Order Code RL34421

CRS Report for Congress

Satellite Surveillance: Domestic Issues

March 21, 2008

Richard A. Best Jr.
Specialist in National Defense
Foreign Affairs, Defense, and Trade Division

Jennifer K. Elsea
Legislative Attorney
American Law Division

Prepared for Members and
Committees of Congress

Satellite Surveillance: Domestic Issues

Summary

Reconnaissance satellites, first deployed in the early 1960s to peer into denied regions of the Soviet Union and other secretive enemy states, have from time to time been used by civilian agencies of the federal government to assist with mapping, disaster relief, and environmental concerns. These uses have been coordinated by the Civil Applications Office at the U.S. Geological Survey, a component of the Interior Department. Post 9/11, the Bush Administration has sought to encourage use of satellite-derived data for homeland security and law enforcement purposes, in addition to the civil applications that have been supported for years. In 2007, it moved to transfer responsibility for coordinating civilian use of satellites to the Department of Homeland Security. The transfer occurred, however, apparently without notification of key congressional oversight committees.

Members of Congress and outside groups have raised concerns that using satellites for law enforcement purposes may infringe on the privacy and Fourth Amendment rights of U.S. persons. Other commentators have questioned whether the proposed surveillance will violate the Posse Comitatus Act or other restrictions on military involvement in civilian law enforcement, or would otherwise exceed the statutory mandates of the agencies involved. Such concerns led Congress to preclude any funds in the Consolidated Appropriations Act, 2008 (H.R. 2764, P.L. 110-161), from being used to "commence operations of the National Applications Office ... until the Secretary [of the Department of Homeland Security] certifies that these programs comply with all existing laws, including all applicable privacy and civil liberties standards, and that certification is reviewed by the Government Accountability Office." (Section 525.)

This report provides background on the development of intelligence satellites and identifies the roles various agencies play in their management and use. Issues surrounding the current policy and proposed changes are discussed, including the findings of an Independent Study Group (ISG) with respect to the increased sharing of satellite intelligence data. There follows a discussion of legal considerations, including whether satellite reconnaissance might constitute a "search" within the meaning of the Fourth Amendment; an overview of statutory authorities, as well as restrictions that might apply; and a brief description of executive branch authorities and Department of Defense directives that might apply. The report concludes by suggesting policy issues Congress may consider as it deliberates the potential advantages and pitfalls that may be encountered in expanding the role of satellite intelligence for homeland security purposes.

The report will be updated as new information becomes available.

Contents

Satellite Surveillance: Domestic Issues

Background

The development of satellite reconnaissance systems is one of the major and enduring accomplishments of the U.S. Intelligence Community. Beginning in the Eisenhower Administration, officials in the Department of Defense (DOD) and the Central Intelligence Agency (CIA) developed "remote sensing" devices that would permit the gathering of accurate information on capabilities of potential enemies without entailing the risks of manned overflights or of covert agents. Satellite imagery undergirded U.S. strategic planning for a quarter century and a series of arms control agreements with the Soviet Union. In early years, film canisters were returned to earth and processed at ground stations for further dissemination. In the 1970s it became possible to forward data by electrical transmission directly to collection agencies.

The efforts of intelligence agencies are focused abroad, and satellite passes were optimized to gather information on areas of interest, mostly in Europe and Asia. At the same time, satellites also passed over U.S. territory, and collection on domestic targets could be obtained as a "free good." In addition, it was often necessary to undertake "engineering passes" by which technical specialists could compare imagery with data obtained directly from ground observation. Engineering passes provided detailed aerial photography of domestic sites. Declassified documents published by the National Security Archive indicate that as early as 1968 consideration was being given to provide images captured by intelligence satellites to civilian agencies on issues such as hydrology and oceanography, mapping, and emergency preparedness.[1]

In the mid-1970s, there was extensive concern about past efforts of the CIA and other agencies to monitor U.S. persons, and these concerns extended to reconnaissance satellites. The 1975 Rockefeller Commission (the Commission on CIA Activities Within the United States) reviewed the issues involved in domestic overhead photography and reported that the CIA, then in charge of most satellite efforts, had provided photography for mapping, assessing natural disasters, conducting route surveys for the Alaska pipeline, national forest inventories, determining the extent of snow cover in the Sierras to forecast the extent of runoff, and detecting crop blight in the Plains States. The Commission noted that it was possible that a small percentage of aerial photography was being used for law enforcement and was "outside the scope of proper CIA activity." "The Commission believes, however, that the legislators, when they prohibited the CIA from engaging

---

[1] See National Security Archives, *U.S. Reconnaissance Satellites: Domestic Targets: Documents Describe Use of Satellites in Support of Civil Agencies*, [http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB229/index.htm], September 14, 2007.

in law enforcement activities in the 1947 enactment of the National Security Act, could not have contemplated the systems presently in use."[2]

In response to the Rockefeller Commission's conclusions and other concerns, the Civil Applications Committee (CAC) was established in 1976 to serve as an interface through which the needs of civilian agencies for satellite data could be reviewed and prioritized. The CAC was created by a joint memorandum signed by the Assistant to the President for National Security Affairs, the Director of the Office of Management and Budget, and the Director of Central Intelligence.

With a staff of some 10 officials, the CAC has provided the principal means of communication between civil users of intelligence capabilities and the providers in the Intelligence Community under the chairmanship of the Director of the U.S. Geological Survey, a component of the Interior Department, and there is a secretariat hosted by the Geological Survey.[3]

By July 2001, the CAC had a membership of some 10 departments and independent agencies:

U.S. Department of the Interior
U.S. Department of Agriculture
U.S. Department of Commerce
U.S. Department of Energy
U.S. Department of Transportation
U.S. Environmental Protection Agency
National Emergency Management Agency
National Aeronautics and Space Administration
National Science Foundation
U.S. Army Corps of Engineers

Associate members included the following:

National Imagery and Mapping Agency[4]
National Reconnaissance Office
Central Intelligence Agency (Director of Central Intelligence Environmental and Societal Issues Center)
Department of State

The end of the Cold War saw increased interest in exploiting the Intelligence Community's collection and analytical assets for civilian purposes, especially in

---

[2] U.S., Commission on CIA Activities Within the United States, Report to the President, June 1975, p. 230. The Commissioners added: "It should be noted that the CIA did turn down a request from the Alcohol and Tobacco Unit of the Treasury Department to help locate moonshine stills in the North Carolina mountains using infrared photography, on the ground that such activity was law enforcement in nature." p. 231, n.

[3] Department of the Interior, Fact Sheet, Civil Applications Committee, April 2001.

[4] NIMA was renamed the National Geospatial-Intelligence Agency (NGA) in November 2003 pursuant to the FY2004 Defense Authorization Act (section 921, P.L. 108-136).

regard to environmental issues. Intelligence agencies provided more analytical products to government agencies outside of the national security community. In 1992, as part of Project Medea, a group of civilian scientists were asked to review data collected by intelligence satellites to determine the usefulness of the data to the scientific community. In a number of areas, information gathered by intelligence satellites was deemed especially important — deforestation, indications of global warming, and reductions in rain forests. In response to this effort, President Clinton issued Executive Order 12951,[5] making public some 860,000 satellite images taken from 1960 to 1972. Some of these images were of U.S. territory — clouds off the California coast, the Mojave Desert, the Luquillo experimental forest in Puerto Rico, and permafrost in Alaska.[6]

The use of intelligence resources for domestic purposes was described by then-Director of Cental Intelligence (DCI) John Deutch in a 1996 speech:

> In the United States, the Intelligence Community provides support to the Federal Emergency Management Activity and other civil agencies when there is a natural disaster. Using data from a variety of sources, within hours after a disaster strikes we can assess and report the nature and scope of the damage — conditions of roads, airports and hospitals; and the status of potential secondary threats such as dams and nuclear facilities. Here I would like to make two points:
>
> First, we only provide this support upon request. To image US territory, we must first get permission.
>
> Second, we provide unclassified products generated from classified information. We have a Disaster Response Team that can quickly produce unclassified maps and diagrams that show the damage resulting from an earthquake, fire, flood, hurricane, oil spill, or volcanic eruption.[7]

Current Policies

Although the precise capabilities of intelligence satellites is classified, they are known to have greater resolution than anything available in commercial markets, such as Google Earth, SPOT, or Landsat. Their usefulness would appear to be unquestionable for map-making and related civilian uses. Satellite information has continued to have important civil applications in such disparate areas as the movement of glaciers in Yakutat Bay in Alaska, forest fires in Montana, and near Mount Pinatubo in the Philippines. They are regularly relied on to provide coverage

---

[5] Executive Order 12951, Release of Imagery Acquired by Space-Based National Intelligence Reconnaissance Systems, 60 Fed. Reg 10,789 (February 24, 1995).

[6] See Loch K. Johnson, *Bombs, Bugs, Drugs and Thugs: Intelligence and America's Quest for Security* (New York: New York University Press, 2000), esp. pps. 50-71; William J. Broad, "U.S. Will Deploy its Spy Satellites on Nature Mission," *New York Times*, November 27, 1995.

[7] John Deutch, "The Environment on the Intelligence Agenda," Speech at the World Affairs Council in Los Angeles, California, July 25, 1996.

of environmental events. Information from intelligence satellites supplements other sources of overhead imagery available to government agencies — from NASA satellites, commercial satellites, or from manned aircraft or unmanned aerial vehicles (UAVs).

Generally, satellite-derived intelligence is combined by the National Geospatial-Intelligence Agency (NGA) with information from airborne platforms, commercial imagery, and other information to meet the needs of military commanders and senior policy makers. The NGA employs a wide range of techniques to prepare mapping and elevation data, scene visualization, and situation analysis. Working through the CAC, the NGA has become a routine partner in disaster relief efforts such as those following the 2004 undersea earthquake and tsunami in the Indian Ocean and Hurricane Katrina in 2005, when the NGA provided graphics for "relief efforts that depicted the locations of major airports, police and fire stations, emergency operations centers, hazardous materials, highways and schools."[8] NGA argues that it "has a strong tradition of collaborating with colleagues across government, non-profit academia and industry arenas to exchange ideas, share best practices, display new GEOINT [geospatial intelligence] solutions and technologies and discuss potential tradecraft advances as they relate to GEOINT."[9] Thus, even though commercial data are available for procurement by any government agency, the NGA and other intelligence agencies believe that their experience and expertise will enable them to provide "value-added" information support to agencies responsible for homeland security and law enforcement.

Satellites are also capable of supporting measurement and signature analysis (MASINT), which is an important, but little known, intelligence discipline, involving information derived from the analysis of radar, laser, infrared, and other emanations. MASINT could be useful for domestic applications in some circumstances; in particular, it might provide evidence of the existence and location of weapons of mass destruction (WMD) materials or WMDs themselves prepared or smuggled in by hostile individuals or groups. The capabilities that satellite-derived information might add to homeland security and law enforcement efforts are inevitably classified but could be investigated and assessed by congressional committees.

The comparative advantages of intelligence satellites are that they can be targeted in an emergency (assuming no foreign intelligence requirements take precedence), their products are cost-free to the requesting agency, and their resolution is higher than what is otherwise available. On the other hand, they may not be available for civil use at a particular time — a prolonged international crisis or ongoing combat operations could significantly limit their availability for civilian uses. They do not "belong" to the civilian agency on a permanent basis.

---

[8] Robert B Murrett, "NGA — Then and Now; Celebrating 10 Years of GEOINT," *Pathfinder*, September/October 2007, pp. 4-5.

[9] Murrett, p. 10. GEOINT is defined as an intelligence discipline that has evolved from the integration of imagery, the information derived from the analysis of imagery, and additional information related to a particular geographic location. See U.S., National Geospatial-Intelligence Agency, "National System of Geospatial Intelligence: Geospatial Intelligence (GEOINT) Basic Doctrine, Publication 1-0," September 2006, pp. 7-8.

Furthermore, the extreme resolution of their imagery may be superfluous for the tasks at hand.

It nevertheless remains uncertain exactly how much "value added" satellites would offer for homeland security and law enforcement purposes. Clearly, additional imagery sources could be useful in many situations, and sophisticated techniques for acquiring information about the presence of WMD materials would be highly valuable, albeit in extremely unlikely circumstances. What other uses would be important remain uncertain and cannot be determined on the basis of unclassified, public materials.

The Independent Study Group

The 9/11 attacks led to a general reconsideration of the relationships between law enforcement and intelligence agencies and in 2002, to the establishment of the Department of Homeland Security (DHS), which has both law enforcement and intelligence responsibilities. Concern with threats to homeland security and international terrorism generally led to a perceived need for increased imaging of the United States. In May 2002, the Senate Intelligence Committee recognized "the valuable role that the National Imagery and Mapping Agency (NIMA) [later renamed as the National Geospatial-Intelligence Agency (NGA)] can play in supporting homeland security operations generally and the newly created U.S. Northern Command, specifically." The Committee expressed concern, however, about the process for authorizing imaging the United States:

> ... [T]he Committee is concerned that the checks and balances in place to ensure against improper imaging requests not be circumvented or otherwise diminished. At the same time, the Committee does not want the added scrutiny given to such requests to unnecessarily hinder urgent collection needs that may arise.

The Committee directed the DCI in coordination with NIMA and the National Reconnaissance Office (NRO) [the organization that builds and operates satellites] to provide a report on the processes for using intelligence satellites to image the U.S. and what changes are being proposed or considered. The report was requested to be provided to the Committee by March 1, 2003.[10]

In December 2004, the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458) established the position of Director of National Intelligence (DNI), in part as a replacement for the DCI, to coordinate intelligence activities and their relationship with law enforcement. One of the intelligence capabilities that appeared to have a greater potential contribution to law enforcement and homeland security was the data collected by satellites.

---

[10] U.S., Congress, 107th Congress, 2d session, Senate, Select Committee on Intelligence, *To Authorize Appropriations for Fiscal Year 2003 for Intelligence and Intelligence-Related Activities of the United States Government, the Community Management Account, the Central Intelligence Agency Retirement and Disability System*, S.Rept. 107-149, May 13, 2002, p. 21.

A further review of the potential contribution of satellite surveillance to the civil sector was undertaken in 2005 by an Independent Study Group (ISG) established by the Office of the DNI. Keith Hall, a former director of the NRO, was designated as chairman of the ISG. Nine civilian experts and three from government agencies completed the membership of the ISG, with staff support from the Booz Allen Hamilton consulting firm.

The group reviewed the use of satellite information for scientific and environmental research, including monitoring and recovery from natural disasters and related hazards, and considered the potential for additional missions. The ISG concluded that far better use could be made of satellite-derived data:

> As the nation searches for methods to improve information and intelligence sharing for homeland security, the ISG believes that geospatial information — often, but not exclusively, maps and map products — are a compelling tool for sharing information. While localities and police services may differ in their sophistication with remote sensing data and technology, virtually everyone has familiarity with maps and map products as decision aids. This is an area where both the Intelligence Community and the civil agencies have extensive experience providing information, even information derived from sensitive sources.[11]

The ISG discussed at some length the past inability or unwillingness of law enforcement agencies to make use of information available from intelligence satellites. It argued that the law enforcement community:

> ... has virtually no significant engagement with the IC [Intelligence Community] for the use of [satellite] collection resources. They are viewed by the IC as a major risk to 'sources and methods' during the discovery process inherent in prosecutions and trials. They are also constrained by extremely limited budgets, and they generally focus on criminal activity post event rather than preventing an event. These attributes make them unappealing to the IC as a customer and partner. In cases where important and useful IC information is provided, the highly classified nature of the sources and methods involved are either placed in jeopardy in the discovery process leading up to prosecution, or the prosecution is jeopardized by potential IC decisions to not allow their information to be so used. This conflict of interests and objectives is a classic prescription for dysfunction, and has led the IC and LE [law enforcement] communities to generally treat each other with extreme caution.[12]

The ISG noted the opportunities for the domestic applications of satellite reconnaissance, but argued that not enough was being done to take advantage of them.

> The current system operates in a risk-averse vice risk-management environment where protection of sources and methods and individual civil liberties, while important concerns to be carefully considered and taken into account, are the

---

[11] *Independent Study Group Final Report, Civil Applications Committee (CAC) Blue Ribbon Study* [hereafter cited as *ISG Report*], September 2005, p. 40.

[12] *ISG Report*, p. 27.

> predominant concerns unreasonably operating to limit appropriate support to the defense of homeland.[13]

The ISG suggested that the disinclination to use information from intelligence satellites for law enforcement and homeland security purposes was another instance of the intelligence/law enforcement "wall" that was extensively discussed in the aftermath of 9/11.[14] The protection of intelligence sources and methods (from the discovery process in a judicial proceeding) was an ongoing concern of intelligence agencies, while the desire to ensure that intelligence agencies are not used to gather information on U.S. persons had led to the establishment of the CAC in the 1970s.[15] The result of these deeply felt concerns in practice had meant that officials in all agencies believed they had sound reasons to avoid, or at least minimize, information sharing between intelligence and law enforcement agencies.

The drafters of the ISG sought to establish a venue through which information from intelligence satellites could be shared with DHS and law enforcement agencies. They argued: "The root of the problem is a lack of a clearly articulated comprehensive policy on the use of IC [Intelligence Community] capabilities for domestic needs."[16] Based on a judgment that the CAC had not effectively provided information to law enforcement agencies, the commission suggested that DHS, a member of the Intelligence Community, serve as the intermediary between the Intelligence Community and state, local, and tribal law enforcement agencies serving as the executive agent of what it termed a new Domestic Applications Office (DAO). This recommendation was based on the premise that "DHS was created to help foster better relations between all facets of LE [law enforcement] and the IC [Intelligence Community], as to facilitate the collection and movement of terrorism-related intelligence and information in ways not previously considered pre 9/11."[17]

National Applications Office (NAO)

The Administration apparently accepted the thrust of the recommendations of the ISG. In March 2006, a Memorandum of Understanding between the Interior and Homeland Security Departments was signed assigning responsibilities of the two departments for creating and maintaining geospatial information to support homeland security. In May 2007, the DNI designated DHS as the executive agent and

---

[13] *ISG Report*, p. 10.

[14] See U.S. Congress, 107th Congress, 2d session, Senate Select Committee on Intelligence, House Permanent Select Committee on Intelligence, *Joint Inquiry into Intelligence Activities Before and After the Terrorist Attacks of September 11, 2001*, S.Rept. 107-351; H.Rept. 107-792, December 2002, esp. pp. 363-368; U.S., National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report*, 2004, esp. pp. 78-80. See also CRS Report RL33873, *Sharing Law Enforcement and Intelligence Information: the Congressional Role*.

[15] The abiding nature of these concerns was demonstrated in the September 6, 2007 hearing discussed below.

[16] *ISG Report*, p. 5.

[17] *ISG Report*, p. 10.

functional manager of what was designated as a National Applications Office (NAO). There was, however, no public notice of the establishment of the new office at that time.

According to the Administration fact sheet, Congress agreed with this approach and provided funding for the office to initiate operations in the fall of 2007: "Intelligence and Appropriations oversight committees have been briefed and approved the reprogramming."[18] The reprogramming in question probably involved a transfer of funds from an account under the control of the DNI to the DHS.[19] Funding for the Office of the DNI is not part of Homeland Security appropriations legislation but is provided in intelligence appropriations included in defense appropriations legislation. It is possible that this funding was provided in classified annexes of defense legislation that was not brought to the attention of the House Homeland Security Committee or to the Homeland Security Subcommittee of the Appropriations Committee.

It became clear, however, that these actions had not been approved by the House Committee on Homeland Security, which has oversight jurisdiction over the DHS. The publication of media accounts of the establishment of the NAO in August 2007[20] took Members of the Committee by surprise. At a September 6, 2007, hearing on "Turning Spy Satellites on the Homeland: the Privacy and Civil Liberties Implications of the National Applications Office," Committee Chairman Representative Bennie Thompson complained about the absence of notification:

> There was no briefing, no hearing, no phone calls from anyone on [the DHS] staff to inform any member of this committee of why, how or when satellite imagery would be shared with police and sheriff's offices nationwide.

---

[18] Department of Homeland Security, "Fact Sheet: National Applications Office," August 15, 2007 (hereinafter "DHS Fact Sheet").

[19] The ISG recommended that elements of the new initiative "not come out of DHS resources, rather would be resourced by the DNI." ISG Report, p. 17; another element, a program to ensure future domestic applications are considered in the acquisition of surveillance systems "would be initially funded by the DNI and executed by the [DHS]. Over a period of 10 years the program dollars would be reduced at the DNI level and increased at the execution/Agency level and sustained at the Agency level thereafter." Pp. 22-23. It was envisioned that DHS would be responsible for facilities, administration, and infrastructure for the effort; these functions were probably not associated with the NAO in the FY2008 budget submission submitted early in 2007. In late October 2007, Donald Kerr, the recently confirmed Principal Deputy DNI told a trade symposium that funding mechanisms for multi-agency initiatives are currently under review; one approach would be to budget funds to the ODNI and then have them transferred to individual agencies; another would be to have one agency serve as the executive agent for a program. See Remarks and Q&A by the Principal Deputy Director of National Intelligence Dr. Donald Kerr to the 2007 GEOINT Symposium, Sponsored by the United States Geospatial Intelligence Foundation, San Antonio, Texas, October 23, 2007.

[20] Robert Block, "U.S. to Expand Domestic Use of Spy Satellites," *Wall Street Journal*, August 15, 2007; Joby Warrick, "Domestic Use of Spy Satellites to Widen," *Washington Post*, August 16, 2007; Eric Schmitt, "Liberties Advocate Fear Abuse of Satellite Images," *New York Times*, August 17, 2007.

This concern was shared by the Ranking Member, Representative Peter King.

At the same hearing, witnesses from civil liberties organizations criticized "turning our nation's surveillance capabilities inwards upon our own population," and argued, "If spy satellites are to be deployed domestically, it is vital that the most rigorous checks and balances and oversight mechanisms be put in place."[21] Although they had little criticism of using satellite data for mapping and disaster relief purposes, they expressed deep concern about the possibility of highly sophisticated technical systems being used on a wide scale by law enforcement agencies. Lisa Graves, the Deputy Director of the Center for National Security Studies, argued that

> ... deploying these extraordinary powers against people in the U.S. would fundamentally alter the relationship between the government and the governed. Calling this 'Big brother in the sky' is modest given the array . . . that might be available multi-headed, medusa-like powers to monitor Americans encompassed by this array of arrays.[22]

The witnesses recommended that the committee investigate further and withhold funds until civil liberties issues are resolved.

The principal DHS witness, Charles Allen, the Under Secretary for Intelligence and Analysis and a long-time intelligence official, defended the new office:

> National Technical Means (NTM) — such as overhead imagery from satellites — have been used for decades, lawfully and appropriately, to support a variety of domestic uses by the US government's scientific, law enforcement and security agencies. The NAO, when operational, will facilitate the use of remote sensing capabilities to support a wide variety of customers, many of whom previously have relied on *ad hoc* processes to access these intelligence capabilities. The NAO will provide not only a well-ordered, transparent process for its customers but also will ensure that full protection of civil rights, civil liberties and privacy are applied to the use of these remote sensing capabilities.[23]

---

[21] See Statement of Barry Steinhardt, Director, Technology and Liberty Project, American Civil Liberties Union on the Privacy and Civil Liberties Implications of Domestic Spy Satellites before the House Committee on Homeland Security, September 6, 2007; also, Statement of Lisa Graves, Deputy Director of the Center for National Security Studies, "'Big Brother in the Sky' and other Grave Civil Liberties Concerns about the Administration's Unilateral Action to Deploy Military Satellites to Spy on the Continental United States for Domestic Law Enforcement Purposes," before the Committee on Homeland Security, United States House of Representatives, September 1, 2007.

[22] Lisa Graves, Deputy Director of the Center for National Security Studies, Statement before the Committee on Homeland Security, United States House of Representatives, September 1, 2007.

[23] Assistant Secretary Charles E. Allen, Chief Intelligence Officer, Department of Homeland Security, Statement for the Record before the House of Representatives Committee on Homeland Security, September 6, 2007. Traditionally the term NTM has included various intelligence disciplines, including signals intelligence; however, at this hearing Allen stated offered the following clarification: "Allow me to state categorically, the NAO will have no relationship or interaction with either the FISA [Foreign Intelligence Surveillance Act] or

(continued...)

The leadership of the Homeland Security Committee stated that

> we are gravely concerned by the Department's [DHS'] lack of progress in creating the appropriate legal and operational safeguards necessary for ensuring that military spy satellites do not become the 'Big Brother in the Sky' that some in the privacy and civil liberties community have described. Accordingly, the Committee on Homeland Security, like the House Homeland Security Appropriations Subcommittee, have asked the Department [DHS] to provide a written legal framework for the NAO and the standard operating procedures (SOPs) under which it will operate in order to allow Members an opportunity to review the plans and suggest changes to ensure that the Constitutional rights of all Americans are protected.[24]

Concern was also expressed that the use of satellites to support law enforcement efforts might not be consistent with the Posse Comitatus Act of 1878, which precludes the use of military forces to execute domestic laws.[25] Some observers argue, however, that although the Posse Comitatus statute applies to the uniformed services, they do not apply to DOD agencies providing information to civilian law enforcement agencies.[26]

According to media reports, in late September 2007, DHS delayed opening the NAO in order to provide congressional committees with more detailed information regarding NAO plans with special attention to civil liberties issues.[27] Until the NAO opens, the CAC reportedly will continue to respond to domestic needs.

After several months of consideration, the Administration appears to be ready to submit plans for the NAO to Congress. In testimony to the Intelligence, Information Sharing and Terrorism Risk Assessment of the House Homeland Security Committee on February 26, 2008, Charles Allen stated, "We're in the final process of having the charter [of the NAO] signed by the principals involved, the Secretary of Defense, the Attorney General, the Director of National Intelligence, and the Secretary of the Interior. We believe we have an agreed upon charter that will be very clear to you on permissible and impermissible uses of the National Applications

---

[23] (...continued)
the Terrorist Surveillance Programs." It should be noted, however, that the ISG included "NSA [National Security Agency] worldwide assets" among the intelligence capabilities under discussion. Pp. 8,14.

[24] Letter from Chairman Bennie G. Thompson, Chairman, House Committee on Homeland Security, *et al.* to the Hon. David E. Price, Chair, Subcommittee on Homeland Security, Committee on Appropriations and the Hon. Harold Rogers, Ranking Member, Subcommittee on Homeland Security, Committee on Appropriations, September 26, 2007.

[25] For an overview of the Posse Comitatus Act, see CRS Report 95-964, *The Posse Comitatus Act and Related Matters: the Use of the Military to Execute Civilian Law*.

[26] See *infra* at 19-22.

[27] See Chris Strohm, "Opening of DHS Satellite Office Delayed Amid Criticism," *Government Executive*, October 1, 2007.

Office.... We are very confident that we have privacy and civil rights and civil liberties fully protected."[28]

The future of U.S. satellite programs is uncertain at present. Intelligence and military satellite programs require multi-billion dollar investments, and some observers have argued that many of their functions could be performed by UAVs or by greater reliance on commercial satellites. The ISG notes that enhancement of the current structure for using intelligence satellites to support homeland security and law enforcement would require "major augmentation of resources, people, budget authority and a new charter to capture the new environment in which it would operate."[29] Further, the ISG explicitly recommended that "the domestic users be given a 'seat at the table' to influence policy, R&D and acquisition decisions."[30] Some skeptics suggest that adding requirements for supporting homeland defense and law enforcement may be influenced by a determination to provide a broader justification for satellite programs that are currently under close scrutiny in both the executive branch and in Congress.

Legal Considerations

Members' concerns about the constitutionality of the National Applications Office have been expressed not only in correspondence but are also reflected in statutory law. The Consolidated Appropriations Act, 2008 (P.L. 110-161, Division E, Section 525), signed by the President on December 26, 2007, provides that "None of the funds provided in this Act shall be available to commence operations of the National Applications Office ... until the Secretary certifies that these programs comply with all existing laws, including all applicable privacy and civil liberties standards, and that certification is reviewed by the Government Accountability Office."

Observers see a number of legal issues involved in the use of satellite-derived information for law enforcement purposes, although discussion and analysis are complicated by the classified nature of satellite capabilities and operations and the absence of public information about ways that satellite-derived information could be used by law enforcement agencies. Most frequently, the proposed expansion of the use of satellite intelligence for domestic law enforcement purposes has been called into question on the basis of possible civil liberties implications, including concerns about privacy rights.

Other commentators have also questioned whether the proposed surveillance will violate the Posse Comitatus Act, post-Civil War legislation that restricted the use

---

[28] Testimony of Charles E. Allen, Under Secretary, Intelligence and Analysis, Department of Homeland Security, before Intelligence, Information Sharing and Terrorism Risk Assessment Subcommittee, Homeland Security Committee, House of Representatives, February 26, 2008, Transcript, Federal News Service.

[29] *ISG Report*, p. 25.

[30] *ISG Report*, p. 4.

of military forces for domestic law enforcement. A key consideration in this regard is the nature of the intelligence agencies that would be involved. The CIA is a civilian institution to which some military personnel on active duty are assigned. DHS is also a civilian department with both law enforcement and intelligence responsibilities. The NRO, which develops and operates satellites, and the NGA, which processes and analyzes the data collected, are components of DOD. Although the NRO is currently headed by a civilian, both agencies have sizable numbers of active duty military personnel assigned. Questions about the appropriate or lawful assignment of military personnel to functions that substantively support domestic law enforcement thus have particular relevance to the NGA and NRO.

The following sections describe the state of the law regarding the application of Fourth Amendment analysis to satellite surveillance (not including electronic surveillance of communications[31]), as well as the current statutory framework regarding intelligence collection and military involvement in law enforcement.

Constitutional Rights

The Fourth Amendment provides that

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated; and no Warrants shall issue but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

In general, the amendment prohibits the government from conducting unreasonable searches or seizures of "the people" and their property, in most cases (subject to a number of exceptions) requiring a warrant supported by a particularized description of the object of the search or seizure.[32] The term "search" refers to a governmental infringement of an expectation of privacy that society is prepared to consider reasonable, that is, under circumstances where an individual reasonably expects that the privacy of his or her person, home, papers, or effects are protected from uninvited intrusion.[33] A "seizure" occurs when there is meaningful governmental interference

---

[31] Presumably, the National Applications Office will have no role with respect to communications intelligence gathered by means of NSA satellites. *See* Statement of Assistant Secretary Charles E. Allen, *supra* note 23. If communications intelligence by satellite in some form is involved in the proposed program, legal considerations not addressed here may come into play.

[32] Katz v. United States, 389 U.S. 347, 360 (1967)(Harlan, J., concurring)(stating that warrantless searches and seizures are per se unreasonable and violative of the Fourth Amendment "subject only to a few specifically established and well-delineated exceptions").

[33] *See, e.g.*, United States v. Bond, 529 U.S. 334, 338 (2000).

in a property interest[34] or intentional detention of a person.[35] Searches and seizures can involve intangible as well as tangible things.[36]

Government surveillance where there is no legitimate expectation of privacy does not amount to a "search" within the meaning of the Fourth Amendment and therefore carries no requirement for a warrant, probable cause, or even any semblance of reasonableness. A finding that surveillance does constitute a search leads to an analysis of whether it was conducted reasonably under the circumstances. All such analysis tends to be rather fact-intensive, and factors said to be important to the analysis frequently cut against each other. The circumstances under which satellite surveillance constitutes a search and, if so, whether it is reasonable, may depend on what information is collected from where, and how the collection is accomplished.

Searches and Non-searches Distinguished. Traditionally, government conduct that did not involve a physical trespass of an individual's person, home, papers, or effects did not constitute a "search" within the meaning of the Fourth Amendment. Surveillance that could be accomplished without entering the premises of the targeted individual was held not to implicate the Fourth Amendment at all.[37] The emphasis on the trespass doctrine appeared to change in 1967 with the Supreme Court's decision in *Katz v. United States*, which held that the Fourth Amendment protected the petitioner's conversation intercepted through the use of an electronic device placed on the outside of a public phone booth.[38] The Amendment is now said to cover people rather than places,[39] so that a person might have a legitimate expectation of privacy even in a public place.

However, *Katz* also reinforced the "plain view" doctrine, which holds that a government official who merely observes (or smells, hears, or touches) something from a lawful vantage point does not conduct a "search." As Justice Harlan wrote:

> What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.[40]

---

[34] Maryland v. Macon, 472 U.S. 463 (1985).

[35] Michigan v. Chesternut, 486 U.S. 567 (1988)(police have seized a person if that person reasonably believes she is not free to leave). Arrests inside a private residence generally require a warrant, Payton v. New York, 445 U.S. 573 (1980), while arrests outside the home need only be supported by probable cause, United States v. Watson, 423 U.S. 411 (1976).

[36] Warden v. Hayden, 387 U.S. 294, 304 (1967); Wong Sun v. United States, 371 U.S. 471, 485-486 (1963).

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

[38] 389 U.S. 347 (1967).

[39] *Id*. at 353.

[40] *Id*. at 351-52.

Whether evidence can be considered to be in "plain view" of a lawfully present police officer who requires binoculars (or some other vision-enhancing technology) to view it appears to depend on whether the object is hidden and whether a court believes the equipment used to view it to be in common use, both of which are factors in assessing the legitimacy of a person's expectation to be free from such observation.[41] That a person has taken normal precautions to maintain her privacy, that is, precautions customarily taken by those seeking to exclude others, is also a factor in determining legitimacy of expectation.[42]

Echoes of the trespass doctrine repudiated in *Katz* frequently reverberate throughout decisions regarding whether a given claim to an expectation of privacy is reasonable, for example, by determining whether a law enforcement officer was lawfully positioned to make a particular observation regarding the goings-on in or near a private home.[43] Consequently, persons continue to have a greater expectation of privacy in the home than they have in public places.[44] The curtilage of a private home[45] receives greater protection than privately owned land used for business purposes. Under the "open field" doctrine, Fourth Amendment protection does not extend to activities that take place out of doors in an area beyond the curtilage of a home, despite efforts to maintain privacy and notwithstanding the fact that law enforcement officers had to commit trespass to come within viewing range,[46] unless perhaps particularly sophisticated sensory enhancement technology is utilized.[47]

The Supreme Court has not addressed whether satellite imagery constitutes a search within the meaning of the Fourth Amendment. However, the Court has applied the expectation of privacy test to aerial surveillance to conclude that no search was conducted.[48] In *California v. Ciraolo*,[49] the Supreme Court determined

---

[41] *See* WAYNE R. LAFAVE, I SEARCH AND SEIZURE § 2.2 (4th ed., 2004) (suggesting two factors: "(1) the level of sophistication of the equipment utilized by the police; and (2) the extent to which the incriminating objects or actions were out of the line of normal sight from contiguous areas where passersby or others might be").

[42] *E.g.*, *id.* at 352; United States v. Chadwick, 433 U.S. 1, 11 (1977).

[43] *E.g.* Harris v. United States, 390 U.S. 234 (1968).

[44] *See* Kyllo v. United States, 533 U.S. 27, 31 (2001) ("'At the very core' of the Fourth Amendment 'stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.'" (citing Silverman v. United States, 365 U.S. 505, 511 (1961)); Payton v. New York, 445 U.S. 573, 589-590 (1980).

[45] The curtilage of a dwelling is "the area to which extends the intimate activity associated with the 'sanctity of a man's home and the privacies of life.'" Oliver v. United States, 466 U.S. 170, 180 (1984)(quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

[46] Hester v. United States, 265 U.S. 57 (1924); Oliver v. United States, 466 U.S. 170, 177-80 (1984) (reaffirming *Hester* and "open fields" doctrine in light of *Katz*). The majority differentiated *Katz*, involving the interception of a conversation from a public place, as a search of a *person* rather than an area. 466 U.S. at 176 & n.6.

[47] *See* Dow Chemical Co. v. United States, 476 U.S. 227 (1986) (discussed *infra*).

[48] For commentary comparing aerial surveillance and other technologies with satellite (continued...)

5-4 that the aerial observation from an altitude of 1,000 feet of a fenced-in backyard within the curtilage of a home, conducted without a warrant, did not constitute a search. The defendant was growing marijuana in a small garden plot in his backyard, protected by two fences from observation by casual passers by. That the marijuana could be seen from public navigable airspace without the use of sensory enhancement equipment defeated the defendant's claim to a reasonable expectation of privacy, even in the curtilage of his private home.[50]

On the same day that *Ciraolo* was handed down, the Supreme Court issued its 5-4 opinion in *Dow Chemical Co. v. United States*,[51] which addressed aerial photography of an industrial compound from much greater heights (but still within navigable airspace) by government regulators using a specialized mapping camera. The surveillance here was likewise not a search, although the Court suggested that such surveillance might have been a search had it involved the curtilage of a private home[52] or used less commonly available technology.[53] The Court also suggested that imagery taken from a satellite might not be permissible:

> It may well be, as the Government concedes, that surveillance of private property by using highly sophisticated surveillance equipment not generally available to the public, such as satellite technology, might be constitutionally proscribed absent a warrant.[54]

The Court did not explain whether the use of equipment with capabilities identical to those of the mapping equipment at issue would be less reasonable if such equipment were mounted on a satellite rather than an aircraft. The infrequency of private space travel might be a factor tipping in favor of Fourth Amendment protection, given the Court's emphasis on the reasonableness of government officials' being at a vantage point where any member of the public might plausibly be. However, any emphasis in the aerial surveillance cases as to the observing

---

[48] (...continued)
surveillance for Fourth Amendment purposes, see Patrick Korody, Note: *Satellite Surveillance Within U.S. Borders*, 65 OHIO ST. L.J. 1627 (2004); Ric Simmons, *From Katz to Kyllo: A Blueprint for Adapting the Fourth Amendment to Twenty-First Century Technologies*, 53 HASTINGS L.J. 1303 (2002).

[49] 476 U.S. 207 (1986).

[50] *Id*. at 213-14.

[51] 476 U.S. 227 (1986).

[52] *Id*. at 237 & n.4 (finding it "find it important that this is not an area immediately adjacent to a private home, where privacy expectations are most heightened.") The Court also found it significant that Dow made no effort to guard against aerial surveillance. *Id*.

[53] *Id*. at 238 ("...EPA was not employing some unique sensory device that, for example, could penetrate the walls of buildings and record conversations in Dow's plants, offices, or laboratories, but rather a conventional, albeit precise, commercial camera commonly used in mapmaking.") The dissent objected that the sophisticated and costly equipment utilized permitted the government to discern objects on the ground that a human being in an aircraft overhead could not otherwise observe. *Id*. at 243 & n.4 (Powell, J., dissenting).

[54] *Id*. at 238.

officer's location in "public navigable airspace" should probably be read as a possible objection to the use of aircraft flying *below* navigable airspace, which would be more physically intrusive than ordinary aerial overflights and might well encroach on property interests. By contrast, satellites using passive surveillance technologies are arguably less physically intrusive, possibly making an expectation of privacy from them less reasonable.

The Supreme Court addressed whether an observation made from a low-flying helicopter constituted a search in *Florida v. Riley*,[55] a plurality concluding that it did not. At issue was the use of a police helicopter, hovering at 400 feet (an altitude prohibited for fixed-wing aircraft), to observe, through an opening in a greenhouse roof, marijuana growing inside. The plurality read *Ciraolo* as establishing that so long as there was no breach of the Federal Aviation Agency (FAA) safety regulations, the property owner had no legitimate reason to expect privacy with respect to non-intimate activities undertaken in the curtilage of his home that were plainly visible from above. Five justices would have preferred to consider how often members of the public actually make low-altitude helicopter flights over populated areas in determining whether the claimed expectation of privacy was reasonable. The plurality suggested that surveillance overflights that comply with FAA regulations might nevertheless constitute searches if they were to involve "undue noise, [] wind, dust, or threat of injury" or to reveal "intimate details connected with the use of the home or curtilage."[56]

The Supreme Court has not addressed whether the use of airborne surveillance equipment other than those involving standard photography (recording visible light) would implicate Fourth Amendment concerns. However, *Kyllo v. United States*[57] strongly suggests such concerns would arise, at least if the surveillance targets a private dwelling. In *Kyllo*, a federal agent used infrared thermal imaging equipment to compare the heat emanating from a triplex unit to the heat signatures of other nearby residences. Based in part on the equipment reading indicating that the defendant's home was warmer than the others, the agent obtained a search warrant. Officers searched the home and seized marijuana plants growing inside. The government argued that the Fourth Amendment had no application, because the defendant had made no effort to conceal the heat escaping the walls of his home and therefor had no reasonable expectation that passers-by would not take notice.

The Supreme Court disagreed, 5-4, holding that the use of sense-enhancing technology not in general public use, in order to reveal details about the interior of a private home that could not otherwise be ascertained without entering the home, constitutes a search. The majority placed great emphasis on the fact that the technique was aimed at a private dwelling, yet it is not clear from the decision whether (or why) the use of such technology against a barn or private office should yield a different result. The threshold for determining when surveillance equipment can be said to have achieved usage common enough to upend the legitimacy of a

---

[55] 488 U.S. 445 (1989).

[56] *Id*. at 452 (White, J., plurality opinion).

[57] 533 U.S. 27 (2001).

resident's expectation of privacy was left unresolved. The dissent criticized the usage criterion as "somewhat perverse [as a guarantor of Fourth Amendment protection] because it seems likely that the threat to privacy will grow, rather than recede, as the use of intrusive equipment becomes more readily available."[58] The secrecy shrouding satellite surveillance capabilities may amplify the difference between the average individual's subjective expectation of privacy and the real extent of their risk of observation by the government.

The use of surveillance techniques that are so narrowly focused that they can only reveal unlawful activity or contraband may not constitute a search,[59] at least when it takes place outside of a home and is not aimed at a person. In *United States v. Place*,[60] the Supreme Court concluded that the use of a drug-sniffing dog to indicate the presence of narcotics in closed luggage was not a search because it "does not expose noncontraband items that otherwise would remain hidden from public view...."[61] Thus, satellite surveillance technology that would enable the government to uncover the presence of unlawful activity or contraband, and nothing more, might not constitute a search at all. Under *Kyllo*, however, technology that can reveal the presence of phenomena (like heat) that may form part of a "signature" associated with unlawful activity, but not the activity itself, would nevertheless constitute a search, at least if the signature emanates from a private dwelling.[62] It is also unclear whether artificial means of limiting the information revealed by a sensor so that the operator has no way of identifying non-contraband would, by itself, make the use of such a sensor not a search.

Reasonable Warrantless Searches. If a particular type of satellite surveillance is deemed to be a search within the meaning of the Fourth Amendment, it is permissible only if its conduct is reasonable. The "reasonableness"of a search is generally determined through a balancing test that weighs the degree to which the search intrudes upon an individual's legitimate expectation of privacy and the degree

---

[58] *Id*. at 47 (Stevens, J., dissenting).

[59] *See* Simmons, *supra* note 47, at 1348-56 (positing a special category of "binary search" that would not be a search for Fourth Amendment purposes because it could not reveal innocent activity or non-contraband).

[60] 462 U.S. 696 (1983).

[61] *Id* at 707. The Court need not have resolved the issue, having found the evidence inadmissible as the fruits of an unlawful seizure of the luggage, but the Court has followed the results in other instances. *See, e.g.*, United States v. Jacobsen, 466 U.S. 109, 123 (1984) (chemical test that could reveal only the presence of cocaine in white powder validly in the possession of police did not infringe the defendant's legitimate expectation of privacy because "the interest in 'privately' possessing cocaine [is] illegitimate"); City of Indianapolis v. Edmond, 531 U.S. 32 (2000) (canine sniffs of exteriors of automobiles stopped at random checkpoint set up to search for narcotics did not transform the temporary seizures into searches, although the seizures themselves were improper).

[62] *Compare* United States v. Knotts, 460 U.S. 276 (1983)(surveillance using beeper technology to track location of container on public roads does not constitute a search) *with* United States v. Karo, 468 U.S. 705 (1984)(use of tracking device to detect the presence of contraband within a home constitutes a search).

to which it is necessary for the promotion of legitimate governmental interests.[63] Oftentimes, the reasonableness factor may be determined by the adequacy of the applicable warrant and whether the officer conducting the search complied with its terms; however, warrants are not required in each instance. In particular, warrantless searches may be reasonable if "exigent circumstances" would prevent the timely application for a warrant.[64]

There is also a "special needs" exception for warrantless searches not based on individualized suspicion, particularly when conducted for purposes other than ordinary law enforcement.[65] For example, the government may conduct routine inspections, without warrant or suspicion, of persons and things crossing a U.S. border (or its functional equivalent), and remain within the reasonableness requirement of the Fourth Amendment.[66] Although the Fourth Amendment does not state that its warrant requirement is limited to searches conducted in the context of criminal investigations, what is "reasonable" under those circumstances may differ from what may be deemed "reasonable" in circumstances where fewer liberty interests are arguably at stake. Many courts have found an exception to the warrant requirement for searches conducted primarily for foreign intelligence gathering purposes.[67] Evidence of criminal activity discovered during these types of

---

[63] Delaware v. Prouse, 440 U.S. 648, 654 (1979).

[64] *See, e.g.,* Warden v. Hayden, 387 U.S. 294, 298-99 (1957)(finding warrantless search of a house justified where armed robbery suspect and weapons were believed to be inside because a delay would endanger the lives of officers and citizens).

[65] Klarfeld v. United States, 944 F.2d 583, 586 (9th Cir. 1991); *see* Chandler v. Miller, 520 U.S. 305, 314 (1997)(drug testing of public officials not justified by special need separate from law enforcement); Veronia School District v. Acton, 515 U.S. 646 (1995)(random drug testing of students participating in interscholastic athletics justified to deter drug use); United States v. Ramsey, 431 U.S. 606, 616 (1977)(sustaining suspicionless searches of mail entering the country); Illinois v. Andreas, 463 U.S. 765 (1983)(upholding customs searches of locked containers shipped from abroad).

[66] United States v. Flores-Montano, 541 U.S. 149, 153 (2004)("[S]earches made at the border, pursuant to the longstanding right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border.")(quoting *United States v. Ramsey*, 431 U.S. 606, 616 (1977)).

[67] The Supreme Court held in *United States v. United States District Court*, 407 U.S. 297 (1972) that domestic national security surveillance by wiretapping was subject to the Warrant Clause of the Fourth Amendment, but expressly declared that its holding did not apply to electronic surveillance of foreign powers or their agents. *Id.* at 308. Lower courts have upheld warrantless electronic surveillance for foreign intelligence purposes. *See* United States v. Truong Dinh Hung, 629 F.2d 908, 912-13 (4th Cir. 1980), *cert. denied*, 454 U.S. 1144 (1982)(warrantless wiretap and bug of one suspected of collaborating with a foreign power held reasonable so long as the surveillance was conducted primarily for foreign intelligence reasons); United States v. Butenko, 494 F.2d 593 (3rd Cir.), *cert. denied sub nom.* Ivanov v. United States, 419 U.S. 881 (1974)(warrantless electronic surveillance was lawful if its primary purpose was to gather foreign intelligence information). *But see* Zweibon v. Mitchell, 516 F.2d 594, 613-14 (D.C. Cir. 1975), *cert. denied*, 425 U.S. 944 (1976) (opining in dicta that "absent exigent circumstances, all warrantless electronic

(continued...)

permissible warrantless searches may be used in criminal prosecutions. Warrantless satellite surveillance that falls unambiguously into a special needs exception can be conducted without a warrant subject to a test of its reasonableness, but may require a showing of probable cause in some cases.

Statutory Authorities and Restrictions

Courts frequently look to the statutory basis for government conduct as part of their inquiry into whether the investigation is a search to begin with or whether it was conducted reasonably.[68] Consequently, the following statutory authorities, as well as any statutes Congress may choose to enact with respect to domestic satellite surveillance, may have a bearing on how courts treat the fruits of such surveillance. The following provides an overview of relevant intelligence authorities, in particular those affecting the Department of Defense.[69]

The National Security Act. The primary authority for the NRO lies in the National Security Act of 1947, as amended, which provides that the DNI is responsible for providing timely and objective national intelligence "based upon all sources available to the intelligence community and other appropriate entities."[70] The Secretary of Defense has significant authorities and responsibilities related to the collection of national intelligence, including the management of military intelligence satellites.[71]

The National Security Act expressly provides for the use of intelligence to assist law enforcement officials *abroad*:

> [E]lements of the intelligence community may, upon the request of a United States law enforcement agency, collect information outside the United States about individuals who are not United States persons. Such elements may collect such information notwithstanding that the law enforcement agency intends to use

---

[67] (...continued)
surveillance is unreasonable and therefore unconstitutional"). Subsequent to these cases, Congress passed the Foreign Intelligence Surveillance Act (FISA), P.L. 95-511, Title I, October 25, 1978, 92 Stat. 1796, codified as amended at 50 U.S.C. § 1801 *et seq.*, to provide a means for judicially authorized foreign intelligence surveillance in the United States.

[68] *See, e.g.*, Dow Chemical Co. v. United States, 476 U.S. 227, 233-34 (1986) (discussing whether EPA had statutory search to conduct aerial surveillance of plant), Florida v. Riley, 533 U.S. 27 (2001)(plurality)(lawfulness of overflight for Fourth Amendment purposes dependent on compliance with FAA regulations); *see also* Orin Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801 (2004); Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 FORDHAM L. REV. 747 (2005).

[69] Authorities regarding communications intelligence are not included. The Administration indicated the proposed domestic satellite surveillance program would not encompass FISA surveillance or the so-called Terrorist Surveillance Program. *See supra* note 23.

[70] 50 U.S.C. § 403-1(a).

[71] 50 U.S.C. §§ 403-4a and 403(5); 10 U.S.C. § 441 (establishing National Geospatial-Intelligence Agency).

> the information collected for purposes of a law enforcement investigation or counterintelligence investigation.[72]

DOD intelligence agencies, including the NRO, are subject to certain limitations when providing such assistance. 50 U.S.C. § 403-5a(b) provides that such assistance "may not include the direct participation of a member of the Army, Navy, Air Force, or Marine Corps in an arrest or similar activity" and may not be provided "if the provision of such assistance will adversely affect the military preparedness of the United States." The Secretary of Defense is required to establish regulations governing the provision of assistance to law enforcement agencies by DOD intelligence elements.[73]

The Posse Comitatus Act and Statutory Exceptions. The National Security Act neither authorizes nor prohibits the use of intelligence for law enforcement purposes within the United States, but other statutes apply. Military personnel assigned to defense intelligence entities are subject to the Posse Comitatus Act, which provides that

> Whoever, except in cases and under circumstances expressly authorized by the Constitution or Act of Congress, willfully uses any part of the Army or the Air Force as a posse comitatus or otherwise to execute the laws shall be fined under this title or imprisoned not more than two years, or both.[74]

Questions regarding which activities violate the Posse Comitatus Act arise most often in the context of assistance to civilian police. At least in that context, the courts have held that, absent a recognized exception, the Act is violated (1) when civilian law enforcement officials make "direct active use" of military investigators, (2) when the use of the military "pervades the activities" of the civilian officials, or (3) when the military is used so as to subject citizens to the exercise of military power that is "regulatory, prescriptive, or compulsory in nature."[75] The Act does not apply to the Navy or Marines[76] and does not prohibit activities conducted for a military purpose that incidentally benefit civilian law enforcement bodies.

Inside the United States (as well as abroad), DOD support for law enforcement agencies is authorized in accordance with chapter 18 of title 10, U.S. Code. The legislation contains both explicit grants of authority and restrictions on the use of that authority for DOD assistance to law enforcement agencies — federal, state, and local

---

[72] 50 U.S.C. 403-5a.

[73] 50 U.S.C. 403-5a(c).

[74] 18 U.S.C. § 1385.

[75] According to DOD doctrine, "direct assistance" by military personnel includes searches and seizures as well as the surveillance of individuals. DODD 5525.5 DoD Cooperation with Civilian Law Enforcement Officials, Encl. 4 § E4.1.3, January 15, 1986.

[76] Department of Defense regulations effectively place them under similar constraints, and the limitations on assistance to civilian law enforcement authorities apply to them, 10 U.S.C. § 375.

— particularly in the form of information and equipment.[77] Section 371 specifically authorizes the Secretary of Defense to share information acquired during military operations, and encourages the armed forces to plan their activities with an eye to the production of incidental civilian benefits. Under sections 372 through 374, DOD equipment and facilities, including intelligence collection assets, may be made available to civilian authorities.

DOD personnel are permitted to provide training and expert advice to civilian law enforcement personnel, and may conduct maintenance on equipment it provides. However, DOD personnel are expressly authorized to operate the DOD-provided equipment only in support of certain federal law enforcement operations, which include counter-terrorism operations, renditions of suspected terrorists from a foreign country to the United States to stand trial, and investigations involving violations of certain laws that control imports, exports, immigration, drug trafficking, and terrorism.[78] DOD personnel are authorized to operate equipment for the purpose of, among other things, detection, monitoring, and communication of the movement of air and sea traffic, as well as surface traffic outside of the geographic boundary of the United States and within the United States not to exceed 25 miles of the boundary (if the initial detection occurred outside of the boundary), and "aerial reconnaissance."[79] DOD equipment, facilities, and personnel may also be provided if necessary during emergency situations involving chemical or biological weapons of mass destruction.[80] Permitted forms of assistance in such an event include the operation of equipment to "monitor, contain, disable, or dispose of the weapon involved or elements of the weapon."[81]

The authority granted in sections 371-382 is subject to three general caveats. It may not be used in any way that could undermine the military capability of the United States[82]; the civilian beneficiaries of military aid must pay for the assistance;[83] and the Secretary of Defense must issue regulations to ensure that the authority of sections 371 to 382 does not "include or permit direct participation by a member of the Army, Navy, Air Force, or Marine Corps in a search, seizure, arrest, or other similar activity unless participation in such activity by such member is otherwise authorized by law."[84] For the emergency provision of assistance in cases involving weapons of mass destruction, DOD and DOJ regulations prohibit DOD personnel (including civilians) from making arrests and from directly participating in a search or seizure or the collection of intelligence for law enforcement purposes, *unless* the action is "considered necessary for the immediate protection of human life, and

---

[77] 10 U.S.C. §§ 371-382.

[78] 10 U.S.C. § 374.

[79] 10 U.S.C. §§ 374 and 382.

[80] 10 U.S.C. § 382.

[81] 10 U.S.C. § 382(c).

[82] 10 U.S.C. § 376.

[83] 10 U.S.C. § 377.

[84] 10 U.S.C. § 375.

civilian law enforcement officials are not capable of taking the action" or the action is otherwise authorized by law.[85]

It appears that DOD initially presumed that the statutory term "search" in 10 U.S.C. § 375 was intended to be "coextensive with the same term in the Fourth Amendment," so that military assistance would be prohibited in connection with any law enforcement activities that constitute a "search" within the meaning of the Fourth Amendment.[86] However, DOJ's Office of Legal Counsel disagreed, opining in 1991 that the use of military personnel to conduct aerial infrared monitoring of private property for law enforcement purposes is "aerial reconnaissance"authorized by 10 U.S.C. § 374(b)(2)(B), and is neither inconsistent with 10 U.S.C. § 375 (assistance may not involve military personnel in search, seizure or arrest) nor prohibited by the Posse Comitatus Act.[87] To reach this conclusion, OLC relied on its interpretation of the legislative history of § 375 to find that Congress did not mean the term "search" to include all conduct that would constitute a search under the Fourth Amendment. Rather, OLC found,

> when Congress used the term "search" in section 375, it intended that the term encompass at most only searches involving physical contact with civilians or their property, and perhaps only searches involving physical contact that are likely to result in a direct confrontation between military personnel and civilians.[88]

The legislative history suggested to OLC that Congress had intended to codify certain court decisions interpreting the Posse Comitatus Act to have as its primary aim the prevention of any "direct confrontation between military personnel and civilians."[89]

---

[85] 10 U.S.C. § 382.

[86] Military Use of Infrared Radars Technology to Assist Civilian Law Enforcement Agencies, 15 U.S. Op. Off. Legal Counsel 36 (1991). DOD presented the question to the Justice Department after receiving several requests for assistance from DEA to deploy Forward Looking Infrared Radar (FLIR) to identify illicit narcotics production.

[87] *Id.*

[88] *Id*. at 39-40. OLC found noteworthy that the original version of 10 U.S.C. § 375 prohibited military personnel from participating in "an interdiction of a vessel or aircraft, *a search and seizure*, arrest, or other similar activity." *Id*. at 41 (citing P.L. 97-86, tit. IX, § 905(a)(1), 95 Stat. 1099 1116 (1981)(emphasis added)). OLC reasoned that

> The coupling of "search" and "seizure" through use of the conjunctive "and," and the reference to the two as a single event (i.e., "a search and seizure"), strongly suggests that Congress was referring to searches of persons or objects that had been seized and thus were in the custody of law enforcement officers. Searches of seized persons or objects almost always involve physical contact.

Id. While OLC thought the later amendment of the statute to delete the "and" between "search" and "seizure" was meant to clarify that it prohibited even searches that did not result in a seizure, its conclusion that the kind of search to be prohibited encompassed only those involving physical contact remained unaffected.

[89] *Id*. at 42-46.

> It is evident from the legislative history of [10 U.S.C. §§ 371-375] that Congress intended to codify the distinction — articulated by the district court in United States v. Red Feather[90] — between "indirect passive" assistance and "direct active" involvement in law enforcement activity.

Under this analysis, participation of military personnel in satellite surveillance would not constitute a search or similar activity under 10 U.S.C. § 375 and thus would not violate the Posse Comitatus Act. On the other hand, whether the activity is authorized at all may depend on whether it constitutes "aerial reconnaissance" or another activity authorized under 10 U.S.C. § 374 and whether it is conducted for one of the permissible missions.

The question of the relevance of the Posse Comitatus Act and related statutes is complex and entwined with legislation adopted long before the possibility of satellite reconnaissance was contemplated. Congress has been willing in the past to permit military personnel to provide assistance to law enforcement officers but has reaffirmed the continued importance maintaining the separate roles of civil law enforcement authorities and the armed forces.[91] Ultimately, the issue may depend on a shared understanding by the executive and legislative branches of the appropriateness of the use of satellite-derived information for domestic law enforcement purposes and an agreement on the limitations placed on such uses. Observers suggest that the provisions requiring an assessment of the issue in the 2007 Supplementary Appropriations Act can provide an opportunity to reach a suitable shared appreciation.

Executive Branch Authorities

Proper adherence to government regulations (not inconsistent with valid statutes or the Constitution) may also be a factor in determining whether an investigation was a search and whether it was conducted reasonably.

Executive Order 12333. E.O. 12333[92] augments statutory intelligence authority for the Secretary of Defense as well as relevant offices and agencies within the Department. The functions of the NRO are described in paragraph 1.12(c), referring to "Offices for the collection of specialized intelligence through reconnaissance programs," and include "carrying out consolidated reconnaissance programs for specialized intelligence." Assistance to law enforcement agencies is covered in paragraph 2.6 of E.O. 12333, which authorizes agencies within the Intelligence Community to participate in law enforcement activities to investigate or prevent clandestine intelligence activities, international terrorist activities, or narcotics trafficking activities. The order also permits the intelligence elements to provide specialized equipment, technical knowledge, or assistance of expert

---

[90] United States v. Red Feather, 392 F. Supp. 916 (D.S.D. 1975).

[91] *See* 6 U.S.C. § 466 (expressing the sense of Congress reaffirming the continued importance and applicability of the Posse Comitatus Act in light of domestic security threats).

[92] 46 Fed. Reg. 59,941 (1981).

personnel for use by any department or agency, or, when lives are endangered, to support local law enforcement agencies.

E.O. 12333 requires agencies within the Intelligence Community to use "the least intrusive collection techniques feasible within the United States or directed against United States persons abroad."[93] Monitoring devices may be used only "in accordance with procedures established by the head of the agency concerned and approved by the Attorney General. Such procedures shall protect constitutional and other legal rights and limit use of such information to lawful governmental purposes."[94] The Attorney General is delegated the authority to approve the use, within the United States or against a United States person abroad, of "any technique for which a warrant would be required if undertaken for law enforcement purposes, provided that such techniques shall not be undertaken unless the Attorney General has determined in each case that there is probable cause to believe that the technique is directed against a foreign power or an agent of a foreign power."[95]

DOD Directives. DOD Directives (DODD) establish or describe policy, programs, and organizations; define missions; provide authority; and assign responsibilities. The directive governing DOD Intelligence Activities states that "[a]ll DoD intelligence and CI activities shall be carried out pursuant to the authorities and restrictions of the U.S. Constitution, applicable law, [E.O. 12333, and other DOD policies and procedures]," as well as "Presidential guidance concerning the authorities and responsibilities of the Director of National Intelligence (DNI)."[96] It further notes that "special emphasis shall be given to the protection of the constitutional rights and privacy of U.S. persons."[97]

DODD 5240.1-R governs the intentional collection of foreign intelligence information about a U.S. person, permitting such collection only if the targeted person is "reasonably believed to be an officer or employee, or otherwise acting for or on behalf, of a foreign power; or is reasonably believed to be engaged or about to engage, in international terrorist or international narcotics activities"; or "is reasonably believed to be a prisoner of war; missing in action; or the target, the hostage, or victim of international terrorist organizations."[98]

In general, intelligence collection against U.S. persons requires a reasonable belief that the targeted person poses a threat or has knowledge relevant to a valid intelligence mission of the Department of Defense. Such collection must be carried out using the least intrusive means, which generally means that information should

---

[93] *Id.* para. 2.4.

[94] *Id.*

[95] *Id.* para. 2.5.

[96] DODD 5240.1: DOD Intelligence Activities § 4, August 27, 2007.

[97] *Id.*

[98] DODD 5240.1-R, Procedures Governing the Activities of DoD Intelligence Components that Affect U.S. Persons, § C2.3.3 (December 1982).

be collected from open sources or with the consent of the person concerned.[99] If such collection is not feasible or sufficient, the information is to be collected from cooperating sources or through the use of other lawful investigative techniques, if necessary obtaining a judicial warrant or the approval of the Attorney General. However, unintentionally collected intelligence, or collection not targeting specific persons, is not subject to these restrictions. The directive specifically permits the collection of information from overhead reconnaissance that is not directed at specific U.S. persons.[100]

The Administration has indicated that the NAO activities it envisions will comply fully with E.O. 12333 and other relevant statutes and regulations.[101] Further, the NAO will "rely on existing, longstanding practice and procedures established by the Intelligence Community to ensure the appropriate protection of privacy and civil liberties,"[102] and will be subject to multiple layers of oversight. The above regulations suggest the view that the purpose and focus of satellite intelligence collection activity will play a major role in determining the extent of civil liberties protections that will apply.

Conclusion

In reviewing plans for the NAO, Congress may focus on the following issues:

- How important will be the "value added" by satellite imagery to homeland security and law enforcement?
- What effect would a more extensive use of satellite imagery for domestic purposes have on national security missions?
- Will replacing the CAC which has been in the Geologic Survey of the Interior Department with the NAO in DHS complicate the use of satellite imagery for mapmaking and other civil purposes?
- How to ensure that the NAO operates in accordance with statutes governing the role of intelligence agencies in supporting homeland defense and law enforcement efforts, protecting civil liberties of U.S. persons.
- Are adequate oversight mechanisms in place for appropriations committees, intelligence committees, and homeland security/governmental affairs committees?

---

[99] *Id* § C2.4.

[100] *Id*. § C2.3.12.

[101] *See* DHS Fact Sheet, *supra* note 18.

[102] *Id*.

- How will DHS and the ODNI budget for the NAO; what are funding plans for FY2009 and for follow-on years?

Although mechanisms for using imagery and other data acquired by satellites for some domestic needs have been in existence since the 1970s without controversy, the possibility of using satellites to support law enforcement and homeland security missions has raised serious concerns among Members of Congress and individuals and groups concerned about the possibility of using intelligence resources as a weapon against U.S. persons. The complexities of congressional oversight of agencies with law enforcement and foreign intelligence missions along with widely circulated reports that Congress was not notified of new satellite missions contributed significantly to these concerns. The Administration delayed the establishment of the NAO and has provided an opportunity for further congressional consideration of the issues involved.