneys working in its National Security Law Unit to expedite the processing of FISA applications.⁸

The attacks upon our nation have prompted the Congress and the Executive Branch to take unprecedented steps to enhance the safety and well being of our people, including measures to improve the government's ability to investigate and prevent terrorist activities. While some such measures may well be necessary, they also are subject to abuse. There is now a significant danger that if the government can show a "measurable" foreign intelligence purpose⁹ in a given situation, it will elect to use FISA procedures rather than the more exacting standards of Title III, even in a case where the overriding purpose is to bring a criminal prosecution. This situation puts at risk core guarantees of our Constitution, including the Fourth Amendment's protections from unreasonable searches, associational rights protected under the First Amendment, and the Fifth Amendment privilege against self-incrimination.

Under FISA, only the government can appeal a decision by the Court of Review. Thus, that court's Nov. 18 ruling may well be the final judicial statement for the foreseeable future regarding the scope and application of the statute. Any correction in the balance between security needs and constitutional rights therefore must come from the Congress.

⁵ Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. 90-351, tit. III, 82 Stat. 211, adding 18 U.S.C. § 2510 et seq. ("Title III").

⁶ *In re: Sealed Case No. 02-001*, F.I.S. Ct. Rev. (Nov. 18, 2002).

⁷ *Id.*

⁸ Transcript of Attorney General Ashcroft News Conference Regarding Decision of Foreign Intelligence Surveillance Court of Review, November 18, 2002 (hereinafter the "Ashcroft transcript").

⁹ *Id.* At 15.

The proposed resolution urges the Congress to undertake steps to lessen the risk that Constitutional rights will be circumscribed. While expressing no position regarding the specific means by which the Congress should achieve this objective, the proposal does urge specific actions in two areas of primary concern.

First, the recommendation calls upon the Congress to conduct regular and timely oversight of the Justice Department's use of FISA to ensure that investigations comply with the First, Fourth, and Fifth Amendments to the Constitution and adhere to the Act's purposes of accommodating and advancing both the government's interest in pursuing legitimate intelligence activity and the individual's interest in being free from improper government intrusion. Such oversight should include public hearings except where the requirements of national security make open proceedings inappropriate.

Second, the proposed resolution calls for legislation to (1) clarify that FISA is intended to be used only for bona fide foreign intelligence-gathering purposes and not to circumvent the Fourth Amendment requirements applicable to domestic law enforcement investigations; and (2) provide to Congress and the public an annual statistical report regarding the government's use of FISA authorities. Such a report would be comparable to those prepared by the DOJ for the Administrative Office of the United States Courts regarding the use of Title III wiretap authority, without disclosing information regarding specific cases and with redactions, as necessary, to protect classified information, intelligence sources, and methods.

Debate about how to protect this nation adequately while also respecting basic freedoms undoubtedly will continue in the 108th Congress as further anti-terrorism initiatives unfold. By adopting this proposed resolution now, the American Bar Association can be an active participant in that debate and offer possible solutions in an area of critical concern to our members as lawyers and as citizens.

Background

In 1967, the U. S. Supreme Court established in *Katz v. United States*¹⁰ that electronic surveillance constitutes a search subject to Fourth Amendment privacy protections. The privacy threat inherent in electronic surveillance is especially harmful because of the potential that innocent communications will be intercepted. As Justice Douglas similarly noted in a concurring opinion in *Berger v. New York*¹¹ earlier that same year, “The traditional wiretap or electronic eavesdropping device constitutes a dragnet, sweeping in all conversations within its scope—without regard to the participants or the nature of the conversations. It intrudes upon the privacy of those not even suspected of crime and intercepts the most intimate of conversations.”

¹⁰ *Katz v. United States* 389 U. S. 347 (1967) (“Katz”).

¹¹ *Berger v. New York*, 388 U. S. 41, 65 (1967) (“Berger”).

In *Berger*, the Court outlines seven requirements for conducting electronic surveillance consistent with constitutional guarantees: (1) a showing of probable cause that a particular offense has been or is about to be committed; (2) a description with particularity of the conversations to be intercepted; (3) a limitation on the surveillance to a specific, limited period of time in order to minimize the invasion of privacy; (4) continuing probable cause showings for the surveillance to continue beyond the original termination date; (5) the ending of surveillance once the conversation sought is seized; (6) notice to the party surveilled absent an adequate showing of exigency; and (7) a return on the warrant so that the issuing court may oversee and limit the use of the intercepted conversations.

Responding to the *Katz* and *Berger* decisions and growing reports of abuses of government surveillance throughout the 1960's, Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act of 1968¹² to establish uniform, stringent procedures for government use of electronic surveillance in criminal investigations. One of these requirements, incorporating Fourth Amendment principles, is that law enforcement agents may not conduct such surveillance except upon a judge's finding of probable cause that a serious crime has been or is about to be committed.¹³

In addition to requiring probable cause to believe that the subject is committing, has committed, or is about to commit enumerated offenses, Title III surveillance requires probable cause to believe that the target is using the surveilled facility "in connection with the . . . offense."¹⁴ Surveillance targets eventually must receive notification of the surveillance, and targets who later face criminal prosecution can obtain the application under which the court approved the surveillance. Title III orders normally authorize surveillance only for 30 days or less, subject to renewal only under the same requirements that govern initial applications.

In enacting Title III, Congress recognized the special requirements of national security investigations. Just as the Supreme Court had acknowledged in *Katz* that the Executive Branch can establish special surveillance procedures not subject to Fourth Amendment requirements in national security investigations, the statute specifies that "[N]othing in Title III shall . . . be deemed to limit the constitutional power of the President to take such measures as he deems necessary to protect the United States against the overthrow of the Government by force or other unlawful means, or against

¹² Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. 90-351, tit. III, 82 Stat. 211, adding 18 U.S.C. § 2510 et seq. ("Title III").

¹³ 18 U.S.C. § 2518(3)(a).

¹⁴ 18 U.S.C. § 2518(3)(d).

any other clear and present danger to the structure or existence of the Government.”¹⁵

Within a few years, congressional deference began to wane as evidence mounted of extensive governmental misuse of wiretap authority to harass anti-war dissenters; wiretap conversations of government officials, journalists, and civil rights leaders; and conduct other improper domestic surveillance. In 1975-76, the U. S. Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities (“the Church Committee”) held hearings on the government’s use of electronic surveillance and concluded that the government’s use of covert surveillance had been excessive, had circumvented the democratic process, and had violated the Constitution. The Church Committee recommended that Congress prescribe rules to control these activities.¹⁶

Meanwhile, the Supreme Court also had invited Congress to consider establishing special standards to regulate national security surveillance. In *United States v. United States District Court* (“Keith”),¹⁷ the Court recognized the danger of “yielding too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech,”¹⁸ but accepted “potential distinctions between criminal surveillances and those involving the domestic security.” The Court added that “Congress may wish to consider protective standards for the latter which differ from those already prescribed for specified crimes in Title III. Different standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens.”¹⁹

Passage of FISA

The abuses documented in the Church Committee Report, together with the Court’s invitation to the Congress in *Keith* to enact protections against such abuse, helped prompt enactment of FISA in 1978. The statute established special procedures for surveillance in investigations in which the collection of foreign intelligence information is the sole or “primary” purpose. However, FISA’s procedural safeguards for subjects of surveillance are significantly less stringent than those established under Title III for criminal cases.

¹⁵ *Id.*

¹⁶ Senate Select Comm. to Study Governmental Operations With Respect to Intelligence Activities, Final Report, S. Rep. No. 755, 94th Cong., 2d Sess., BK. 1, Foreign and Military Intelligence 614-96 (1976) (“The Church Committee Report”).

¹⁷ *United States v. United States Dist. Court*, 407 U. S. 297 (1972) (“Keith”).

¹⁸ *Id.* at 317.

¹⁹ *Id.* at 322-23.

For example, Title III requires a showing of probable cause that a surveillance target has committed, is committing, or is about to commit a crime. Surveillance orders under FISA, by contrast, require only probable cause to believe that the target is “a foreign power or agent thereof”²⁰ or, if the surveillance is directed at a “U. S. person,”²¹ probable cause to believe that the target is “knowingly engage[d] in clandestine intelligence gathering activities.”²² Also unlike Title III, FISA requires no showing that the target is using the surveilled facility in connection with a crime, and contains no provision for notifying a target that his privacy has been compromised or for providing a target either the application upon which the surveillance was based or the contents of the intercepted communications. While Title III orders run a maximum of 30 days, FISA provides for much longer periods of surveillance. The reporting requirements established by FISA are much more limited than those required under Title III.

However, FISA does establish some procedures to limit potential overreach or constitutional violations. Most important is the requirement that procedures be implemented to minimize the collection, retention, and dissemination of information about United States persons.²³ These so-called minimization procedures²⁴ are designed to prevent foreign intelligence-gathering authorities from being used in routine criminal investigations. Because there often are overlaps between foreign intelligence gathering and criminal investigations, one common minimization procedure is what is known as an information-screening wall. A wall requires an official not involved in a given criminal investigation to review any raw materials obtained through FISA surveillance and pass on only information that might be relevant to the investigation. Use of the wall has been a key factor in helping ensure that information obtained pursuant to FISA warrants is not used improperly in domestic criminal cases.

The special Foreign Intelligence Surveillance Court established under FISA also is intended as a check on potential abuse of FISA authority. Comprised of seven federal

²⁰ 50 U.S.C. § 1805(a)(3)(A).

²¹ A “United States person” is defined FISA as, “a citizen of the United States, an alien lawfully admitted for permanent residence, ... an unincorporated association a substantial number of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power.” 50 U.S.C. § 1801(i).

²² 50 U.S.C. § 1801(b)(2)(A).

²³ § 1801(h)(1).

²⁴ Minimization procedures, as defined by 50 U.S.C. § 1801(h), are “specific procedures, which shall be adopted by the Attorney General, that are reasonably designed, in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination of nonpublicly available information (meaning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information).

district court judges appointed by the Chief Justice of the United States from different federal circuits in staggered terms, the FISC reviews all DOJ applications for FISA orders.

FISA proceedings, however, are not adversarial, but are based entirely upon the DOJ's submissions, made through its Office of Intelligence Policy and Review. The DOJ itself screens applications for counterintelligence warrants by agencies before submitting them to the FISC, and the Attorney General personally approves each final FISA application. The records and files of the cases in which warrants are sought are sealed and generally may not be revealed even to persons whose prosecutions are based upon evidence obtained under FISA warrants.

FISA provides for government appeals of adverse FISC decisions to the Foreign Intelligence Surveillance Court of Review, the court never had convened to consider a matter. Before it ruled the DOJ's proposed new FISA implementation rules and the FISC opinion regarding them.

FISA Amendments in the USA Patriot Act

FISA provided the government unprecedented statutory authority to pursue foreign intelligence-gathering activities, subject only to any constraints the FISC might place upon it in a given case. Following the September 11 tragedy, however, the Administration concluded that further enhancement of the government's surveillance powers was necessary to counter terrorism. The USA Patriot Act, passed a month after September 11, contains several amendments to FISA that expand these powers.

Under the Act, the government now can apply for FISA orders in any investigation in which foreign intelligence gathering is a "significant"²⁵ purpose, rather than the primary purpose of the surveillance. This change greatly expands the range of investigations in which a FISA warrant can be granted, including investigations in which the predominant purpose is criminal enforcement.

The Patriot Act also expands FISA authority to permit "roving wiretaps," which allows the interception of any communications made to or by an intelligence target without specifying the particular telephone line, computer, or other facility to be monitored, and it requires any third parties to a communication (such as common carriers and others) to provide assistance necessary to accomplish the surveillance. It has been argued such "generic" wiretap orders may not comport with the Fourth Amendment's requirement that any search warrant "particularly describe the place to be searched." At

²⁵ 50 U.S.C. § 1804(a)(7)(B).

the very least, such orders increase the likelihood that the private communications of law-abiding American citizens might be intercepted incidentally, particularly in public facilities such as libraries, universities, computer labs, and cyber-cafes.

The Act also eliminates the former FISA requirement that the government prove that the surveillance target is "an agent of a foreign power" before obtaining a pen register/trap and trace order under FISA.²⁶ The government now can obtain a pen register/trap and trace order for any investigation to gather foreign intelligence information without any showing that the telephone user is engaged in international terrorism or clandestine intelligence activities. This amendment also increases the risk that innocent persons will be caught up in FISA surveillances.²⁷

Finally, while FISA originally authorized warrants only for electronic surveillance, it now permits issuance of search warrants for "any tangible thing," which can include books, records, papers, floppy disks, data tapes, and computers with hard drives.²⁸ This amendment, which overrides state library confidentiality laws protecting library records, permits the government to compel production of business records, medical records, educational records, and library records, including stored electronic data and communications, without requiring the agent to demonstrate "probable cause," the existence of specific facts to support the belief that a crime has been committed, or a likelihood that the items sought are evidence of a crime. A person served with a search warrant issued under FISA rules is forbidden to disclose, under of penalty of law, the existence of the warrant or the fact that records were produced as a result of the warrant.

The FISC and Court of Review Decisions

In March 2002, following enactment of the Patriot Act, the Attorney General submitted a memorandum to the FISC requesting approval of proposed new information-sharing procedures and other proposals. This memorandum, entitled, "Intelligence Sharing Procedures for Foreign Intelligence and Foreign Counterintelligence Investigations Conducted by the FBI," included proposed new "minimization" procedures that would break down significantly the information-screening walls established under prior DOJ procedures.

²⁶ 50 U.S.C. § 1842. (A pen register collects the outgoing phone numbers placed from a specific telephone line, a trap and trace device captures the incoming numbers placed to a specific phone line. For example, a caller-id box is a trap and trace device).

²⁷ Notably, the Act does include a provision prohibiting use of FISA pen register surveillance under any circumstances against a U. S. citizen, if the investigation is being conducted "solely on the basis of activities protected by the First Amendment."

²⁸ 50 U.S.C. § 1862

The proposed new rules permit FISA surveillance to be initiated, directed, and controlled by law enforcement officials. Criminal prosecutors are to be given routine access to information obtained pursuant to FISA warrants, and the prosecutor is to be allowed to direct intelligence investigations when appropriate.

The FISC which never before had ruled against the government, rejected these proposals.²⁹

Citing serious abuses of existing FISA authority,³⁰ the FISC concluded that the proposed new procedures would give prosecutors too much control over intelligence investigations and would allow the government to circumvent the more stringent Title III wiretap requirements by obtaining information for criminal investigations under the lower FISA standards. As the court stated, "The 2002 procedures appear to be designed to amend the law and substitute the FISA for Title III electronic surveillance and Rule 41 searches."³¹

On August 22, 2002, the Attorney General filed a formal appeal of the FISC opinion with the Court of Review.³² The court heard DOJ's oral argument in defense of its proposed rules in a closed hearing on September 9, 2002. This proceeding, like all those held before the FISC, was non-adversarial; there was no party appointed to argue the position taken by the lower court.

In a decision announced on Nov. 18, 2002, the Court of Review rejected the FISC's conclusions. The court held that FISA, as amended by the Patriot Act, supports the government's position that ". . . the restrictions imposed by the FISA court are not required by FISA or the Constitution."³³ It found that the FISC had read into FISA limitations that never existed and do not appear anywhere in the statute. Indeed, the Court of Review went so far as to say that the DOJ's own pre-Patriot Act procedures requiring the separation of foreign intelligence-gathering activities from criminal

²⁹ In Re All Matters Submitted to the Foreign Intelligence Surveillance Court, Memorandum Opinion, May 17, 2002 ("May 17 Opinion").

³⁰ The May 17 Opinion states that the Justice Department and FBI supplied erroneous information to the FISC in more than 75 applications for search warrants and wiretaps and improperly shared intelligence information with investigators and prosecutors handling criminal cases on at least four occasions.

³¹ Id. at 22.

³² The government did not appeal the FISC's May 17 decision. In July, the government submitted an apparently unrelated FISA application, which was granted by the FISC. However, in the opinion, the FISC (Baker, J.) denied the government's request that the July application be subject to the unmodified March 2002 procedures, and ruled that the surveillance order would be subject to the March 2002 procedures, as modified by the FISC's May 17 Opinion. The government's appeal relates to the FISC's July decision.

³³ *In re: Sealed Case No. 02-001*, F.I.S. Ct. Rev. (Nov. 18, 2002).

investigations had misinterpreted the statute and placed unnecessary restrictions upon the government's investigative powers.

The Court of Review's decision effectively eliminates the minimization procedures originally established in FISA to maintain the wall between federal personnel conducting surveillance on suspected foreign agents and criminal prosecutors investigating crimes. There is now a significant danger that if the government can show a "measurable" foreign intelligence purpose in a given situation, it will elect to use FISA procedures rather than the more exacting standards of Title III, even in a case where the overriding purpose is to bring a criminal prosecution. Indeed, the Attorney General has indicated his intention to do so.

Legislative Responses to Date

The 107th Congress had adjourned by the time the Court of Review issued its opinion. But the May 17 FISC Opinion already had led to inquiries in both houses of the Congress.

In June 2002, the House Judiciary Committee asked the Justice Department for information concerning implementation of the Patriot Act in preparation for anticipated hearings to "allow further public discussion of these and other issues relating to the Department of Justice's activity in investigating terrorists or potential terrorist attacks."³⁴ The DOJ replied that information responsive to some of the Committee's questions was classified and could be provided only to the House Intelligence Committee.³⁵ The classified answers related to questions asked about FISA, specifically.³⁶ The House

³⁴ Letter from Rep. F. James Sensenbrenner, Jr., Chairman, House of Representatives Committee on the Judiciary, to Attorney General John Ashcroft 1 (June 13, 2002).

³⁵ Letter from the Office of the Attorney General to Rep. Sensenbrenner, Chairman, House of Representatives Committee on the Judiciary 1 (July 26, 2002).

³⁶ Questions included: how many times the DOJ has obtained and utilized roving wiretap, search, and surveillance orders under FISA; how many times the DOJ has obtained orders to install pen registers for use on facilities used by United States persons; how many applications have been made for tangible objects, including how many total applications were made and, of those, how many applications were made by FBI Assistant Special Agents in Charge, rather than a higher ranking official, and how many orders were issued upon the application of FBI Assistant Special Agents in Charge; how many times the Patriot Act amendments have been used to obtain records from a public library, bookstore, or newspaper, specifically whether records sought have related to named individuals, whether the records sought have included the entire data base, and whether the decision to seek orders for bookstore, library, or newspaper records was subject to any special policies or procedures such as requiring supervisory approval or requiring a determination that the information is essential to an investigation and could not be obtained through any other means; how many U.S. persons have been subject to new FISA surveillance orders since enactment of the Act, and how that number compares with the number of U.S. persons subject to such orders during the same period in the prior fiscal year; and what

Judiciary Committee, while sensitive to the need for classifying certain FISA-related matters, has indicated that operations of the FISC and the Court of Review also are important matters for its own review.

The Senate also engaged in oversight efforts in response to the FISC opinion. The Senate Intelligence Committee held a hearing on July 31, and the Senate Judiciary Committee, on September 10.

It seems certain that Congress will soon revisit these questions. Indeed, some legislative proposals have already been introduced that would further erode constitutional protections in intelligence-gathering investigations.³⁷

The Proposed ABA Resolution

The government's surveillance authority, even in the realm of foreign intelligence and after the terrorist attacks of September 11, is not and should not be absolute. Although the government must have the tools necessary to do everything possible to prevent another attack on our nation, the recent Court of Review decision creates a significant risk of excessive use of government surveillance authority without adequate oversight.

In *Keith*, the Supreme Court stated that standards that differ from those set forth in Title III could comport with the Fourth Amendment, as long as they are "reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens."³⁸ FISA represented Congress's attempt to meet that test. The decision by the Court of Review has upset that balance, and it is up to the Congress to restore it.

The proposed resolution calls upon the Congress “. . . to conduct regular and timely oversight, including public hearings, where appropriate, to ensure that government investigations undertaken pursuant to the Foreign Intelligence Surveillance Act comply with the First, Fourth, and Fifth Amendments to the Constitution and adhere to the Act’s purposes of accommodating and advancing both the government's interest in pursuing

procedures are in place to ensure that searches and surveillances are not sought solely on the basis of activities protected by the First Amendment.

³⁷ E.g., one proposal, S. 2659, would lower the standard of proof required for issuance of FISA orders regarding non-United States persons from “probable cause” to “reasonable suspicion” and to delete the limitation of FISA’s application to an “agent of a foreign power,” at least with regard to non-U. S. persons.

³⁸ *Keith* at 322-23.

legitimate intelligence activity and the individual's interest in being free from improper government intrusion.”

The proposed resolution also urges the Congress to amend FISA to clarify that FISA is intended to be used only for bona fide foreign intelligence-gathering purposes and not to circumvent the Fourth Amendment requirements applicable to domestic law enforcement investigations.

Finally, to aid congressional oversight and to increase confidence that a largely secret court in which fundamental rights are at stake is working properly, the proposed resolution calls for annual statistical reports on the use of FISA. The existing reporting requirement is limited to a report of the aggregate number of applications each year, without further detail. To be meaningful, the report should be comparable, although certainly not identical, to the reports prepared for the Administrative Office of the United States Courts, pursuant to 18 U.S.C. § 2519, regarding the use of federal wiretap authority. Such information as the number of electronic surveillance and searches, number of targets, number of roving wiretaps, number of search or surveillance targets prosecuted, and the number of targets who are U. S. persons generally could be provided without risk to national security. This reporting would not entail disclosures of specific cases and redactions could be made, as necessary, to protect classified information, intelligence sources, and methods.

Conclusion

In the pre-FISA era of largely unregulated surveillance, the Supreme Court observed that government surveillance of communications inherently "involves an intrusion on privacy that is broad in scope" and its "indiscriminate use . . . in law enforcement raises grave constitutional questions."³⁹ Despite subsequent legislation to guard against government misuse of its surveillance powers, the possibility of indiscriminate use of such powers remains a real threat today.

Regular congressional oversight of government activity pursuant to FISA would restore an appropriate balance between the executive and legislative branches of government in the conduct of surveillance activities. Appropriate reporting procedures would enhance public confidence that the government's national security initiatives are being carried out within the bounds of the nation's constitutional framework. And legislative changes advocated in the proposed resolution would help ensure that measures intended to protect our nation do not instead become a means of constraining or eliminating fundamental constitutional rights.

³⁹ *Berger v. New York*, 388 U. S. 41, 56 (1967).

The proposed resolution should be adopted by the ABA House of Delegates in order to strike a proper balance between individual liberty and executive branch foreign surveillance authority.

Respectfully submitted,

Mark D. Agrast, Chair
Section of Individual Rights and Responsibilities

February 2003

GENERAL INFORMATION FORM

Submitting Entity: Section of Individual Rights and Responsibilities

Submitted By: Mark D. Agrast, Section Chair

1. Summary of Recommendation(s).

The resolution urges the Congress to conduct regular and timely oversight of the government's use of the Foreign Intelligence Surveillance Act (FISA) to ensure that FISA investigations comply with the First, Fourth, and Fifth Amendments to the Constitution and adhere to the Act's purposes of accommodating and advancing both the government's interest in pursuing legitimate intelligence activity and the individual's interest in being free from improper government intrusion.

The resolution also calls for amendments to FISA to (1) clarify that FISA is intended to be used only for bona fide foreign intelligence-gathering purposes and not to circumvent the Fourth Amendment requirements applicable to domestic law enforcement investigations; and (2) provide for an annual statistical report, available to the public, regarding the government's use of its surveillance authority under FISA.

2. Approval by Submitting Entity.

The Council of the Section of Individual Rights and Responsibilities approved the Report with Recommendation in principle on October 18, 2002, during its fall meeting. The final version of the Report with Recommendation was approved for submission on Dec. 4, 2002.

3. Has this or a similar recommendation been submitted to the House or Board previously?

This recommendation has not been submitted previously to the House of Delegates or the Board of Governors. However, several recommendations regarding the ABA's support of privacy and surveillance protections have been submitted to and approved by the House of Delegates in previous years.

4. What existing Association policies are relevant to this recommendation and how would they be affected by its adoption?

The ABA has adopted several resolutions in support of communications privacy, including policies dealing with electronic surveillance (01M103A). The proposed Resolution would build upon this and other existing policies, including policies that:

- Support legislation to facilitate and regulate the exchange of criminal justice information in a manner to protect against unauthorized use and to ensure privacy. 8/72
- Support various principles to protect the privacy of personal records that are kept by the government or by organizations. 8/79
- Support amendment of the federal wiretap law to protect the transmission of all forms of information, including voice, data, and video; support statutory control of government access to messages stored by electronic mail systems and remote data processing services. 8/86
- Urge courts to accord lawyer-client electronic mail communications the same expectations of privacy and confidentiality as those accorded traditional means of communication. (98A119A) 8/98
- Urge courts to adopt principles that wireless telephone communications should be accorded same expectations of privacy as ordinary telephone calls, and that use of such phones by lawyers does not alter the lawyer-client communication privilege. (99A117) 8/99

5. What urgency exists which requires action at this meeting of the House?

Approval of the proposed resolution at the ABA 2003 Midyear Meeting in Seattle is essential to enable the ABA to promote federal legislation to help preserve fundamental Constitutional rights currently at risk as a result of recent governmental and judicial actions involving the scope and application of the Foreign Intelligence Surveillance Act (FISA). These actions have brought many more individuals and investigations under FISA authority, with its low-threshold standards for issuance and operation of surveillance warrants, and have greatly weakened longstanding distinctions between the government's criminal investigations, traditionally guided by Fourth Amendment principles, and its intelligence-gathering activities, subject primarily only to FISA provisions. These results, which implicate individuals' Fourth and Fifth Amendment rights, as well as privacy under First Amendment associational rights, can be addressed only through federal legislation to amend FISA. Because the government has indicated that it intends to increase its use of FISA surveillance significantly and because the Congress is likely to consider FISA-related legislation in its next term, it is important to have the proposed ABA policy in place early in the new congressional term so that the ABA can participate in that debate and offer possible solutions in an area of critical concern to ABA members as lawyers and as citizens.

6. Status of Legislation. (If applicable.)

There is no legislation pending as of the submission of this report with recommendation.

But the recommendation concerns the Foreign Intelligence Surveillance Act (FISA), which the Congress enacted in 1978 to prescribe procedures for government's use of electronic surveillance and physical search of persons engaged in espionage or international terrorism against the United States on behalf of a foreign power and established a special Foreign Intelligence Surveillance Court (FISC) to review government requests for approval of surveillance applications, as well as a special Court of Review to consider government appeals from any denials of FISA applications. In October 2001, the Congress enacted the USA Patriot Act, which included several provisions expanding government surveillance powers under FISA. In March 2002, the U. S. Department of Justice sought approval from the FISC for new rules for implementing FISA. In June 2002, the FISC rejected the proposed rules; in November 2002, the Court of Review reversed the FISC decision. There is no provision for appeal of a Court of Review decision. It therefore is likely that legislation relating to this decision could be introduced in the next Congress.

In the last Congress, several bills addressing FISA issues were introduced in the Senate but none was adopted. It is likely that these bills will be re-introduced in the new Congress. In addition, it is likely that one or both Houses will hold hearings on FISA-related issues.

7. Cost to the Association. (Both direct and indirect costs.)

Adoption of this recommendation would result only in minor indirect costs associated with Governmental Affairs and Section staff time devoted to the policy subject matter as part of the staff members' overall substantive responsibilities.

8. Disclosure of Interest. (If applicable.)

There are no known conflicts of interest.

9. Referrals.

By copy of this information form, this Report with Recommendation will be referred to the following:

All ABA Sections and Divisions
ABA Task Force on Terrorism and National Security
ABA Standing Committee on Law and National Security

10. Contact Person. (Prior to the meeting.)

Marc S. Rotenberg, Chair, IRR Section Privacy and Information Protection Committee
1718 Connecticut Ave NW, Suite 200
Washington DC 20009
Tel.: 202/483-1140
Fax: 202/483 1248
E-mail: rotenberg@epic.org

Penny Wakefield, IRR Section Director
American Bar Association
740 15th Street, NW
Washington, DC 20005
Tel.: 202/662-1030
Fax: 202/662-1032
E-mail: Wakefieldp@staff.abanet.org

11. Contact Person. (Who will present the report to the House.)

C. Elisia Frazier, IRR Section Delegate
200 E. Berry Street, No. 2R-13
Fort Wayne, IN 46802-2706
Tel.: 219/455-5493
Fax: 219/455-5403
E-mail: cef1938@comcast.com

12. Contact Person Regarding Amendments to This Recommendation. (Are there any known proposed amendments at this time? If so, please provide the name, address, telephone, fax and ABA/net number of the person to contact below.)

There are no known proposed amendments at this time. The contact person regarding amendments to this recommendation is:

Mark D. Agrast, Chair, IRR Section
1419 Crittenden St., NW
Washington, DC 20011
Tel.: 202/225-3111
Fax: 202/225-5658
E-mail: mark.agrast@mail.house.gov