Fordham Law Review

Volume 48 | Issue 6 Article 1

1980

Intelligence Gathering and the Law: Conflict or Compatibility?

Benjamin R. Civiletti

Intelligence Gathering and the Law: Conflict or Compatibility?

Cover Page Footnote

Attorney General of the United States. This Article is adapted from the Tenth Annual John F. Sonnett Memorial Lecture, delivered by the Attorney General at the Fordham University School of Law on January 15, 1980. This Article was prepared with the assistance of several attorneys in the Department of Justice, particularly Kenneth B. Reisenfeld of the Office of Intelligence Policy and Review.

INTELLIGENCE GATHERING AND THE LAW: CONFLICT OR COMPATIBILITY?

*BENJAMIN R. CIVILETTI**

INTRODUCTION

THESE are troubled times for international legal order. A band of terrorists has seized the American Embassy in Tehran and holds United States diplomats hostage.[1] The International Court of Justice[2] considered this international outrage and ruled unanimously that the hostages must be freed.[3] The court declared that "[t]here is no more fundamental prerequisite for the conduct of relations between states than the inviolability of diplomatic envoys and embassies," a principle of international law so well established that "thoughout history nations of all creeds and cultures have observed reciprocal obligations for that purpose."[4] Iran refused to comply with the court's order to release the hostages. With similar disdain for international law, Soviet armed forces have invaded a sovereign nation and installed a puppet government.[5] Following a Soviet veto of a Security Council resolution,[6] the United Nations General Assembly overwhelmingly condemned the actions of the Soviet Union and declared that the invasion and occupation of Afghanistan is deplorable and inconsistent with the principles of the United Nations charter.[7]

Iran's continuing defiance of the very foundations of international law demonstrates the fragility of the law as a means of ordering human behavior. The action of the Soviet Union damages the rule of law even

---

* Attorney General of the United States. This Article is adapted from the Tenth Annual John F. Sonnett Memorial Lecture, delivered by the Attorney General at the Fordham University School of Law on January 15, 1980. This Article was prepared with the assistance of several attorneys in the Department of Justice, particularly Kenneth B. Reisenfeld of the Office of Intelligence Policy and Review.

1. N.Y. Times, Nov. 5, 1979, § A, at 1, col. 4; *id.*, Apr. 8, 1980, § A, at 1, col. 3.

2. The International Court of Justice (ICJ) is the "principal judicial organ of the United Nations." U.N. Charter art. 92, 59 Stat. 1031, 1051 (1945), T. S No. 993, at 21. The ICJ consists of 15 members, each from different nations, who serve for nine-year terms. Statute of the International Court of Justice, June 26, 1945, arts. 3, 13, 59 Stat. 1055, 1055-56, T. S. No. 993, at 25-26. Member states of the United Nations may unilaterally invoke the ICJ's jurisdiction in several situations, including a dispute involving "any question of international law [and] the existence of any fact which, if established, would constitute a breach of an international obligation." *Id.*, art. 36, 59 Stat. at 1060, T. S. No. 993, at 30.

3. United States Diplomatic and Consular Staff in Tehran, United States v. Iran, I.C.J. (Order of Dec. 15, 1979).

4. *Id.* at 16.

5. N.Y. Times, Dec. 27, 1979, § A, at 1, col. 6; *id.*, Dec. 31, 1979, § A, at 1, col. 4.

6. N.Y. Times, Jan. 8, 1980, § A, at 1, col. 2.

7. G.A. Res. ES-6/2 (Jan. 14, 1980).

more significantly because its action cannot be rationalized as an aberrational act by revolutionary terrorists. Indeed, the Soviets claim shamelessly that their invasion was required by a mutual defense treaty with Afghanistan.[8] Both events illustrate that international law is not self-executing, and that our ability to enforce the law through peaceful means is limited. When the law is broken with apparent impunity, the ensuing frustration may result in a willingness to reject the very concept of law itself and a temptation to engage in acts we would otherwise condemn. There are indications that such feelings are astir within our nation today. Nevertheless, we must not permit our frustration to result in the abandonment of recently developed legal strictures on the intelligence-gathering activities of the United States.

This Article focuses on the evolving relationship between the rule of law and the intelligence-gathering activities of our government. The collection and utilization of intelligence information are essential ingredients of foreign policy and national security, and the dramatic increase in international tensions emphasizes our country's crucial need for timely and accurate foreign intelligence. Nevertheless, past excesses in the conduct of intelligence activities indicate that such operations cannot be implemented without careful regard for the rule of law.[9] The following analysis considers the complexities of developing a rule of law that comports with the genuine need of our government to engage in foreign intelligence activities and preserves the civil liberties and privacy interests of our citizens.[10]

I. THE NATURE AND ROLE OF INTELLIGENCE GATHERING

In the past, the line between foreign and domestic intelligence gathering often was not clearly drawn.[11] The Executive Branch,

8. N.Y. Times, Dec. 31, 1979, § A, at 1, col. 1.

9. A number of congressional committees and executive commissions have thoroughly investigated instances of misconduct by the intelligence agencies. *E.g.*, S. Rep. No. 755, 94th Cong., 2d Sess. (1976) [hereinafter cited as the Church Committee Report]; *United States Intelligence Agencies and Activities: Performance of the Intelligence Community: Hearings Before the House Select Comm. on Intelligence*, 94th Cong., 1st Sess. (1974); *Domestic Intelligence Operations for Internal Security Purposes: Hearings Before the House Comm. on Internal Security*, 93rd Cong., 2d Sess. (1974); Staff of Subcomm. on Constitutional Rights of the Senate Comm. on the Judiciary, 92nd Cong., 2d Sess., Report on Army Surveillance of Civilians: A Documentary Analysis (1972); Commission on CIA Activities Within the United States, Report to the President (June, 1975), [hereinafter cited as the Rockefeller Commission Report].

10. A number of authors have grappled with the evolving rule of law in the area of national security. *E.g.*, Theoharis & Meyer, *The "National Security" Justification for Electronic Eavesdropping: An Elusive Exception*, 14 Wayne L. Rev. 749 (1968); *Developments in the Law — The National Security Interest and Civil Liberties*, 85 Harv. L. Rev. 1130 (1972); Comment, *Privacy and Political Freedom: Applicability of the Fourth Amendment to "National Security" Investigations*, 17 U.C.L.A. L. Rev. 1205 (1970); Note, *Foreign Security Surveillance and the Fourth Amendment*, 87 Harv. L. Rev. 976 (1974).

11. The difficulty of distinguishing between domestic and foreign intelligence-gathering operations has partially resulted from an inability to define clearly the terms applicable to

however, is now careful to distinguish these two concerns. Thus, intelligence is defined to include only foreign intelligence and counterintelligence,[12] both of which, in turn, are defined as information relating to "*foreign* powers, organizations or persons."[13] Recent bureaucratic reorganizations and the promulgation of rules, regulations, and guidelines have also reflected this sharp domestic/foreign distinction.[14] In the Federal Bureau of Investigation (FBI), for example,

various types of surveillances. The confusion has generally been clarified as case law and statute have increasingly abandoned or defined the term national security. For example, in Katz v. United States, 389 U.S. 347 (1967), the Court reserved decision on the question of the applicability of the fourth amendment warrant requirement to national security electronic surveillance. *Id.* at 358 n.23.

In United States v. United States Dist. Court (Keith), 407 U.S. 297 (1972), the Court analyzed the domestic aspects of national security but once again reserved "the issues which may be involved with respect to activities of foreign powers or their agents." *Id.* at 322 (footnote omitted); *see* United States v. Smith, 321 F. Supp. 424, 429 (C.D. Cal. 1971) (applicability of warrant requirement to *foreign* national security surveillance not decided, although warrant mandated for *domestic* security surveillances). *Keith* may have added to the confusion surrounding the meaning of national security. The opinion emphasizes that it is often difficult to distinguish between domestic and foreign threats to the nation's security. 407 U.S. at 309 n.8. The Court acknowledged that Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510-2520 (1976), uses the term national security to refer only to the activities of foreign powers. *Id.* § 2511(3). Nevertheless, the Court continued to apply the term national security to both domestic and foreign intelligence operations. 407 U.S. at 309 n.8.

In Zweibon v. Mitchell, 516 F.2d 594 (D.C. Cir. 1975) (en banc), *cert. denied*, 425 U.S. 944 (1976), the court extended *Keith* and the warrant requirement to a wiretap of a domestic organization that is neither the agent of, nor acting in collaboration with, a foreign power, even if the surveillance is undertaken in the name of foreign intelligence gathering. The court, in a very long footnote, attempted to distinguish between "internal security" or "domestic security" and "foreign security." *Id.* at 613 n.42. The court's efforts failed, however, when it concluded: " 'National security' will generally be used interchangeably with 'foreign security,' except where the context makes it clear that it refers to both 'foreign security and 'internal security.' " *Id.* On remand, the district court established its own categorization and distinguished "domestic security," "domestic national security," and "foreign security" surveillances. Zweibon v. Mitchell, 444 F. Supp. 1296, 1299 n.3 (D.D.C. 1978), *rev'd in part and remanded on other grounds*, 606 F.2d 1172 (D.C. Cir. 1979). Although these classifications appear to correlate roughly with the distinctions provided in Exec. Order No. 12036, 3 C.F.R. 112 (1979), the terminology used may foster continued confusion.

12. Exec. Order No. 12036, § 4-206, 3 C.F.R. 112, 133 (1979).

13. *Id.* §§ 4-202, -205, 3 C.F.R. 112, 133 (1979) (emphasis added). Foreign intelligence is defined as "information relating to the capabilities, intentions and activities of foreign powers, organizations or persons," *id.* § 4-205, 3 C.F.R. at 133, and counterintelligence is defined as "information gathered and activities conducted to protect against espionage and other clandestine intelligence activities, sabotage, international terrorist activities or assassinations conducted for or on behalf of foreign powers, organizations or persons." *Id.* § 4-202, 3 C.F.R. at 133. Intelligence organizations have not always had the benefit of such specific definitions. Sherman Kent, former chairman of the CIA's Board of National Estimates, described intelligence in his pivotal book as comprising three definitional subjects: knowledge that our nation must have regarding other nations to assure itself that planning and decisionmaking will not be conducted in ignorance; an organization structured to obtain, centralize, and evaluate that knowledge; and the activity of gathering such knowledge. S. Kent, Strategic Intelligence For American World Policy at ix (1949).

14. Although many of the regulations and guidelines are not available in published form, they

criminal and intelligence investigations are handled by two separate divisions.[15] Similarly, the President's Executive Order on Intelligence Activities specifically provides that it does not "apply to or interfere with any authorized civil or criminal law enforcement responsibility of any department or agency."[16]

This distinction between foreign intelligence and domestic law enforcement reflects not only the attitude of the courts[17] and the legislature,[18] but also the present belief of the Executive Branch that the purposes of intelligence gathering are fundamentally different from those of domestic law enforcement and, therefore, require different regulations. Law enforcement is intended to discover and punish acts which society deems unacceptable. Intelligence activities are intended to acquire information so that the President and his advisors can make informed decisions in conducting international diplomacy, foreign relations, and national security affairs.[19] In counterintelligence, however, there are some areas in which intelligence and domestic law-enforcement interests overlap. This intersection is particularly appar-

---

can be obtained from the agency which they govern. Requests should be made in the same manner as requests under the Freedom of Information Act.

15. All foreign intelligence and counterintelligence investigations are handled by the Intelligence Division (Division 5), and all domestic security and international terrorism investigations are within the purview of the Criminal Investigation Division (Division 6). *See* note 14 *supra.*

16. Exec. Order No. 12036, § 4-107, 3 C.F.R. 112, 133 (1979).

17. *See* note 11 *supra.*

18. *See* notes 49-59 *infra* and accompanying text.

19. Positive foreign intelligence surveillances differ markedly from those in criminal investigations. For example, a foreign intelligence surveillance may be undertaken without probable cause to believe a crime has been committed, and may be of considerable duration and scope. United States v. Humphrey, 456 F. Supp. 51, 56 (E.D. Va. 1978). Its purpose is to gather information about the intentions and capabilities of a foreign government, not to obtain admissible evidence of a crime. *Id. But see* United States v. Stone, 305 F. Supp. 75, 82 (D.D.C. 1969) (foreign intelligence wiretap used as evidence in criminal trial); United States v. O'Baugh, 304 F. Supp. 767, 768 (D.D.C. 1969) (wiretap of embassy used as evidence in criminal proceeding). Foreign counterintelligence activities more closely parallel law enforcement activities. Nevertheless, while it is true that many activities of the targets of counterintelligence surveillances may be criminal, *see, e.g.,* 18 U.S.C. § 641 (1976) (relating to unauthorized use of government property); *id.* §§ 792-799 (relating to espionage); *id.* §§ 2151-2157 (relating to sabotage); *id* §§ 2381-2391 (relating to treason, sedition, and subversive activities), the primary objective of the surveillance is not preparation for prosecution. *But see,* United States v. Humphrey, 456 F. Supp. at 56 (distinguishing between foreign intelligence surveillance and domestic surveillance and stating that: "It would seem rare that the government would engage in domestic electronic surveillance without some plans to prosecute *at some time.*"); Zweibon v. Mitchell, 516 F.2d 594, 648 (D.C. Cir. 1975) (en banc) (claiming it is a "myth to characterize national security surveillance as purely non-prosecutorial in the criminal sense"), *cert. denied,* 425 U.S. 944 (1976). The objective of a counterintelligence surveillance is to identify, isolate, and prevent breaches of security in the foreign intelligence and national defense apparatus. The distinction between certain intelligence surveillances and law enforcement activities was carefully set forth in the Senate Report accompanying the Foreign Intelligence Surveillance Act. S. Rep. No. 604, 95th Cong., 1st Sess. 4-7 (1977), *reprinted in* [1978] U.S. Code Cong. & Ad. News 3904, 3905-09.

ent when the government attempts to monitor clandestine information gathering by foreign agents in the United States because many forms of foreign espionage conducted within our nation's borders are crimes under federal law.[20] The need to observe the activities of agents of foreign powers and to defend against their operations demands considerable caution.[21]

Intelligence activities, which, as presently defined, pertain only to foreign affairs and national security issues,[22] must be kept strong and effective. The government needs to obtain the best information available concerning the intentions and activities of foreign powers. The ability of the United States to react to events in foreign lands is limited under any circumstances. Without timely and accurate information, the ability to react constructively is eliminated. Moreover, obtaining critical intelligence is exceedingly difficult. Although it may be virtually impossible, given today's technology, for any country to conceal substantial troop movements, the transfer of funds and arms and the strategies of foreign governments are not as readily detectable. Unless we possess current, accurate knowledge about the actions a foreign power is likely to take, our information base is limited; and the more limited our information base, the more speculative are our analyses, and the greater the danger to our security. Secrecy, however, is an

20. *See* note 19 *supra*. There has been some concern regarding the adequacy of the espionage statutes in certain circumstances. *See Espionage Laws and Leaks: Hearings Before the Subcomm. on Legislation of the House Permanent Select Comm. on Intelligence*, 96th Cong., 1st Sess. (1979). *See generally* Edgar & Schmidt, *The Espionage Statutes and the Publication of Defense Information*, 73 Colum. L. Rev. 929 (1973); Nimmer, *National Security Secrets v. Free Speech: The Issues Left Undecided in the Ellsberg Case*, 26 Stan. L. Rev. 311 (1974).

21. Only a small percentage of all counterintelligence cases can be considered for successful criminal prosecutions, and investigations of foreign intelligence agents are seldom conducted from the outset as they would be were eventual prosecution expected. Many counterintelligence professionals believe that criminal prosecutions should never be brought against hostile agents because doing so may only result in their replacement by other, unknown agents of whose activities we may not be aware. Moreover, criminal proceedings may not only confirm the accuracy of classified information that has been passed to a foreign power, but may also reveal at least some of the material to a far wider audience. This problem is known as "graymail." *See* Senate Select Comm. on Intelligence, 95th Cong., 2d Sess., Report on National Security Secrets and the Administration of Justice (Comm. Print 1978). Graymail problems, however, are not insurmountable. For example, in United States v. Kampiles, 609 F.2d 1233 (7th Cir. 1979), the trial court's procedures and judgment avoided the graymail problem. The trial court prevented classified information from being introduced at trial by issuing a protective order after in camera, ex parte proceedings in which the government presented evidence of the sensitive document that was passed to the Soviets and of the FBI's counterintelligence investigation into the document's disappearance. *Id.* at 1248. The court of appeals upheld the espionage conviction based upon the defendant's confession that he had met with and sold a classified document to a Soviet intelligence officer and upon sufficient other evidence to corroborate the reliability of the defendant's confession. *Id.* at 1238.

The Administration has introduced legislation to resolve the graymail problem and to establish a workable and fair procedure for handling classified information in criminal cases. *See* note 102 *infra*.

22. *See* note 13 *supra* and accompanying text.

essential element of effective intelligence gathering. Even if we are able to gain information concerning a hostile foreign nation, our success will be shortlived if we disclose the facts of our success. Further, if we reveal the information obtained, we will not only lose our advantage and risk changes in the acquired plans, but we will also jeopardize or perhaps destroy our sources and methods of gathering information.[23]

What makes these seemingly self-evident observations controversial is that intelligence activities can come perilously close to intruding upon our most basic statutory and constitutional rights.[24] This inherent danger is increased by the highly sophisticated technological advances, commonly used throughout the world today, that widen the range of possible intelligence-gathering activities. The necessity of secrecy, however, often prohibits any judicial review of questionable intelligence activities.[25] The Executive Branch, therefore, is required to redouble its efforts to ensure that intelligence activities are not exempted from all responsible checks and balances.[26] The need to create

---

23. There is continuing debate concerning the need for and scope of legitimate government secrecy. *Compare* Snepp v. United States, 100 S. Ct. 763, 765 n.3 (1980) (stating "[t]he [g]overnment has a compelling interest in protecting both the secrecy of information important to our national security and the appearance of confidentiality so essential to the effective operation of our foreign intelligence service") *and* Colby, *Intelligence Secrecy and Security in a Free Society,* Int'l Security 3 (Fall 1976) (setting forth a conceptual framework for limiting unnecessary government disclosures) *with* Church Committee Report, *supra* note 9, (Bk. I) at 16 (recognizing the dangers of excessive secrecy to a democracy) *and* M. Halperin & D. Hoffman, Top Secret: National Security and the Right to Know (1977) (arguing that the secrecy veil of the intelligence community needs to be pierced). *See generally Investigation of Publication of Select Comm. on Intelligence Report: Hearings Before the House Comm. on Standards of Official Conduct,* 94th Cong., 2d Sess. (1976).

24. *See* pt. III *infra.*

25. The Foreign Intelligence Surveillance Act of 1978, 50 U.S.C.A. §§ 1801-1811 (West Supp. 1979), does provide judicial review of certain intelligence activities. *See* note 48 *infra.* The proposed National Intelligence Act of 1980, S. 2284, 96th Cong., 1st Sess., 126 Cong. Rec. S1307 (daily ed. Feb. 8, 1980) [hereinafter cited as S. 2284], would expand the scope of judicial review to cover physical searches as well as electronic surveillance both within the United States and abroad. *Id.* § 801.

26. Executive Order 12036 and its implementing regulations create an effective structure for oversight of intelligence activities within the Executive Branch. The duty to identify, inspect, and report unlawful or improper activity is placed upon senior officers throughout the intelligence community. Exec. Order No. 12036, § 1-7, 3 C.F.R. 112, 119-20 (1979). This obligation is reinforced and monitored by the Inspectors General and General Counsel for each agency. *Id.* § 3-2, 3 C.F.R. at 131. These officers are required to investigate and report to the Intelligence Oversight Board any activities that raise questions of legality or propriety. *Id.* The executive order also gives the Attorney General substantial oversight and review responsibilities. *Id.* § 3-3, 3 C.F.R. at 131. For example, the Attorney General is empowered to establish and approve procedures for each agency which will ensure compliance with law and protection of constitutional rights and privacy. *Id.* § 3-305, 3 C.F.R. at 131. To advise and assist the Attorney General in connection with his intelligence-related responsibilities, the Office of Intelligence Policy and Review was established. 45 Fed. Reg. 13729 (1980) (to be codified in 28 C.F.R. § 0.33). This

durable mechanisms to regulate and review intelligence activities has led to the evolution of intelligence law.

II. THE DEVELOPMENT OF INTELLIGENCE LAW

Although both law enforcement and intelligence activities have existed in this country since before the creation of the Republic,[27] they have developed largely along separate tracks because of their conflicting natures. Law enforcement emphasizes openness, stability, and a balancing of interests; its concerns are domestic and its scope is comprehensive. Intelligence activities require secrecy, flexibility, and a single-mindedness of purpose; they focus on foreign developments and rapid adaptability to specific circumstances. Given these disparities, it is no surprise that law enforcement and intelligence activities did not converge in the United States until recently.

The first permanent peacetime intelligence organizations in the United States were created in the latter part of the nineteenth century.[28] These were relatively ineffective, however, and during World War I the nation relied to a great extent on the intelligence capabilities of its allies.[29] It was not until World War II that American intelligence efforts began to flourish under the Office of Strategic Services.[30] Apart from various directives dealing essentially with organizational matters, there was almost no accompanying development of law relating to intelligence activities.[31]

After World War II, a permanent Central Intelligence Agency (CIA) was created by the National Security Act of 1947.[32] This statute was the first public declaration by any nation concerning the existence and functions of its intelligence service. The Act is remarkably concise; in

office is currently staffed by ten attorneys and is under the direction of the Counsel for Intelligence Policy. The Executive Branch oversight apparatus also includes the President's Intelligence Oversight Board (IOB), which is composed of three individuals appointed by the President. Exec. Order No. 12036, § 3-1, 3 C.F.R. at 130. The IOB periodically reviews the oversight procedures and guidelines of each intelligence agency, forwards reports of illegality to the Attorney General, and informs the President of its findings and any serious questions of legality or propriety. *Id.* § 3-102, 3 C.F.R. at 130-31. This comprehensive system of oversight within the Executive Branch is supplemented by extensive review in Congress. *See* note 104 *infra*.

27. There is clear evidence that General Washington authorized and relied upon substantial intelligence activities in the conduct of the American Revolution. For an excellent account of the history and evolution of United States intelligence capabilities, see A. Dulles, The Craft of Intelligence (1963). *See also* H. Ransom, Central Intelligence and National Security (1958); Church Committee Report, *supra* note 9, (Bk. VI) at 9-15.

28. The first permanent intelligence agency was the Office of Intelligence established by the Navy in 1882. Church Committee Report, *supra* note 9, (Bk. VI) at 309. Three years later the Army organized its own intelligence unit, the Military Intelligence Division. *Id.*

29. A. Dulles, *supra* note 27, at 40-41.

30. H. Ransom, The Intelligence Establishment 65-76 (1970).

31. A. Dulles, *supra* note 27, at 42-44.

32. 50 U.S.C. § 403 (1976).

five short subparagraphs it instructs the CIA to collect intelligence information and to perform other related functions at the direction of the National Security Council.[33] The Act's sole express restriction is the proviso that the CIA should not have any police, subpoena, or law enforcement powers or internal security functions.[34] This limitation was as much a concession to established law enforcement agencies as it was an effort to prevent the creation of an American secret police.[35]

With the exception of espionage statutes enacted originally in 1917 and subsequently amended,[36] and administrative housekeeping laws enacted to facilitate the operation of the CIA and the National Security Agency, there were no other laws expressly relating to United States intelligence activities from 1947 until the 1970's.[37] In fact, during this period laws were passed that, if taken literally, would have obstructed or prevented clearly legitimate and necessary intelligence programs.[38] Faced with an absence of particularized law or precedent and an array of general purpose laws inappropriate to intelligence endeavors, the government and its intelligence agencies understandably ignored the broad range of legal strictures that apply in other areas of governmental activity. The deference shown to intelligence matters for almost thirty years by the public, press, Judiciary, Congress, executive officials, various Presidents and Attorneys General considerably strengthened the assumption that intelligence efforts were so different or special that modified legal standards should be applied to them.[39]

---

33. *Id.* § 403(d)(1)-(5).

34. *Id.* § 403(d)(3).

35. Rockefeller Commission Report, *supra* note 9, at 61. S. 2284, *supra* note 25, proposes to replace the National Security Act provisions governing intelligence activities. As Senator Huddleston noted when he introduced S. 2284: "The National Security Act of 1947, the current 'charter' for intelligence activities, is vague and cursory. As Clark Clifford, a primary author of that legislation, told this committee, that act was considered interim legislation that would be replaced once the Executive and Congress better knew what was required. [In S. 2284] we have given the intelligence community authority to do what needs to be done." 126 Cong. Rec. S1305 (daily ed. Feb. 8, 1980).

36. 18 U.S.C. §§ 792-794 (1976).

37. A key aspect of the present structure and functioning of the intelligence community is that of all the organizations engaged in foreign intelligence, only the CIA has been created by legislation. The National Security Agency, the FBI, and the Defense Intelligence Agency have been operating without legislative charters.

38. For example, there are a variety of statutes which, if applied literally, would limit the ability of the FBI to engage in undercover investigative operations for the collection of foreign intelligence or counterintelligence. *E.g.*, 31 U.S.C. § 484 (1976) (restricting the use of proceeds from government operations); *id.* § 521 (restricting the deposit into banks of proceeds from government operations); *id.* § 869 (restricting acquisition or creation of proprietary corporations or business entities). In recent years, Congress has used the Department of Justice Appropriation Authorization Act to provide an annual waiver from these requirements for intelligence operations. *See, e.g.*, Dep't of Justice, Appropriations Act, Fiscal Year 1980, P.L. 96-132, § 7(a), 93 Stat. 1040, 1045-46, *reprinted in* [1979] U.S. Code Cong. & Ad. News.

39. It was not until 1972 that the Supreme Court acknowledged the Executive Branch did not

Over the past few years, however, this perception has changed, and express legal principles have been specifically developed to govern intelligence activities. Although there may continue to be some confusion about how the law applies to a particular matter, there is no longer any doubt that intelligence activities are subject to definable legal standards.

The first comprehensive statement of intelligence law, which delineated various standards, authorizations, and prohibitions designed to govern our intelligence operations, was announced by President Ford on February 18, 1976.[40] After two years of experience with President Ford's order, President Carter issued his own executive order which broadens and strengthens the controls over the intelligence community.[41] For example, this order requires that various procedures be developed, subject to the approval of the Attorney General, to govern the complete range of collection and dissemination practices by all intelligence agencies when the information collected or disseminated pertains to persons entitled to the protection of the United States Constitution.[42] The United States is the only country that has issued such a comprehensive statement.

President Carter also ordered that the government's document classification system be changed.[43] This new executive order officially embraces the principle that even a properly classified document should sometimes be declassified if the public interest in disclosure outweighs the damage to national security that might reasonably be expected from disclosure.[44] The order also creates an administrative mechanism, complete with disciplinary sanctions, designed to eliminate any abuses of the system,[45] such as the unnecessary classification of documents.[46]

---

have full discretion to undertake intelligence operations to protect national security. United States v. United States Dist. Court (Keith), 407 U.S. 297, 316-17 (1972). In fact, the Justice Department declined prosecution of individuals involved in two large-scale mail opening programs operating between 1953 and 1973 because of the ambiguity of the law as it related to intelligence operations during that period. Dep't of Justice, Report Concerning Its Investigations and Prosecutorial Decisions With Respect to Central Intelligence Agency Mail Opening Activities in the United States (1977). Since *Keith,* however, the courts have attempted to define the constitutional limits of intelligence investigations. *See* note 11 *supra.*

40. Exec. Order No. 11905, 3 C.F.R. 90 (1977).

41. Exec. Order No. 12036, 3 C.F.R. 112 (1979). For example, President Carter's order goes well beyond President Ford's order in specifying the preconditions for targeting United States persons for electronic surveillance. *Compare id.* § 2-202, 3 C.F.R. at 126 *with* Exec. Order No. 11905, § 5(b)(2), 3 C.F.R. 90, 100 (1977). President Carter's order also governs, for the first time, television and movie surveillance, Exec. Order No. 12036, § 2-203, 3 C.F.R. at 126, and covert procurement and contracting. *Id.* § 2-303, 3 C.F.R. at 129.

42. Exec. Order No. 12036, § 2-201, 3 C.F.R. 112, 126 (1979).

43. Exec. Order No. 12065, 3 C.F.R. 190 (1979).

44. *Id.* § 3-303, 3 C.F.R. 190, 197 (1979).

45. *Id.* § 5, 3 C.F.R. 190, 201-04 (1979).

46. *Id.* § 1-3 to -6, 3 C.F.R. 190, 193-95 (1979).

Congress has also played an important role in the development of intelligence law. In 1978, Congress enacted the Foreign Intelligence Surveillance Act (FISA),[47] which mandates judicial review of certain proposals from intelligence agencies regarding the conduct of intelligence-related electronic surveillance in the United States.[48] Moreover, the Attorney General retains sole authority to approve agency-certified surveillance applications before they are submitted to the court.[49] This judicial and executive review process helps ensure that only necessary and carefully considered electronic surveillances will be initiated.[50] Governing standards for intelligence operations are also provided by the Case-Zablocki Act, which requires that Congress be advised of any international agreement to which the United States is a party, including agreements between intelligence services.[51] Both the Senate and the House of Representatives have created independent committees with primary responsibility for overseeing the activities of the intelligence agencies.[52] The Freedom of Information Act[53] and the Privacy Act[54] have also had a significant effect on the information collection, dissemination, and storage practices of the intelligence agencies.

For the past three years, Administration and Congressional representatives have endeavored to develop comprehensive charter legislation that would delineate proper and improper intelligence activities.[55] This goal, however, has proved far more elusive than many

47. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified at 50 U.S.C.A. §§ 1801-1811 (West Supp. 1979)).

48. FISA directs the Chief Justice to "publicly designate seven district court judges from seven of the United States judicial circuits who shall constitute a court which shall have jurisdiction to hear applications for and grant orders approving electronic surveillance anywhere within the United States." 50 U.S.C.A. § 1803(a) (West Supp. 1979). The Chief Justice is also directed to designate three judges "who together shall comprise a court of review which shall have jurisdiction to review the denial of any application made under this Act." *Id.* § 1803(b). The Attorney General, rather than the court, is authorized to approve electronic surveillance of certain communications transmitted by means of communications used exclusively between or among foreign powers and of technical intelligence from property under the open and exclusive control of a foreign power. *Id.* § 1802(a)(1)(A)-(B). The Attorney General must advise the court of his actions. *Id.* § 1802(a)(3).

49. *Id.* § 1804.

50. Experience has demonstrated that our intelligence agencies are functioning well under FISA. The record refutes the argument that congressional consideration of such statutes would undermine the entire intelligence apparatus of the United States. *See generally* S. Rep. No. 379, 96th Cong., 1st Sess. (1979).

51. 1 U.S.C. § 112(b) (1976 & Supp. II 1978).

52. The Senate Select Committee on Intelligence was created by S. Res. 400, 94th Cong., 2d Sess., 122 Cong. Rec. 14673-75 (1976). The House Permanent Select Committee on Intelligence was established by H. R. Res. 658, 95th Cong., 1st Sess., 123 Cong. Rec. H7104-06 (daily ed. July 14, 1977).

53. 5 U.S.C. § 552 (1976).

54. *Id.* § 552a.

55. One of the purposes of the Church Committee was to create a record to serve as a foundation for drafting such legislation. Church Committee Report, *supra* note 9.

had anticipated. Intelligence agencies are called upon to operate in societies with vastly different cultures, most of which we do not fully understand, and to provide services in an atmosphere of international political tension and volatility. The effort to reach agreement on a charter that gives the agencies sufficient flexibility to meet changing situations to protect our security, without delegating virtually unlimited discretion, has been herculean.

On February 8, 1980, Senators Huddleston, Mathias, Bayh, and Goldwater introduced the very complex and comprehensive National Intelligence Act of 1980 (S. 2284).[56] With few exceptions, S. 2284 represents a consensus of the Executive Branch and the Senate Select Committee on Intelligence concerning the principles governing United States intelligence activities.[57] S. 2284 carefully balances the practical need for an intelligence apparatus with the guarantees provided by the Constitution and other relevant laws, and, for the first time, legislatively defines and authorizes the activities and conduct of the entire intelligence community. S. 2284 also provides workable standards for the initiation of activities concerning United States persons,[58] by providing a clear hierarchy of responsibility and oversight, and by prohibiting certain activities that are anathema to American democracy.[59] Regardless of whether S. 2284 becomes law, however, its formulation and consideration by the Senate has had the positive effect of focusing attention on the policy choices required to be made in conducting our intelligence activities and on the structural tools available for implementing those choices. As long as we continue to examine objectively the legal guidelines for our intelligence operations, I am confident we will neither abandon our progress nor retreat from what we have gained.

III. ILLUSTRATIVE CONSTITUTIONAL PROBLEMS IN INTELLIGENCE GATHERING

The basic tension in intelligence-gathering activities exists between the government's legitimate need for information and the individual's right to privacy.[60] Although federal law protects United States per-

56. S. 2284, *supra* note 25.

57. President Carter stated there was "virtually complete agreement [between the Executive Branch and the Senate Select Committee on Intelligence] on the organization of the intelligence community and on the authorizations and restrictions pertaining to intelligence collection and special activities." 126 Cong. Rec. S1307 (daily ed. Feb. 8, 1980). He continued, however, to state that "a few issues remain to be resolved." *Id.* One of the primary disagreements between the administration and the authors of S. 2284 relates to prior reporting to Congress of covert operations and sensitive collection operations. *See* note 105 *infra*.

58. *See* note 61 *infra*.

59. For example, S. 2284, *supra* note 25, prohibits assassination, *id* § 131, covert domestic propaganda, *id.* § 133; covert contracting with educational institutions, *id.* § 134, and accomplishing indirectly what cannot be done directly, *id.* § 135.

60. Fortunately for all Americans, the vast preponderance of the information our government

sons[61] from excessive or improper intrusions into their private affairs in the name of national security,[62] intelligence activities aimed at collecting information not publicly available[63] inevitably involve some incursion into the privacy of individuals or organizations. The rights which may be affected by intelligence activities directed against non-consenting United States persons arise from the Constitution, particu-

---

seeks comes from foreign persons and organizations, most of them located outside the United States. In *all* cases, the federal government collects the information this country needs without intentionally violating United States law. United States law contains few limitations on the collection of intelligence from foreign sources. *See, e.g.,* 50 U.S.C.A. § 1802(a)(1)(A)(i) (West Supp. 1979) (electronic surveillance directed at communications exclusively between or among foreign powers may be approved by the Attorney General without court order); Exec. Order No. 12036, § 2-208, 3 C.F.R. 112, 128 (1979) (restricting only the collection of nonpublicly available information concerning United States persons).

61. A United States person is defined in Executive Order 12036 as "a citizen of the United States, an alien lawfully admitted for permanent residence, an unincorporated association organized in the United States or substantially composed of United States citizens or aliens admitted for permanent residence, or a corporation incorporated in the United States." Exec. Order No. 12036, § 4-214, 3 C.F.R. 112, 135 (1979). FISA uses a similar definition. 50 U.S.C.A. § 1801(i) (West Supp. 1979). S. 2284, *supra* note 25, however, provides a more limited definition of United States person. *Id.* § 103(21). For example, it excludes corporations incorporated in the United States and unincorporated associations organized in the United States which are "openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments." *Id.* One's status as a United States person is, in general, not determined by one's location. Thus, a United States citizen abroad remains a United States person for intelligence law purposes, while a foreign visitor to this country does not automatically become a United States person upon entry into this country. There are a number of restrictions in the law which protect foreign visitors from unwarranted intelligence activities in this country, but those limitations are significantly different from the ones applicable to United States persons. For example, Executive Order 12036 protects United States persons and foreign visitors alike from unregulated covert electronic or mechanical monitoring, physical searches, mail surveillance in the United States, and from unlawful physical surveillance by the FBI. Exec. Order No. 12036, §§ 2-202 to -206, 3 C.F.R. at 126-27. The protections provided for foreign visitors, however, are far more limited than those mandated for United States persons. *See, e.g., id.* § 2-208, 3 C.F.R. at 128.

62. *See, e.g.,* Exec. Order No. 12036, §§ 2-1 to -3, 3 C.F.R. 112, 125-30 (1979).

63. The collection, retention, and dissemination of publicly available information is not regulated by Executive Order 12036 or by the procedures for the various intelligence agencies which were approved by the Attorney General pursuant to this order. Exec. Order No. 12036, § 2-201, -208, 3 C.F.R. 112, 126, 128 (1979). Consequently, the definition of publicly available information is a threshold consideration to the application of legal standards to intelligence gathering. The procedures for the CIA and the Department of Defense define the term publicly available similarly. The Defense Department's definition provides: " 'Available publicly' means information that has been published or broadcast for general public consumption, is available upon request to a member of the general public, could lawfully be seen or heard by any casual observer, or is made available at a meeting open to the general public." *See* note 14 *supra*. S. 2284, *supra* note 25, fails to define what information is publicly available but provides the following standard for the collection and use of publicly available information: "Publicly available information concerning any United States person may be collected by an entity of the intelligence community when such information is relevant to a lawful function of that entity, and may be retained and disseminated for lawful governmental purposes." *Id.* § 211(c).

larly the first and fourth amendments. Because our government does not exist as an end unto itself, but as a means of preserving certain precious freedoms for each of us, we cannot allow a need to protect the nation to become an excuse to violate the very rights the government was instituted to protect. Nevertheless, we cannot ignore the government's legitimate need for intelligence information which may, at times affect the freedoms guaranteed by the Constitution.

A. *First Amendment Issues*

United States persons may acquire their knowledge of foreign governments in the course of political activities protected by the first amendment, and courts are often required to balance these first amendment rights with the government's need for intelligence information.[64] It is generally recognized that, in certain circumstances, the government can compel a person to disclose information about such protected activities.[65] The courts have adopted an exacting standard to analyze the encroachment that a compelled disclosure imposes on first amendment freedoms. The governmental interest in disclosure must be substantial. Also, courts have required that there be a "relevant correlation"[66] or "substantial relation"[67] between the governmental interest and the specific information to be revealed, and that the direct and indirect burdens on an individual's or group's associational rights be carefully scrutinized.[68] A final factor that weighs in the balance is

---

64. The first amendment freedoms of association and of expression are implicated whenever the government compels an individual to delineate his political affiliations before a legislative committee, *e.g.*, Eastland v. United States Servicemen's Fund, 421 U.S. 491, 509 (1975); Gibson v. Florida Legislative Investigation Comm., 372 U.S. 539, 544-46 (1963); Sweezy v. New Hampshire, 354 U.S. 234, 249-50 (1957), or a grand jury, *e.g.*, Branzburg v. Hayes, 408 U.S. 665, 690-91 (1972); Bursey v. United States, 466 F.2d 1059, 1085-86 (9th Cir. 1972); *In re* Wood, 430 F. Supp. 41, 45-46 (S.D.N.Y. 1977); *In re* Verplank, 329 F. Supp. 433, 437-38 (C.D. Cal. 1971), or to identify his political beliefs as a condition of exercising first amendment rights, *e.g.*, Lamont v. Postmaster Gen., 381 U.S. 301, 305-07 (1965); NAACP v. Alabama, 357 U.S. 449, 462 (1958), or of obtaining government employment, *e.g.*, Shelton v. Tucker, 364 U.S. 479, 487-88 (1960). *See generally* L. Tribe, American Constitutional Law § 12-2, at 581-82 (1978).

65. There are, however, severe limits on the government's right to compel information. For example, it is unconstitutional for a state to compel a private political organization to furnish its membership list to the state where the effect of doing so would be to subject the organization's members to economic reprisal, loss of employment, or physical coercion. *E.g.*, Louisiana *ex rel.* Gremillion v. NAACP, 366 U.S. 293, 295-96 (1961) (upholding temporary injunction restraining enforcement of statute requiring certain not-for-profit organizations to file membership lists); Bates v. City of Little Rock, 361 U.S. 516, 527 (1960) (invalidating occupational license tax statute which required membership list); NAACP v. Alabama, 357 U.S. 449, 466 (1958) (reversing civil contempt judgment against NAACP for refusing to disclose its membership list in violation of foreign corporation registration statute). These foreseeable consequences would dramatically chill the individual's freedom of expression and of private political association.

66. Bates v. City of Little Rock, 361 U.S. 516, 525 (1960).

67. Gibson v. Florida Legislative Investigation Comm., 372 U.S. 539, 546 (1963).

68. Buckley v. Valeo, 424 U.S. 1, 64-68 (1976) (per curiam). Exacting "scrutiny is necessary

the government's ability to pursue its goal in a manner less intrusive on fundamental personal liberties.[69]

Utilizing this balancing standard, courts have held it constitutional for the United States to compel private citizens to disclose their contributions to presidential campaigns,[70] to require private lobbyists for foreign governments to register,[71] and to require citizens acting as

---

even if any deterrent effect on the exercise of First Amendment rights arises, not through direct government action, but indirectly as an unintended but inevitable result of the government's conduct in requiring disclosure." *Id.* at 65 (citing NAACP v. Alabama, 357 U.S. 449, 461 (1958)).

69. Lamont v. Postmaster Gen., 381 U.S. 301, 310 (1965) (Brennan, J., concurring); Shelton v. Tucker, 364 U.S. 479, 488 (1960). This ad hoc balancing test has been criticized for being "so unstructured that it can hardly be described as a rule of law at all." T. Emerson, The System of Freedom of Expression 16 (1970). Nevertheless, the Supreme Court in Buckley v. Valeo, 424 U.S. 1 (1976) (per curiam), used the balancing test and acknowledged that the governmental interest in disclosure must be weighed against not only the damage to the individuals involved but also the injury suffered by the public at large. *Id.* at 64-68. *Buckley,* however, made it more difficult to prove a constitutional abridgement by requiring evidence of such probable harassment resulting from disclosure as was found in NAACP v. Alabama, 357 U.S. 449, 462 (1958). 424 U.S. at 72. According to Chief Justice Burger, this increased evidentiary burden on litigants challenging compelled disclosure marks a departure from the "historic safeguards guaranteed by the First Amendment." *Id.* at 238 (Burger, C.J., concurring in part and dissenting in part).

70. In Buckley v. Valeo, 424 U.S. 1 (1976) (per curiam), the Supreme Court upheld the requirement of the Federal Election Campaign Act of 1971, 2 U.S.C. §§ 431-456 (1976), that political committees record and transmit to the government the names of individuals contributing in excess of ten dollars to political committees or independent candidates. The Court considered the substantial governmental interest in maintaining the integrity of the electoral process to be of such magnitude as to outweigh the possibility of first amendment infringements. 424 U.S. at 66-68. The Court upheld the ten-dollar minimal threshold reporting requirement based upon a finding that it was not irrational. *Id.* at 83. This deference to a complex congressional judgment represents the Court's hesitation to substitute its judgment for that of the legislature. *See* Shelton v. Tucker, 364 U.S. 479, 490 (1960) (Frankfurter, J., dissenting); *cf. id.* at 488 ("legislative abridgment [of first amendment freedoms] must be viewed in the light of less drastic means for achieving the same basic purpose.") (footnote omitted).

In a slightly different context, *Shelton's* least restrictive alternative test has been more stringently applied. In Pollard v. Roberts, 283 F. Supp. 248 (E.D. Ark.), *aff'd per curiam,* 393 U.S. 14 (1968), the district court enjoined a quasi-grand jury investigation which had subpoenaed essentially the contributor list of the Arkansas branch of the National Republican Party. The prosecutor issued the subpoena in the course of his investigation of possible election law violations. The court, relying on the principles of *Shelton,* held that "even if a [s]tate can legitimately compel a limited disclosure of individuals affiliated with a group, it does not follow that the [s]tate can compel a sweeping and indiscriminate identification of all of the members of the group in excess of the [s]tate's legitimate need for information." *Id.* at 257.

71. The reporting requirements of the Foreign Agents Registration Act of 1938, as amended, 22 U.S.C. §§ 601-621 (1976), were upheld against a first amendment challenge in Attorney Gen. v. Irish N. Aid Comm., 346 F. Supp. 1384, 1389-91 (S.D.N.Y.), *cert. denied,* 409 U.S. 1080 (1972). The court found that the disclosure of defendant's activities bore a substantial relation to a legitimate government interest—informing the government and the public as to sources of foreign propaganda—and that the government interest outweighed "any possible infringement of the first amendment rights of the defendant's members or contributors." *Id.* at 1391. The court was careful to emphasize the vital governmental interest in safeguarding our political process from unacknowledged foreign influences and, on the basis of these concerns and the foreseeable complications with United States foreign policy, rejected the first amendment claim. *Id.*

agents of a foreign power to disclose the details of their agency and their activities.[72] The law is less settled, however, when the government obtains information about an individual's activities without his consent, and under circumstances in which that person is not subject to legislative, judicial or administrative compulsion. Judicial opinions indicate that it is not unconstitutional for an undercover agent in a law enforcement investigation to obtain information that a person is willing to disclose, even though that disclosure is induced by some form of deception.[73] Nevertheless, when the information disclosed concerns political activities and is gathered by a law enforcement agency for purposes other than criminal prosecution the practice may be unconstitutional.[74]

72. There are three basic statutes requiring the registration of individuals or organizations that serve as spokesmen or agents for, or receive money from, foreign governments. First, 22 U.S.C. § 612 (1976) provides that anyone who acts as an agent of a foreign principal must file a registration statement with the Attorney General. The registration statement must contain a thorough description of the registrant's business and employees, the agency relationship, and the activities performed for the principal. Second, 18 U.S.C. § 951 (1976) requires that anyone who acts as an agent of a foreign government must notify the Secretary of State. Third, 18 U.S.C. § 2386 (1976) provides that organizations which accept support from foreign governments must register with the Attorney General if they engage in activities designed to forceably control or overthrow the United States government, or if they engage in activities constituting military training. This statute has been successfully challenged under the fifth amendment. *See* Albertson v. Subversive Activities Control Bd., 382 U.S. 70, 77-78 (1965).

73. The use of informers or infiltrators in a criminal investigation does not give rise to any violation of the first or fourth amendments. Handschu v. Special Servs. Div. 349 F. Supp. 766, 769 (S.D.N.Y. 1972). For fourth amendment purposes, a person assumes the risk that any known party to a conversation concerning criminal conduct is an undercover police agent. *E.g.*, Hoffa v. United States, 385 U.S. 293, 300-03 (1966); Lewis v. United States, 385 U.S. 206, 211 (1966). The fourth amendment, however, does restrict the scope of permissible activities of an undercover agent. *See, e.g.*, Gouled v. United States, 255 U.S. 298, 304-06 (1921) (informant overstepped constitutional bounds when he obtained entry into business office of suspect by deception and secretly ransacked office and seized incriminating documents). Infiltration for law-enforcement purposes into a political organization or rally which might dampen the exercise of first amendment rights of the participants has also been upheld. Socialist Workers Party v. Attorney Gen., 419 U.S. 1314, 1319-20 (1974); United States v. McLeod, 385 F.2d 734, 750 (5th Cir. 1967). Nevertheless, because of the inherent danger that first amendment activities may be significantly impaired, undercover investigations in university classes or political organization meetings will be sustained only if there is a substantial government interest to justify the probable impairment of first amendment rights. White v. Davis, 13 Cal. 3d 757, 768-73, 533 P.2d 222, 229-32, 120 Cal. Rptr. 94, 101-04 (1975) (in bank); *see* Socialist Workers Party v. Attorney Gen., 419 U.S. at 1319.

74. *Compare* White v. Davis, 13 Cal. 2d 757, 773, 533 P.2d 222, 232, 120 Cal. Rptr. 94, 104 (1975) (in bank) (reversing demurrer of plaintiff's complaint and finding that police undercover surveillance on university campus, which gathered information that pertained to no illegal activity, was a prima facie violation of first amendment rights) *with* Fifth Ave. Peace Parade Comm. v. Gray, 480 F.2d 326, 332-33 (2d Cir. 1973) (affirming dismissal of complaint and finding police surveillance of a large antiwar demonstration to be a perfectly lawful method of preserving public safety and deterring violence), *cert. denied*, 415 U.S. 948 (1974) *and* Anderson v. Sills, 56 N.J. 210, 229-31, 265 A.2d 678, 688-89 (1970) (reversing injunction of widespread police surveillance program and holding that, absent proof of bad faith or arbitrariness, the Executive Branch should perform "detectional and preventive" functions and gather any information reasonably believed to be necessary without judicial interference). *See generally* Note,

Although these decisions are helpful, they do not specifically address the different considerations that exist when the information is sought by an intelligence agency for intelligence-gathering rather than law-enforcement purposes.[75] If the government can compel agents of foreign powers to register and describe their political activities, is it unconstitutional to place covert domestic agents in those same foreign agent groups to obtain information?[76] Case law indicates there is no absolute answer and that each situation must be carefully considered, balancing both the need of the government and the effect on the individual.[77]

The Executive Branch has tried to provide some guidance in this area. President Carter's Executive Order on United States Intelligence Activities generally prohibits an intelligence agency from covertly placing agents in any organization in the United States unless the organization is acting on behalf of a foreign power and is primarily composed of individuals who are not United States persons,[78] or unless the infiltration is undertaken on behalf of the FBI as part of a lawful bureau investigation.[79] The order also permits agencies to have employees participate in organizations, without disclosure of their intelli-

---

Domestic Intelligence Informants, the First Amendment and the Need for Prior Judicial Review, 26 Buffalo L. Rev. 173 (1976); Note, *Governmental Investigations of the Exercise of First Amendment Rights: Citizens' Rights and Remedies*, 60 Minn. L. Rev. 1257 (1976).

75. *But cf.* United States v. United States Dist. Court (Keith), 407 U.S. 297, 320 (1972) (extending fourth amendment to domestic security electronic surveillances); Zweibon v. Mitchell, 516 F.2d 594, 611-13 (D.C. Cir. 1975) (en banc) (extending fourth amendment to national security electronic surveillance), *cert. denied*, 425 U.S. 944 (1976).

76. There is very little case law in this area because of the difficulty of proving sufficiently specific injuries to overcome the threshold case and controversy standing requirement as articulated in Laird v. Tatum, 408 U.S. 1 (1972). Mere allegations of a subjective chilling impact of government surveillance on first amendment activities is not an adequate basis for justiciability. *Id.* at 12-13. Allegations of disruption, harassment, or bad faith are generally required before one can litigate first amendment rights when intelligence activities are involved. *E.g.*, Berlin Democratic Club v. Rumsfeld, 410 F. Supp. 144, 149-51 (D.D.C. 1976).

77. In Buckley v. Valeo, 424 U.S. 1 (1976) (per curiam), the Court refused to grant a blanket exemption from the federal contributor reporting requirements for all minor parties and independent candidates. *Id.* at 74. Instead, the Court established a case-by-case procedure which allows each such party to prove that disclosure of contributor lists would substantially impair its members' constitutional rights. *Id.* Since *Buckley*, political parties have had varying success in the lower courts. *Compare* Wisconsin Socialist Workers 1976 Campaign Comm. v. McCann, 433 F. Supp. 540, 548-49 (E.D. Wis. 1977) (injunction issued relieving party from complying with Wisconsin Campaign Financing Act) *and* Partido Nuevo Progresista v. Hernandez Colon, 415 F. Supp. 475, 482-83 (D.P.R. 1976) (per curiam) (injunction issued prohibiting the use of government inspectors to enforce Puerto Rico's political contribution and disclosure statute) *with* Oregon Socialist Workers 1974 Campaign Comm. v. Paulus, 432 F. Supp. 1255, 1259-60 (D. Or. 1977) (injunction denied where Oregon Campaign Disclosure Act was found to have minimal impact on first amendment rights of party).

78. *See* note 61 *supra*.

79. Exec. Order No. 12036, § 2-207(a), 3 C.F.R. 112, 127 (1979).

gence affiliation, in certain narrow circumstances under publicly available guidelines approved by the Attorney General.[80] The CIA, for instance, is not required to disclose participation by agency employees in domestic organizations for the purpose of developing individual associations and credentials needed to substantiate a cover employment.[81] Approval of such undisclosed participation must be given by an appropriate CIA senior official, and all such approvals are subject to review by the Attorney General.[82] These procedures go considerably beyond the requirements of any existing statute or judicial decision. They reflect an awareness of the chilling effect that undisclosed government involvement may have on the exercise of first amendment freedoms and privacy. Thus, the procedures attempt to balance the competing interests of the individual and the government by defining categories of permissible participation and by requiring appropriate review in each case.

B. *Fourth Amendment Issues*

Another constitutional provision often at issue in intelligence gathering is the fourth amendment's prohibition against unreasonable searches and seizures.[83] Intelligence techniques involve traditional searches as well as the utilization of new technology that has not yet

---

80. Executive Order 12036 and the procedures adopted pursuant to it have established formal controls over this sensitive form of information gathering. Exec. Order No. 12036, § 2-207, 3 C.F.R. 112, 127 (1979). Guidelines have been approved thus far for the CIA, the Department of Defense, and the FBI. *See* note 14 *supra*. *But see* Wisconsin Socialist Workers 1976 Campaign Comm. v. McCann, 433 F. Supp. 540, 548 (E.D. Wis. 1977) (prior to adoption of Executive Order 12036 and public procedures, the court expressed skepticism that harassment of dissident political groups had been terminated).

81. The CIA guidelines authorize undisclosed participation in organizations in the United States "to develop associations and credentials to be utilized for purposes relating to foreign intelligence as for example by joining an organization to which an employee would ordinarily be expected to belong if his cover employment were his true employment." Such undisclosed participation is also permitted "to obtain training or education relevant to CIA employment . . . to obtain publications of organizations whose membership is open to the general public . . . to maintain or enhance the qualifications of CIA employees, and to make it possible for them to stay abreast of developments in their fields of professional expertise . . . to maintain the cover of CIA personnel, programs and facilities which are not publicly acknowledged as such by the United States Government . . . to utilize individuals on a witting or voluntary basis who are members of an organization within the United States to develop persons of foreign nationality as sources or contacts for purposes related to foreign intelligence . . . to place employees in an organization within the United States to identify and develop persons of foreign nationality as sources or contacts for purposes related to foreign intelligence [and] to protect the degree of CIA interest in a particular foreign intelligence subject matter, but limited to participation in an organization that permits such participation by government employees in their official capacities." *See* note 14 *supra*.

82. Exec. Order No. 12036, § 2-207, 3 C.F.R. 112, 127 (1979).

83. U.S. Const. amend IV.

been considered by the courts. The FISA[84] requires that a court order be obtained for most traditional forms of wiretapping or eavesdropping conducted within the United States.[85] Such a warrant is also required before the government employs most surveillance devices in the United States to gather information under circumstances where there is "a reasonable expectation of privacy and a warrant would be required for law-enforcement purposes."[86] For example, consider the instrument known as a beeper. This device is attached to a vehicle and emits periodic radio signals which enable the person monitoring the device to determine the location of the vehicle. The FISA does not require a court order before a beeper can be used to determine the location of a foreign agent's car unless, under applicable decisions, a court order would be required if the FBI used such a device to locate a bank robber. Thus, while the fourth amendment's applicability to the use of beepers is not yet completely clear, these devices have been involved in numerous criminal cases and there is some judicial precedent to which intelligence agencies can turn for guidance.[87]

---

84. *See* notes 47-50 *supra* and accompanying text.

85. 50 U.S.C.A. §§ 1801-1804 (West Supp. 1979).

86. *Id.* § 1801(f)(1), (4). *See* note 48 *supra*. The drafters of FISA relied on the Supreme Court's decision in Katz v. United States, 389 U.S. 347 (1967), and intended the statute to reflect evolving concepts of the fourth amendment as interpreted by the courts. Thus, the legislative history of FISA manifests Congress' intention to incorporate the *Katz* standard for constitutionally protected privacy interests into the definition of electronic surveillance, which serves to activate the statute's requirements. S. Rep. No. 604, 95th Cong., 1st Sess. 4-18 (1977), *reprinted in* [1978] U.S. Code Cong. & Ad. News 3904, 3905-20.

87. Most circuits have recognized that the use of beepers to trace airplanes or automobiles on public thoroughfares does not implicate the fourth amendment primarily because there is no reasonable expectation of privacy in activities that are readily observable in public. *E.g.*, United States v. Bruneau, 594 F.2d 1190, 1197 (8th Cir.) (airplane), *cert. denied*, 100 S. Ct. 94 (1979); United States v. Curtis, 562 F.2d 1153, 1156 (9th Cir. 1977) (airplane), *cert. denied*, 439 U.S. 910 (1978); United States v. Hufford, 539 F.2d 32, 33-34 (9th Cir.) (automobile), *cert. denied*, 429 U.S. 1002 (1976). *But see* United States v. Holmes, 521 F.2d 859, 864 (5th Cir. 1975) (automobile) (holding use of beeper to track vehicles impinges upon reasonable expectation of privacy), *aff'd en banc by equally divided panel*, 537 F.2d 227 (5th Cir. 1976) (per curiam). Subsequent decisions, however, indicate that the original panel decision in *Holmes* is not the settled law of the Fifth Circuit. United States v. Conroy, 589 F.2d 1258, 1263 & n.5 (5th Cir.), *cert. denied*, 100 S. Ct. 60 (1979); United States v. Cheshire, 569 F.2d 887, 888 (5th Cir.), *cert. denied*, 437 U.S. 907 (1978). The First Circuit has concluded that although the use of a beeper to track an automobile constitutes a search within the meaning of the fourth amendment, the lessened expectation of privacy associated with an automobile justifies the use of a beeper without a warrant. United States v. Moore, 562 F.2d 106, 111-12 (1st Cir. 1977), *cert. denied*, 435 U.S. 926 (1978).

Similarly, the placement of a beeper inside contraband is not a search within the meaning of the fourth amendment because there can be no objectively justifiable expectation that the possession of an illicit item or stolen good will not be traced by government authorities. *E.g.*, United States v. Pringle, 576 F.2d 1114, 1119 (5th Cir. 1978) (beeper placed in contraband mail); United States v. Emery, 541 F.2d 887, 889-90 (1st Cir. 1976) (beeper placed in contraband package); *see* United States v. Dubrofsky, 581 F.2d 208, 211-12 (9th Cir. 1978) (beeper placed in

The rapid development of technology, however, permits intelligence agencies to use surveillance devices that have never had the benefit of judicial review. As each new technique is considered, the Department of Justice must determine whether it is necessary to seek court approval before using the device. The FISA thus poses a problem. The court's jurisdiction under the Act is limited to issuing orders for electronic surveillance as defined in the Act.[88] Yet the definition of electronic surveillance itself requires consideration of judicial interpretations of the fourth amendment, and there may not be any precedent covering a particular new technology. For example, case law indicates that a court order must be obtained before a microphonic surveillance device is used to intercept a private conversation if the communicant has a reasonable expectation of privacy.[89] The cases, however, do not clearly define the limits of such an expectation. Placing such a listening device in a home, office, or other private location requires a warrant.[90] Using a tape recorder to record a conversation that can be heard by an individual lawfully in an adjacent room does not require a warrant.[91] Use of a parabolic microphone, such as those used by television crews to enhance the entertainment value of professional football, may well require a warrant.[92] It is often difficult, therefore, to determine when a particular surveillance technique requires a warrant. For instance,

---

contraband package); United States v. Bishop, 530 F.2d 1156, 1157 (5th Cir.) (beeper inserted in stolen bait money), *cert. denied*, 429 U.S. 848 (1976). The placement of a beeper in a lawfully possessed item, however, is a search within the meaning of the fourth amendment and requires a warrant, particularly when it can trace a person's movement within a home United States v Moore, 562 F.2d 106, 112-13 (1st Cir. 1977) (beeper placed in noncontraband package), *cert denied*, 435 U.S. 926 (1978); United States v. Bailey, 465 F. Supp. 1138, 1141 (E.D. Mich. 1979) (beeper placed in noncontraband package). *But see* United States v. Perez, 526 F.2d 859, 862 (5th Cir.) (beeper placed in television set received in exchange for contraband), *cert denied*, 429 U.S 846 (1976). *See generally* Marks & Batey, *Electronic Tracking Devices. Fourth Amendment Problems and Solutions*, 67 Ky. L.J. 987 (1978-1979); Note, *Tracking Devices and the Fourth Amendment*, 13 U.S.F. L. Rev. 203 (1978); Note, *Tracking Katz: Beepers, Privacy and the Fourth Amendment*, 86 Yale L.J. 1461 (1977).

88. 50 U.S.C.A. § 1801(f) (West Supp. 1979).

89. Katz v. United States, 389 U.S. 347 (1967), is the seminal case prohibiting the warrantless use of electronic surveillance devices when the target has a reasonable expectation of privacy Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U S C §§ 2510-2520 (1976), imposes criminal penalties, *id.* § 2511, and authorizes recovery of civil damages, *id* § 2520, for the warrantless use of bugs or wiretaps in certain circumstances.

90. *See* Berger v. New York, 388 U.S. 41 (1967) (bringing eavesdropping within the purview of the fourth amendment).

91. United States v. Carroll, 337 F. Supp. 1260 (D.D.C. 1971) (using a tape recorder no more sensitive than the human ear, defendant recorded a conversation, which he could hear without assistance or contrivance from his adjacent hotel room)

92. *See* Lopez v. United States, 373 U.S. 427, 465-66 (1963) (Brennan, J., dissenting) (highlighting danger which modern electronic surveillance devices pose to privacy interests and personal security); United States v. Kim, 415 F. Supp 1252, 1255-56 (D Hawaii 1976) (suggesting there might be a technological limit to reasonable government searches) *See generally*

suppose an intelligence agency is able to use a normal, readily available tape recorder to listen to sounds that are discernible, though not intelligible, to the human ear without any physical intrusion, and then subject that recording to audio enhancement to render the sounds intelligible. Is that activity one which would require a warrant if undertaken for law enforcement purposes? The answer is not clear.[93]

Consider a similar issue. No one would suggest that the FBI must obtain a warrant before reading the daily newspaper. The FBI may act on the basis of information contained in the paper without the slightest suggestion that it has undertaken a search. If members of a criminal conspiracy decide to use the classified advertisement section of the paper to communicate their plans, an FBI agent may certainly read that same section and, if clever enough, discover the conspiracy. The situation is undoubtedly the same if the advertisement is published in a foreign language. Suppose, however, the conspirators believe their advertisement is completely indecipherable by outsiders because it is written in a complicated mathematical code generated by a computer that is beyond the state of the art. Assume further that the FBI is able to break that code by using an even more sophisticated computer. Surely most people would agree that the FBI has not undertaken a search within the meaning of the fourth amendment. The answer, however, is uncertain. It is, of course, possible to argue that the conspirators had a reasonable expectation that their communications were secret. Nevertheless, the decision to put those communications in the public domain, even though in cryptic form, may justify the conclusion that their privacy expectation is not one that the courts are prepared to protect from governmental surveillance. This analysis rests, in part, on reported cases which indicate that one who broadcasts a message on a radio, a public communications medium, does not have an expectation of privacy,[94] and in part, on cases which permit police, without a warrant, to take trash from outside a person's home and subject it to chemical analysis to determine whether any drugs have been discarded.[95]

These first and fourth amendment issues, many of which involve

---

Westin, *Science, Privacy, and Freedom: Issues and Proposals for the 1970's* (pts. 1-2), 66 Colum. L. Rev. 1003, 1205 (1966).

93. *See* note 92 *supra*.

94. United States v. Hall, 488 F.2d 193, 198 (9th Cir. 1973) (holding there is no reasonable expectation of privacy in a radio-telephone conversation that could be received by generally available radio-reception equipment); United States v. Hoffa, 436 F.2d 1243, 1247 (7th Cir. 1970) (holding there is no reasonable expectation of privacy in a telephone conversation from a mobile telephone unit that can be received by an ordinary commercial FM radio receiver), *cert. denied*, 400 U.S. 1000 (1971).

95. United States v. Crowell, 586 F.2d 1020, 1024-25 (4th Cir. 1978), *cert. denied*, 440 U.S. 959 (1979).

attempts to apply case law in novel contexts, are typical of those presented to the Department of Justice. The precedents developed and rules promulgated by the Justice Department, however, are often not subject to judicial review or public comment. Thus, the American principle of checks and balances can be eviscerated when it comes to intelligence activities. It is extremely important, therefore, that we institutionalize in the Executive Branch a process for obtaining a multiplicity of views on the fundamental legal issues arising from intelligence activities.[96] For example, in the Justice Department, the Attorney General receives advice on these matters from former CIA employees, members of the American Civil Liberties Union, and the Department's Office of Intelligence Policy and Review. It is likewise important for intelligence agencies to encourage meaningful in-house criticism of their proposals. The ability to argue against his client's project is one of the most difficult, but most important, skills a lawyer must acquire if his practice is to meet minimal standards of social responsibility.[97] This is particularly true in the government. This process of debate, consideration of conflicting opinions, and careful review will help ensure that intelligence decisions are properly and legally made. Although this process may not always result in perfect legal decisions, it will at least guarantee that the legal issues are considered, the appropriate questions asked, and reasonable conclusions reached.

IV. THE FUTURE OF INTELLIGENCE LAW

The evolution of the law applicable to intelligence activities is directly influenced by world conditions. The current emphasis on legal guidelines for intelligence operations is a result of past excesses which were disclosed during a period in our history when a President was forced out of office and an unpopular war was prolonged despite vigorous public dissatisfaction.[98] Current events, however, may provoke a different analysis. Some may now argue that attempts to regulate intelligence activities are futile and self-destructive. Others may seriously question the costs and benefits of regulation in view of the enormity of hostile acts abroad. While such reexamination is necessary and constructive, it should not cause us to lose sight of the past. Watergate did happen. CHAOS and COINTELPRO were actual programs.[99] Those abuses had their beginnings in action which appeared necessary and reasonable to the officials who began them. As the programs grew, however, the justifications expanded and responsibility disappeared.

96. *See* note 26 *supra* and accompanying text.

97. *See* ABA Canons of Professional Ethics No. 5.

98. *See* note 9 *supra* and accompanying text.

99. *See* Church Committee Report, *supra* note 9, (Bk. II).

The proliferation of law governing intelligence activities has not been entirely without cost. It has limited some of the flexibility and ease of action formerly enjoyed by intelligence officials.[100] We have gained, however, much more than we have lost. Intelligence agencies now operate under the most lucid statements of authority, and limitations thereon, ever available. The protection of individual rights and liberties from infringement by intelligence activities is at a high point. At the same time, there are few, if any, cases in which it has proved impossible under the law to collect truly vital intelligence information. Rather, intelligence officials think more carefully and answer more precisely before proposing or authorizing particular activities.

Nevertheless, there is still more work to be done in this area. Existing law provides inadequate protections to the people who serve our nation as intelligence officers. They need, and deserve, better protection against those who would intentionally disclose their secret mission and jeopardize their safety by revealing their identities. Although public comment and criticism of intelligence activities and specific operations is proper, exposing the identities of particular intelligence personnel and thereby placing them in danger serves no legitimate purpose. Our proper concern for individual liberties must be balanced with a concern for the safety of those who serve our nation in difficult times and under dangerous conditions.[101] We must also adopt

100. *See, e.g., Hearings on H.R. 5129 Before the Subcomm. on Government Information and Individual Rights of the House Government Operations Comm.*, 96th Cong., 1st Sess. (1980) (statement of Frank Carlucci, Deputy Director of Central Intelligence, CIA) (reporting detrimental impact of Freedom of Information Act on security and efficiency of intelligence analysis process and on intelligence gathering from foreign intelligence services and sources, and recommending that CIA be relieved from certain of FOIA's provisions).

101. Several proposals have been introduced in Congress to criminalize disclosure of an intelligence agent's or source's identity. *E.g.*, S. 2284, *supra* note 25, tit. VII; Intelligence Reform Act of 1980, S. 2216, 96th Cong., 2d Sess., 126 Cong. Rec. S366, 369-70 (daily ed. Jan. 24, 1980) [hereinafter cited as S. 2216]; S. 191, 96th Cong., 1st Sess., 125 Cong. Rec. S431 (daily ed. Jan. 23, 1979); H.R. 3762, 96th Cong., 1st Sess., 125 Cong. Rec. H2383 (daily ed. Apr. 26, 1979); H.R. 1068, 96th Cong., 1st Sess., 125 Cong. Rec. H187 (daily ed. Jan. 18, 1979).

Another proposal that has received considerable attention is the Intelligence Identities Protection Act, H.R. 5615, 96th Cong., 1st Sess., 125 Cong. Rec. H9324-25, 9331 (daily ed. Oct. 17, 1979). This bill seeks to restrict the disclosure of information identifying any covert intelligence agent, employee, or source by persons who presently have or formerly had authorized access to classified government information concerning covert identities. *Id.* § 501(a). The bill would also prohibit the disclosure of identifying information by any person, regardless of previous government service or access to classified information, who discloses it with an "intent to impair or impede the foreign intelligence activities of the United States." *Id.* § 501(b). The House Permanent Select Committee on Intelligence has held hearings on this proposal.

The Administration supports an alternative proposal which would (a) prohibit the knowing disclosure of identifying information by any person acting with knowledge that the disclosure is based on classified information, and (b) prohibit current and former government employees, who have had access to information concerning covert identities in the course of their employment,

legal procedures to resolve the problem of graymail, where criminal defendants who have had access to classified information escape punishment by threatening to disclose secret information during a criminal trial.[102] Although it is not impossible to prosecute such cases,[103] the court's ability to protect legally irrelevant secret information from unnecessary disclosure must be strengthened.

Further protection for the intelligence community could also be achieved by a change in the Hughes-Ryan Amendment, which requires the timely reporting of covert action to seven congressional committees.[104] This cumbersome procedure disseminates knowledge of intelligence operations to such a large number of persons that the secrecy essential to their success becomes doubtful. A carefully crafted amendment to the statute should require reporting only to the Senate and House intelligence committees.[105] This would give Congress the

---

from making any disclosure concerning the identity of agents or sources to unauthorized persons, even if the particular disclosures were based purely on speculation or publicly available information. *See Hearings on S. 2284 Before the Senate Select Comm. on Intelligence*, 96th Cong., 1st Sess. (1980). This alternative would balance the need to protect the identities of covert agents and sources with the public's right to free and open discussion of intelligence policies and activities.

102. There are several outstanding legislative proposals to resolve the graymail problem and to prevent the disclosure of classified information during a criminal proceeding. *E.g.*, Classified Information Criminal Trial Procedures Act, H.R. 4736, 96th Cong., 1st Sess., 125 Cong. Rec. H5780 (daily ed. July 11, 1979). H.R. 4736 is a complex legislative proposal which, *inter alia*, creates a procedure for securing pretrial rulings to determine whether classified information may be disclosed at pretrial or trial proceedings, and authorizes the government to take interlocutory appeals from adverse district court orders relating to the disclosure of classified information. The proposal also provides for appropriate protective orders to safeguard classified information disclosed to defendants. H.R. 4736 is strongly supported by the Justice Department

103. *See* note 21 *supra*.

104. The Hughes-Ryan Amendment, 22 U.S.C. § 2422(a) (1976), requires that Presidental findings be made with regard to each proposed covert action operation of the CIA, and that notice of these findings be provided "to the appropriate committees of the Congress, including the Committee on Foreign Relations of the United States Senate and the Committee on Foreign Affairs of the United States House of Representatives." *Id.* Currently such reports are also made to the intelligence committees of both houses, the Senate and House appropriations committees, and the Senate Armed Services Committee, under arrangements between the CIA and these committees.

105. S. 2284, *supra* note 25, and S. 2216, *supra* note 101, propose to repeal the Hughes-Ryan Amendment and replace it with a requirement that only the House and Senate intelligence committees be notified of proposed covert operations. S. 2284, however, would require that Congress receive prior notice of all covert operations. S. 2284, *supra* note 25, §§ 103(18), 125. This contrasts with the requirement of the Hughes-Ryan Amendment to report all such operations in "a timely fashion" to appropriate House and Senate committees. 22 U.S.C. § 2422(a) (1976). S. 2284 would also codify requirements that the intelligence agencies furnish any information requested of them by the intelligence committees, and report to these committees information relating to illegal or improper intelligence activities. *Id.* § 142(a).

The prior notice provision of S. 2284 might unduly jeopardize the safety and security of some

information it needs without unduly jeopardizing intelligence projects.

While we pursue legislative solutions to these problems, the process of self-regulation in the Executive Branch must continue. Many of the regulations are publicly available,[106] and as they gain wider review we will all benefit from the analysis and critical comment of others.[107] The need for governmental self-regulation, however, will increase as modern technology grows ever more sophisticated. The state of the art is already so advanced as to bear little relation to traditional fourth amendment analysis, and will continue to outstrip the development of decisional law for the foreseeable future. Although these technological advances will benefit national security by providing increased efficiency of intelligence gathering, they will also increase the responsibility for fashioning proper safeguards in intelligence law. The interpretation of constitutional provisions, statutes, executive orders, and procedures affecting intelligence gathering will evolve in response to changing perceptions and new experiences. While we must guard against the adoption of an overly pliant construction of our self-imposed rules, I am confident that, in the light of experience, we can continue to devise new standards which do not compromise our essential liberties and which support a strong intelligence community equal to its critical mission.

---

covert operations which require the utmost secrecy. When the Hughes-Ryan Amendment was originally enacted, Congress specifically rejected the language of the Senate bill, which clearly required prior reporting of covert operations. *Compare* Conference Report on Foreign Assistance Act of 1974, H.R. Rep. No. 1610, 93rd Cong., 2d Sess. 12, 42-43, *reprinted in* [1974] U.S. Code Cong. & Ad. News 6734, 6744-45, *with* S. Rep. No. 1299, 93rd Cong., 2d Sess. 43, 90-91, *reprinted in* [1974] U.S. Code Cong. & Ad. News 6674, 6707. The language adopted by Congress requires only timely reporting of covert operations. Experience under the Amendment has proven the wisdom of that decision. Although prior notice is, as a general rule, compatible with national interests, there are occasions where prior notice would jeopardize the safety of individuals involved in the activity or impair the effectiveness of an activity that reasonable people would clearly support. In such cases, timely notice comports with the constitutional role of the President to execute the laws and of Congress to inform itself in order to legislate. Prior notice is not essential to the legislative or oversight process, and subsequent timely notice may be critical to the successful execution of a covert operation.

106. *See* note 14 *supra.*

107. The entire corpus of unclassified rules, regulations, and statutes that is emerging as the substantive field of intelligence law needs to be carefully reviewed by the academic community. Such examination and evaluation is critical to the continued evolution of intelligence law.