BYU Law Review

Volume 2010 | Issue 5 Article 8

11-1-2010

Why Aren't We Using that Intel Stuff? Using Reconnaissance Satellite Imagery in Domestic Disaster Prevention and Response

Carla Crandall

Why Aren't We Using that Intel Stuff? Using Reconnaissance Satellite Imagery in Domestic Disaster Prevention and Response

I. INTRODUCTION

In 2006, U.S. Army Lieutenant General Russel Honoré, the commander responsible for coordinating the U.S. military's Hurricane Katrina response, spoke at an intelligence community symposium about the contribution intelligence information made during Katrina relief efforts.[1] While noting the value of such intelligence, Honoré explained that conflicting views about the legality of its domestic application limited its utility.[2] Specifically, he stated that while some government officials were advising him that satellite intelligence capabilities could not be used within the United States, others were asking: "'Why aren't you using that intel stuff to tell us what's going on down there?'"[3]

By providing disaster planners and responders with a common operational picture,[4] satellite imagery plays an important role in both manmade and natural disaster prevention and response. Former Director of Central Intelligence (DCI) John Deutch explained, for example, that "within hours after a disaster strikes [analysts] can assess and report the nature and scope of the damage—conditions of roads, airports, hospitals, and the status of potential secondary

1. *See* Tim Shorrock, *America Under Surveillance: Granted New Power to Spy Inside the U.S., the Bush Administration May Be Doing More than Eavesdropping on Phone Calls – It Could be Watching Suspects' Every Move*, SALON, Aug. 9, 2007, http://www.salon.com/news/feature/2007/08/09/domestic_surveillance/.

2. *Id.*

3. *Id.* (quoting Lt. Gen. Russel Honoré, Speech at the 2006 GEOINT Symposium (Nov. 14, 2006)).

4. A common operational picture "provides a means by which analysts, policymakers, warfighters, and first responders can rapidly orient to and visualize their environment. It displays the required information in a fashion that supports situational awareness and rapid decision making." THE NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY, THE NATIONAL SYSTEM FOR GEOSPATIAL INTELLIGENCE, GEOSPATIAL INTELLIGENCE (GEOINT) BASIC DOCTRINE PUBLICATION 1-0, 24 (2006) [hereinafter NGA GEOINT BASIC DOCTRINE], http://www.fas.org/irp/agency/nga/doctrine.pdf.

threats such as dams and nuclear facilities."[5] Unfortunately, however, some of the U.S. government's most sophisticated assets and capabilities are being underutilized—due in large part to a lack of clarity and understanding as to how these resources can appropriately be used within the United States.[6] According to one study, "[t]he ultimate effect is missed opportunities to collect, exploit and disseminate domestic information critical to . . . preparing for, responding to, and recovering from" both manmade and natural disasters.[7]

Arguably, these opportunities have been lost due to inadequate transparency—driven by a culture of secrecy—and an unclear legal framework surrounding the domestic use of reconnaissance satellite imagery.[8] Indeed, from the time of its inception, the domestic imagery program has been mired in concern and uncertainty as to its legitimacy and precise parameters. This uneasiness stems largely from the fact that most of the legal constructs that have been established were developed exclusively within the executive branch, leading to doubts as to the sufficiency of programmatic oversight. Perhaps nothing has highlighted these legal inadequacies more than the recent debacle surrounding the National Applications Office (NAO)—an office within the Department of Homeland Security (DHS) that was designed to facilitate wider domestic use of

5. John M. Deutch, Director of Central Intelligence, The Environment on the Intelligence Agenda, Speech at the Los Angeles World Affairs Council (July 25, 1996) (transcript available at http://www.lawac.org/speech/pre%20sept%2004%20speeches/deutch.html).

6. *See* CIVIL APPLICATIONS COMMITTEE (CAC) BLUE RIBBON STUDY, INDEPENDENT STUDY GROUP FINAL REPORT 4–5 (2005) [hereinafter CAC BLUE RIBBON STUDY] ("The current lack of understanding between the users and providers concerning domestic information makes imperative a need for training and education. Domestic users need to know and understand what the [Intelligence Community] can and cannot do in supporting their requirements."); Spencer S. Hsu, *DHS to Cut Police Access to Spy-Satellite Data: Democrat Calls Bush Program 'Ill-Conceived'*, WASH. POST, June 24, 2009, at A8 ("'I have concerns we're not fully utilizing legal and lawfully authorized capabilities of the U.S. government'" quoting Charles Allen, former Undersecretary of the Dep't of Homeland Sec.'s Office of Intelligence and Analysis).

7. CAC BLUE RIBBON STUDY, *supra* note 6, at 5.

8. *See id.* ("The root of the problem is a lack of a clearly articulated comprehensive policy on the use of [Intelligence Community] capabilities for domestic needs."). It is important to note at the outset, however, that the author does *not* contend that reconnaissance satellite imagery is being used in violation of applicable law. Instead, this article suggests that the lack of clarity and transparency surrounding the existing legal framework for domestic imagery limits its use.

reconnaissance satellite capabilities, but which closed before it even opened because of concerns related to civil liberties and the involvement of the Department of Defense (DoD) in civil affairs.[9]

In light of this background, this Comment highlights the critical role reconnaissance satellite imagery can play in disaster planning and response and proposes reforms to address the concerns that currently impede its wider use. Specifically, Part II provides background about the utility of satellite imagery in domestic disaster prevention and response and discusses the comparative advantages of imagery from reconnaissance satellites over that provided by commercial sources. Part III analyzes the development of the current legal framework surrounding the domestic use of reconnaissance satellite assets and argues that a lack of transparency and clear legal guidance contributes to the underutilization of these vital capabilities within the homeland. Part IV explores the recent proposal to create the National Applications Office and discusses the challenges to using satellite imagery that were exposed by that plan. Part V proposes reforms designed to facilitate wider exploitation of reconnaissance satellite imagery for disaster prevention and response. Finally, Part VI concludes.

II. BACKGROUND AND CONTEXT

Imagery collection via satellites has a long pedigree and contributes to the resolution of a wide array of challenges across the globe. Its utility extends from monitoring the proliferation of nuclear weapons[10] to managing refugee camps.[11] This Part focuses on the value of satellite imagery specifically to disaster prevention and response. Beyond explaining satellite imagery's general utility in the disaster context, this Part also highlights the relative advantages of using reconnaissance satellites over those operated by commercial vendors.

9. *See, e.g.*, Hsu, *supra* note 6, at A8; *see also Turning Spy Satellites on the Homeland: The Privacy and Civil Liberties Implications of the National Applications Office: Hearing Before the H. Comm. on Homeland Sec.*, 110th Cong. 35 (2007) [hereinafter *Hearing*] (statement of Hon. Paul C. Broun, Rep. from Georgia) ("I think you have a real Posse Comitatus problem here.").

10. BHUPENDRA JASANI & GOTTHARD STEIN, COMMERCIAL SATELLITE IMAGERY: A TACTIC IN NUCLEAR WEAPON DETERRENCE 6–7 (2002).

11. JOAN JOHNSON-FREESE, SPACE AS A STRATEGIC ASSET 38 (2007).

A. Satellite Imagery in the Disaster Context

Though it is perhaps most recognized for its value after disasters, satellite imagery also plays a significant role in disaster prevention. In fact, it has proven valuable in responding to virtually every type of disaster. For example, analysts can examine imagery for signs of topographic faulting to generate tectonic maps[12] that can aid planners in earthquake zones with land-use decisions. Imagery is also useful in demarcating watersheds and potential flood zones.[13] Indeed, the Federal Emergency Management Agency (FEMA) uses satellite imagery to create flood maps that determine risk premiums for the National Flood Insurance Program.[14] Infrared imaging satellite systems can also be used to assess potential volcanic activity,[15] thereby allowing officials to evacuate vulnerable citizens prior to an impending eruption. Finally, satellite imagery has also been used to prevent manmade disasters, such as those created by terrorist attacks. The National Geospatial-Intelligence Agency (NGA), for instance, is charged with analyzing satellite imagery in support of national security objectives, including the prevention of terrorist attacks.[16] NGA accomplishes this mission by, among other things, analyzing imagery to provide officials with information about "vulnerabilities to [the country's] critical infrastructure and national assets" that "can be the basis for planning and responding to threats or natural disasters."[17] Current customers of NGA's domestic products include not only federal agencies such as FEMA and the

12. *See*, *e.g.*, Sergio R. Galli de Paratesi, *Hazards and Disasters: Concepts and Challenges*, *in* REMOTE SENSING FOR HAZARD MONITORING AND DISASTER ASSESSMENT: MARINE AND COASTAL APPLICATIONS IN THE MEDITERRANEAN REGION 1, 14–15 (Eric Charles Barrett et al. eds., 1991).

13. *See, e.g.*, *id.* at 15.

14. Press Release, FEMA, New Flood Maps Provide a Snapshot of Current Risks (Nov. 15, 2002), http://www.fema.gov/news/newsrelease.fema?id=3754.

15. *See*, *e.g.*, David K. Chester, *Overview: Hazard and Risk*, *in* APPLIED GEOMORPHOLOGY: THEORY AND PRACTICE, 251, 258 T.3 (R. J. Allison ed., 2002).

16. *See* Nat'l Geospatial-Intelligence Agency, https://www1.nga.mil/About/Pages/default.aspx (last modified Feb. 20, 2009). NGA is a member of both the DoD and the Intelligence Community. *Id.*

17. BERTRAM R. BEAULIEU, THE NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY, THE NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY'S ROLE IN HOMELAND DEFENSE AND SECURITY 2 (2004), http://www.gisdevelopment.net/proceedings/gita/2004/papers/024.pdf.

United States Geological Survey (USGS), but also the National Guard and local government officials.[18]

As important as satellite imagery is to disaster prevention, its utility during disaster relief efforts is immeasurable. After a catastrophic disaster, one of the most challenging problems facing responders is that the damage is often so overwhelming that it is difficult to know where to begin recovery operations.[19] Satellite imagery can help combat this problem by providing damage assessments that guide first responders to areas where their efforts will be most fruitful. After an earthquake, for instance, imagery analysts can direct search and rescue teams not only to areas with the highest concentration of collapsed buildings, but also to those with the highest number of potential survivors. More specifically, imagery interpreters can provide information to rescuers as to which collapsed structures were previously multistory,[20] and thus would be more likely to have voids necessary for survival after a collapse. Moreover, in response to wildfires, analysts can identify hot spots using infrared imaging satellites so that firefighters can appropriately direct their suppression efforts.[21] During floods and tsunamis, satellite imagery can be used to assess damage to infrastructure, such as bridges and roads, to effectively direct the movement of aid into a disaster area.[22] Finally, in response to manmade disasters such as those created by terrorist attacks, satellite imagery can be used to determine the extent of destruction. For instance, after the 2001 World Trade

18. *See* Bert R. Beaulieu, *Security Through the Palanterra*, GEOINTELLIGENCE 14, 14 (July / Aug. 2004), *available at* http://www.nima.mil/NGASiteContent/StaticFiles/OCR/Geo0704.pdf ("Though it may come as a surprise to those who view NGA as strictly an intelligence community and defense combat-support agency . . . NGA has also worked with civil government and private-sector partners to support multiple homeland security missions," including natural disasters.).

19. *See*, *e.g.*, Timothy G. Serban, *Attending to the Dead: Morgues, Body Identification, Accompanying and Blessing the Dead*, *in* DISASTER SPIRITUAL CARE: PRACTICAL CLERGY RESPONSES TO COMMUNITY, REGIONAL AND NATIONAL TRAGEDY 245, 253 (Stephen B. Roberts & Willard W. C. Ashley, Sr. eds., 2008).

20. *See generally* Keiko Saito et al., *Using High-Resolution Satellite Images for Post-Earthquake Building Damage Assessment: A Study Following the 26 January 2001 Gujarat Earthquake*, EARTHQUAKE SPECTRA 145, 155–56 (2004).

21. *See*, *e.g.*, Eric S. Kasischke & Nancy H. F. French, *Locating and Estimating the Areal Extent of Wildfires in Alaskan Boreal Forests Using Multiple-Season AVHRR NDVI Composite Data*, 51 REMOTE SENSING ENV'T 263 (1995).

22. *See*, *e.g.*, Ahmed Ghobarah et al., *The Impact of the 26 December 2004 Earthquake and Tsunami on Structures and Infrastructure*, 28 ENGINEERING STRUCTURES 312–13 (2006).

Center attacks, NGA used satellite imagery and high-resolution elevation data to create models of the damaged area, providing responders with better situational awareness with which to carry out their missions.[23]

B. The Comparative Advantages of Using U.S. Reconnaissance Assets

Though satellite imagery can thus clearly play a significant role in disaster preparation and response, it does not necessarily follow that U.S. reconnaissance assets should be used for its collection. While historically imagery systems within the United States were government-controlled, privatization efforts that began during the Reagan Administration have since created a multi-billion dollar commercial satellite industry.[24] Today, the average person needs nothing more than an Internet connection to acquire at least some form of satellite imagery. Even NGA—the government agency charged with exploiting imagery from reconnaissance satellites—routinely contracts with commercial imagery providers to acquire their products.[25] This raises the question of why reconnaissance assets should be used at all.

While reconnaissance satellites were developed to monitor activities in foreign areas where the U.S. government could not procure on-ground information, their unique capabilities also offer advantages over commercial satellites in the domestic disaster context. First, though the precise resolution of reconnaissance satellites is classified, it clearly surpasses that available from commercial sources.[26] There is speculation, for example, that the

23. BEAULIEU, *supra* note 17, at 7.

24. *See*, *e.g.*, Michael R. Hoversten, *U.S. National Security and Government Regulation of Commercial Remote Sensing from Outer Space*, 50 A.F. L. REV. 253, 253–54 (2001).

25. *See* Press Release, Nat'l Geospatial-Intelligence Agency, NGA Awards Contracts for Commercial Satellite Synthetic Aperture Radar (COMSAR) Imagery, Data Products, and Direct Downlink Services (Dec. 29, 2009), https://www1.nga.mil/Newsroom/PressReleases/Press%20Releases/nga0912.pdf; Press Release, Nat'l Geospatial-Intelligence Agency, NGA Awards NextView Second Vendor Agreement (Sept. 30, 2004), https://www1.nga.mil/Newsroom/PressReleases/Press%20Releases/NextView20040930.pdf; Press Release, Nat'l Geospatial-Intelligence Agency, NGA Awards ClearView to ORBIMAGE Inc. (Mar. 29, 2004), https://www1.nga.mil/Newsroom/PressReleases/Press%20Releases/03292004.pdf.

26. RICHARD A. BEST, JR. & JENNIFER K. ELSEA, SATELLITE SURVEILLANCE: DOMESTIC ISSUES, CONGRESSIONAL RESEARCH SERVICE REPORT RL34421 (June 27, 2008), at CRS-4; Joby Warrick, *Domestic Use of Spy Satellites to Widen: Law Enforcement Getting New Access to Secret Imagery*, WASH. POST, Aug. 16, 2007, at A1.

current spatial resolution of reconnaissance satellites is less than four inches.[27] By contrast, one of the most sophisticated commercial satellites is only capable of capturing images at a resolution of sixteen inches.[28] Further, due to concerns about security, U.S. government regulations require that commercial vendors downgrade imagery available to the public to a resolution of approximately twenty inches.[29] While these differences in resolution may seem inconsequential, the higher resolution of reconnaissance satellites can be critical, for instance, in identifying collapsed buildings or damaged infrastructure.[30]

Beyond the differences in resolution, another benefit of using reconnaissance imagery for disaster planning and response is that it is cost-free to the requesting organization.[31] Commercial satellite imagery, on the other hand, is very expensive. Costs vary widely depending on the vendor, the resolution and age of the imagery, and the geographic extent of the imaged area. It is not uncommon, however, to see prices in the range of $8,000 per image for current imagery from high-resolution sensors.[32] Because activities related to

27. Kenneth Silber, *Spy Satellites: Still a Few Steps Ahead*, SPACE.COM, Sept. 21, 1999, http://www.space.com/news/gov_imagery_990921.html. "*Spatial resolution* refers to the smallest spatial element sensed by the satellite. The decision about which type of imagery to use will partially be determined by the size of the smallest item that the mapmaker wants to detect." Kass Green, *Selecting and Interpreting High-Resolution Images*, 98 J. FORESTRY 37 (2000).

28. *See* Andrea Shalal-Esa, *GeoEye Launches High-Resolution Satellite*, REUTERS, Sept. 6, 2008, http://www.reuters.com/article/idUSN0633403420080906.

29. *Id.*

30. *See* Saito et al., *supra* note 20, at 145. To be sure, the differences in resolution likely are inconsequential when it comes to providing a *large-scale* overview of a disaster area. High-resolution satellite imagery would not be necessary, for example, for monitoring polar ice cap melting, deforestation, or desertification.

31. *See* BEST & ELSEA, *supra* note 26, at CRS-5. Obviously operating the nation's satellite program is expensive, but once launched for reconnaissance purposes, the cost is sunk and the satellites can thus be used for multiple purposes without many *additional* costs. Highlighting this point, Charles Allen has expressed, for instance, that "'we're not fully utilizing legal and lawfully authorized capabilities of the U.S. government, capabilities for which U.S. taxpayers paid over decades hundreds of billions of dollars.'" Hsu, *supra* note 6, at A8. The most significant additional cost associated with domestic collection would likely be the opportunity cost of diverting analytical resources from overseas intelligence missions to interpretation of domestic satellite imagery—a cost that would be incurred whether analysts were interpreting imagery from commercial or reconnaissance imagery.

32. Erkki Tomppo et al., *Working Paper: Forest Resources Assessment 2000: The Role of Remote Sensing in Global Forest Assessment* 62 (U.N. Food and Agric. Org. [FAO], Forestry Dep't, Working Paper No. 61, 2002). It is worth noting that as with many commodities on the market, as the industry has expanded, costs have gradually declined.

disaster preparation and response are often inadequately funded, this expense can be prohibitive to those charged with such missions.[33] To be sure, there are efforts underway, such as the International Charter on Space and Major Disasters,[34] to combat this problem. But while the Charter's aim is to provide free or low-cost imagery to those affected by disasters, the reality is that its impact is somewhat limited—at least insofar as U.S. contributions are concerned—by the fact that the imagery donated at no-cost by U.S. companies is archived rather than newly acquired.[35] For disaster response, having up-to-date imagery is obviously vital to ascertaining the extent of recent damage.

A third advantage to using reconnaissance rather than commercial imaging systems is that since the United States itself owns the reconnaissance satellites, the government can target areas of special interest during emergencies.[36] While it would be good business sense for commercial vendors to do the same, the fact is that nothing requires them to do so. Moreover, particularly as to preventing manmade disasters, the government may be disinclined, for security reasons, to reveal the information necessary for commercial companies to target specific areas of interest. Admittedly, to the extent that the government could simply buy the right to all satellite imagery collected by a commercial satellite, general licensing agreements between NGA and commercial imagery providers may

33. *See*, *e.g.*, John C. Baker & Ray A. Williamson, *Satellite Imagery Activism: Sharpening the Focus on Tropical Deforestation*, 27 SING. J. TROPICAL GEOGRAPHY 4, 8 (2006) (noting, for instance, that "it is still relatively expensive for most NGOs and interested individuals to acquire timely satellite imagery data of a high spatial . . . resolution").

34. INTERNATIONAL CHARTER SPACE AND MAJOR DISASTERS: CHARTER ON COOPERATION TO ACHIEVE THE COORDINATED USE OF SPACE FACILITIES IN THE EVENT OF NATURAL OR TECHNOLOGICAL DISASTERS (2000), http://www.disasterscharter.org/web/charter/charter. As its name suggests, this Charter's aim is to provide low or no-cost imagery in response to disasters around the globe, including those within the United States. International disaster response is beyond the scope of this Comment; the point here is simply to highlight that while the Charter may facilitate acquisition of imagery for U.S. responders after a domestic disaster, the efficacy of this process is limited by the fact that U.S. companies are primarily contributing aged imagery.

35. Press Release, U.S. Geological Survey, Commercial Satellite Imagery Companies Partner with the U.S. Geological Survey in Support of International Charter "Space and Major Disasters" (Apr. 12, 2007), http://www.usgs.gov/newsroom/article.asp?ID=1647. Newly acquired imagery will only be available at "a reduced cost." *Id.*

36. BEST & ELSEA, *supra* note 26, at CRS-5. Of course even this capability will be limited by the physical capabilities imposed by both the satellite itself and its orbit.

limit the impact of privatization.[37] Such agreements are expensive, though, and may be seen as a wasted expense considering the availability of reconnaissance assets.

Lastly, it is important to briefly note that using U.S. intelligence assets may provide other benefits that simply are unavailable from private companies. For example, even if the government used commercial rather than reconnaissance satellites, NGA analysts would still be required to *interpret* the imagery. Such analytic capabilities are important because, as one commentator has aptly noted, "unanalyzed collections are practically worthless."[38] Furthermore, given NGA's presence within the Intelligence Community, its analysts would likely be able to acquire information from multiple intelligence disciplines that could be fused to create a more comprehensive picture of potential threats.[39] This integrated capability would simply not be available if intelligence resources were not used, and threats may thus go undiscovered until they are carried out.

III. THE LEGAL FRAMEWORK FOR USING RECONNAISSANCE ASSETS DOMESTICALLY

Because the government has long recognized the advantages discussed previously, U.S. satellite assets have been used for disaster related missions since the 1960s. This Part chronicles the development of the domestic use program since that time, focusing particularly on the legal structures that emerged as the program developed. Most importantly, this Part highlights the fact that a robust legal framework for the domestic use of reconnaissance assets was, in fact, never fashioned. As explained below, the failure to create

37. Shortly after commencement of Operation Enduring Freedom, for example, the National Imagery and Mapping Agency (NIMA, now NGA) contracted with a commercial imagery provider for exclusive access to all high-resolution imagery acquired by the company over Afghanistan. Doing so allowed the DoD to train commercial satellites on low priority targets while using reconnaissance satellites for higher priority targets. This arrangement came at a high cost, however. One report indicates that the contract cost at least $2 million per month. David Corn, *Their Spy in the Sky: US Hires Space Imaging for Satellite Images of Afghanistan*, 273 NATION 6 (2001).

38. Kneilan K. Novak, Ringing the Bell; Sounding the Alarm: A Proposal for the Simultaneous Advancement of Security and Privacy 22–23 (Mar. 2006) (master's thesis, Naval Postgraduate School), http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA445531&Location=U2&doc=GetTRDoc.pdf.

39. *See* NGA GEOINT BASIC DOCTRINE, *supra* note 4, at 10.

a legal regime continues to plague efforts to maximize the contribution of satellite imagery in the disaster context.

A. The Development of the Civil Applications Committee

In 1968, the National Photographic Interpretation Center (NPIC)[40] convened the first interagency committee meeting to facilitate domestic use of reconnaissance satellite imagery.[41] Subsequently, limited domestic collection and analysis commenced, including collection related to Hurricane Camille in 1969, the Santa Barbara oil spill in 1969, and the Los Angeles earthquake in 1971.[42] In 1974, however, the venture became entangled in "allegations that classified U.S. intelligence collections systems were being used to spy on U.S. citizens."[43] As a result of these and other similar allegations, President Gerald Ford established the President's Commission on CIA activities within the United States and charged its members with the task of, among other things, reviewing the domestic use of reconnaissance satellite systems.[44]

Ultimately, the commission found "no impropriety in permitting continued civilian use of [classified overhead] photography."[45] It did,

40. At the time, NPIC was housed within the Central Intelligence Agency (CIA). In 1996, the National Imagery and Mapping Agency (NIMA) Act transferred the CIA's missions and functions related to reconnaissance satellite imagery—including those pertaining to the CAC—to NIMA. NIMA was subsequently renamed the National Geospatial-Intelligence Agency. *See* MICHAEL A. TURNER, WHY SECRET INTELLIGENCE FAILS 31 (2005); Press Release, U.S. Dep't of Defense, National Imagery and Mapping Agency Established (Oct. 1, 1996), http://www.defense.gov/releases/release.aspx?releaseid=1055. (While public documents from 1996 do not appear to mention NIMA's role related to the CAC, subsequent disclosures make clear that NIMA in fact assumed the CIA's role. *See generally* CIVIL APPLICATIONS COMMITTEE (2001) [hereinafter CAC FACT SHEET], http://www.fas.org/irp/eprint/cac-fs.pdf.)

41. Nat'l Photographic Interpretation Center, memorandum for the record (June16, 1968), http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB229/05.pdf. The committee included representatives from the Departments of Agriculture, Commerce, Transportation, and Interior, as well as members from the Office of Emergency Preparedness (OEP), National Aeronautics and Space Administration (NASA), the Defense Intelligence Agency (DIA), and NPIC. *Id*. *See also* JEFFERY T. RICHELSON, U.S. RECONNAISSANCE SATELLITES: DOMESTIC TARGETS, NAT'L SEC. ARCHIVE ELECTRONIC BRIEFING BOOK (2008), http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB229/index.htm.

42. *See* Nat'l Photographic Interpretation Center, memorandum for the record (May 8, 1973), http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB229/12.pdf.

43. CAC BLUE RIBBON STUDY, *supra* note 6, at 6.

44. *See*, *e.g.*, *id*.

45. Memorandum from Henry A. Kissinger, Assistant to the President for National Security Affairs, to the U.S. Secretary of Defense, the U.S. Secretary of Interior, the U.S.

however, recommend the creation of an independent "interagency committee of Federal civil agencies to facilitate appropriate use of [satellite] technology and allay concerns about the potential for improper use of intelligence assets for domestic purposes."[46] Accordingly, in 1975, the Assistant to the President for National Security Affairs, the Director of the Office of Management and Budget (OMB), and the Director of Central Intelligence (DCI) signed a joint memorandum creating the Civil Applications Committee (CAC).[47]

From its inception, the CAC's mission was to "act as the interface between civilian agencies and intelligence collectors" and "oversee civilian agency uses of classified photography in a manner designed to avoid any concerns that domestic photographic coverage is being used improperly."[48] The charter called for a representative from the Department of the Interior (DOI) to chair the committee, and expressly mandated membership of the Departments of Agriculture and Commerce, NASA, the U.S. Army Corps of Engineers (USACE), and the Environmental Protection Agency (EPA).[49] The DCI was also required to appoint a representative to serve *ex officio* on the committee in order to act as a liaison to the Intelligence Community.[50]

Though the classified nature of issues surrounding the CAC makes it difficult to determine precisely how domestic collection initially operated, recently declassified documents do provide some insight into the process. One document that is especially significant concerns the authority of the National Reconnaissance Office (NRO)—the agency that builds and operates the country's reconnaissance satellites[51]—to use the systems to collect imagery within the United States. The memo, written in response to a presidential executive order prohibiting domestic collection against

Secretary of Agriculture, the U.S. Secretary of Commerce, the NASA Administrator, the EPA Administrator, and the Army Chief of Engineers (Oct. 3, 1975), http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB229/18.pdf.

46. CAC BLUE RIBBON STUDY, *supra* note 6, at 7.

47. *See* BEST & ELSEA, *supra* note 26, at CRS-2; Kissinger, *supra* note 45.

48. Kissinger, *supra* note 45.

49. *Id.*

50. *Id.* The CAC was also vested with authority to expand its membership at its own discretion.

51. *See* Nat'l Reconnaissance Office, http://www.nro.gov/ (last visited Jan. 14, 2011).

U.S. persons,[52] discussed the inadvertent collection of data obtained while the satellites were engaged in otherwise "legitimate" purposes such as disaster relief.[53] Because reconnaissance systems were in fact incidentally collecting data against U.S. persons during disaster relief operations, they technically violated the executive order. Still, the internal NRO memo indicated that the Director of the NRO was nevertheless authorized to continue domestic satellite imaging, so long as it was pursued in accordance with the "spirit and intent" of the order.[54] Ensuing NRO policy directives indicated that reconnaissance imagery of U.S. territory "should be minimized and obtained only in response to formal, documented requirements" of the CAC, and that "data inadvertently obtained on U.S. persons or organizations [should] not be used for any purposes and [should] be destroyed at the earliest practical time."[55]

Notwithstanding these directives, concern understandably persisted regarding the legality of operations pursued via the CAC. In 1978, for example, a senior official within the NRO ordered his staff to conduct a study as to the legitimacy of procedures which, in effect, called for civilian agencies acquiring classified imagery via the CAC to "attest[] to the propriety of their [own] collection requirements."[56] In fact, he noted that top administration officials, including the DCI, the Secretary of Defense, and the Director of the NRO were "potentially in a vulnerable position with respect to this issue," largely because of a lack of oversight within Congress or by senior executive officials.[57] While the results of the study are not entirely clear, the official did note in a subsequent memo to the CIA chief responsible for exploiting domestic imagery that "[i]t

52. *See* Exec. Order 11,905, 3 C.F.R. 90 (1977), *reprinted in* 50 U.S.C. § 401 (1977).

53. The Nat'l Sec. Archive, Authority for the National Reconnaissance Program Domestic Satellite Reconnaissance Activities, http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB229/23.pdf (last visited Jan. 14, 2011).

54. *Id.*

55. Memorandum from Charles W. Cook, NRO Deputy Director, to various NRO program managers, date unknown, http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB229/24.pdf; *see also* NRO memorandum for General Kulpa and Mr. Dirks (May 28, 1976), http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB229/25.pdf. It should also be noted that other limited domestic collection was permitted for satellite engineering and testing purposes. *Id.*

56. Memorandum from William L. Shields, NRO Staff Director, to Col. Frederick L. Hoffman, U.S. Air Force (Jan. 26, 1978), http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB229/28b.pdf.

57. *Id.*

appear[ed] unclear whether a current, authoritative legal approach for such domestic use of national intelligence assets exist[ed]."[58] Though he proposed pursuing programmatic approval from the Attorney General,[59] there is no public record indicating that anyone followed this recommendation.

B. The Operations of the Civil Applications Committee

Despite this unsettled legal framework, CAC operations thrived during the 1980s and 1990s.[60] By 2005, the CAC was holding monthly meetings with members from eleven governmental departments and independent agencies, including the National Science Foundation (NSF) and FEMA.[61] As for its current operational functions, the CAC is today charged with oversight duties "includ[ing] disseminating information to Federal users on policies related to the proper nonintelligence use of the [collected] data and the protection of intelligence sources and materials."[62] The CAC also "ensures that domestic imagery requirements are submitted and processed according to *established policies and procedures.*"[63] While those policies and procedures are evidently contained in classified policy directives,[64] there have been a few public disclosures about the process.

According to NGA directives, for example, requests for the domestic use of reconnaissance satellites "are processed and

58. Memorandum from William L. Shields, NRO Staff Director, to COMIREX chairman (Feb. 15, 1978), http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB229/29.pdf.

59. *Id.*

60. Projects included, for example, floodplain mapping for FEMA, bilge oil discharge monitoring for the U.S. Coast Guard, hazardous waste site characterization for the Department of Energy, and wetlands mapping, wildfire detection, and volcanic activity monitoring for the DOI. *See* GOVERNMENT APPLICATIONS TASK FORCE (GATF), PILOT PROJECT SUMMARY (1996), http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB229/34.pdf; Memorandum of Agreement for Cooperation in Wildland Fire Detection, Volcanic Activity Monitoring, and Volcanic Ash Cloud Tracking Between the Deputy Undersecretary of Defense, Space and the U.S. Geological Survey (Apr. 30, 1997), http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB229/35.pdf.

61. *See* CAC BLUE RIBBON STUDY, *supra* note 6, at 7; CAC FACT SHEET, *supra* note 40, at 2.

62. CAC FACT SHEET, *supra* note 40, at 1.

63. *Id.* (emphasis added).

64. *See* Christopher M. Petras, *"Eyes" on Freedom—A View of the Law Governing Military Use of Satellite Reconnaissance in U.S. Homeland Defense*, 31 J. SPACE L. 81, 95 n.61 (2005) (explaining that NIMA's imagery policy related to domestic imagery collection is classified).

approved under the authority of the DCI."[65] Before such collections commence, NGA requires the requestor to fill out a Proper Use Memorandum (PUM).[66] In testimony before Congress, Daniel W. Sutherland, an officer within DHS's Civil Rights and Civil Liberties Office, explained that a PUM is

> a memorandum between the requesting agency and NGA outlining the parameters of permissible requests. A PUM includes the requesting agency's authorized mission permitting use of such information, a description of the intended use of the domestic imagery, who will exploit the domestic imagery, who will receive the domestic imagery and derived products, storage and protection of the imagery, and *certification by an appropriate official of the lawfulness and validity of the request*.[67]

Sutherland further explained that prior to approval, NGA legal and policy experts review all submissions to ensure compliance with applicable law.[68]

C. A Programmatic Review of the Civil Applications Committee

Unfortunately, little more is publicly known about how the CAC works, and even that which is now known would likely have remained undisclosed if not for DHS efforts, beginning in 2005, to create an office known as the National Applications Office (NAO).[69] The vision of the NAO was that it would promote wider distribution of domestic imagery from reconnaissance satellite assets for civil, national security, and law enforcement purposes.[70] The office's genesis sprang from an independent study chartered by the Director of National Intelligence (DNI)[71] and the Director of the USGS to

65. *Id*. at 101. Given the elimination of the DCI, this authority likely currently rests with the Director of National Intelligence. *See infra* note 71.

66. *See Hearing*, *supra* note 9, at 13 (statement of Daniel W. Sutherland, Officer, U.S. Dep't of Homeland Sec. Office of Civil Rights and Civil Liberties).

67. *Id*. (emphasis added).

68. *Id*.

69. Congressional hearings regarding the NAO's operations exposed many details that had not previously been publicly acknowledged.

70. *See* Press Release, Dep't of Homeland Sec., Fact Sheet: National Applications Office (Aug. 15, 2007), http://www.dhs.gov/xnews/releases/pr_1187188414685.shtm.

71. After 9/11, with the passage of the Intelligence Reform Act, the DNI essentially subsumed the duties of the DCI. *See* Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458 § 1081, 118 Stat. 3696 (codified in scattered sections of 50 U.S.C.) ("Any reference to the Director of Central Intelligence or the Director of the Central

review the "operation and future role" of the CAC.[72] These officials felt the study was necessary in light of the fact that "opportunities to better protect the nation" were being missed because of outdated and unclear legal guidance.[73]

In its findings, the study group noted that the policy surrounding domestic use of reconnaissance imagery "is anchored in a complex web of law, National Security Policy and Presidential executive orders, DNI/DCI and DOD Directives, Interagency Agreements, and imagery-specific policy developed, coordinated, promulgated and maintained by" NGA.[74] The group felt that such a framework served to "discourage rather than encourage use by domestic users" since the "legal regime governing the use of [Intelligence Community] capabilities domestically is unsettled."[75] And though the study was largely undertaken to examine national security and law enforcement applications, the group emphasized that the "missed opportunities to collect, exploit and disseminate domestic information" extended even to "preparing for, responding to, and recovering from" manmade and natural disasters.[76]

Beyond the lack of clear *legal* guidance, the study also highlighted that the culture of secrecy within the Intelligence Community perpetuated the problem, and even if legal guidelines were clearer, there was nevertheless a "cultural aversion toward collection of domestic imagery."[77] Although this environment has not received a great deal of attention as specifically related to the satellite reconnaissance community, it has been well documented within the Intelligence Community generally.[78] One commentator, for instance, has fittingly observed that apprehensions regarding "secrecy and the protection of information can lead to increasing

Intelligence Agency in the Director's capacity as the head of the intelligence community . . . shall be deemed to be a reference to the Director of National Intelligence.").

72. CAC BLUE RIBBON STUDY, *supra* note 6, at 4.

73. *Id*.

74. *Id*. at 33.

75. *Id*. at 5, 18; *see also id*. at 29 ("[A]s a result of presentations by lawyers from the intelligence community, the ISG was advised of the uncertainty and conflicting opinions regarding lawful application and use of imagery.").

76. *Id*. at 5.

77. *Id*. at 32–33.

78. This has been especially true in the aftermath of September 11, 2001, given the fact that information-sharing issues were widely cited as a reason for the government's failure to prevent the attacks against the United States. *See*, *e.g.*, John D. Podesta, *Shadow Creep: Government Secrecy Since 9/11*, 2002 J.L. TECH. & POL'Y 361, 362–63 (2002).

risk-aversion and loss-aversion. Prudent regulations and sensible norms initially established to guard against worse-case scenarios can suffer from a kind of 'normative drift'—pretty soon, an old rule like 'if in doubt, classify' becomes the default rule 'always classify.'"[79] As pertaining to reconnaissance satellite imagery, the CAC study group noted that this culture has led to a general "across-the-board application of a SECRET level marking in an effort to protect sources and methods and serve as a hedge against uncertainty."[80] While there are definitely exceptions to this classification scheme, the fact that they are *exceptions* is indicative of the secretive culture within the community that discourages the release of imagery, even for disaster related purposes.

In light of this culture of secrecy and the aforementioned legal complexities surrounding the domestic use of satellite imagery, the study group ultimately concluded that "significant change is needed in policy regimes regulating domestic use of [Intelligence Community] capabilities."[81] The group thus recommended a comprehensive review of all laws, policies, and practices governing domestic satellite collection.[82] Noting that "the same concerns which gave rise to the CAC are likely to emerge again," the group also proposed formation of a Domestic Applications Office (DAO) within DHS to "ensure the capabilities of the [Intelligence Community] are used lawfully and with full consideration of the rights of U.S. persons."[83]

IV. THE NATIONAL APPLICATIONS OFFICE

While it is unclear what efforts—if any—were made toward the recommendation of clarifying the legal framework surrounding domestic satellite collection, work began almost immediately to establish the DAO. Although he had only received the study group's report in December of 2005, by March of 2006, DHS Secretary Michael Chertoff sent a letter to DNI John Negroponte calling for

79. Roderick M. Kramer, *A Failure to Communicate: 9/11 and the Tragedy of the Informational Commons*, 8 INT'L PUB. MGMT. J. 397, 405 (2005).

80. CAC BLUE RIBBON STUDY, *supra* note 6, at 34.

81. *Id.* at 5.

82. *Id.*

83. *Id.* at 15, 30–31.

the transition of all CAC functions to the DAO within sixty days.[84] The DNI moved slightly more deliberatively, but by May of 2007, Negroponte had designated DHS as the executive agent of what had, along the way, become the National Applications Office (NAO).[85] This Part discusses the effort to create the NAO specifically as related to the problems it revealed with the government's domestic imagery collection strategy.

A. Congress Finally Gets Involved in Domestic Imagery Collection

The first public statement about the NAO was made by DHS in August of 2007, less than two months before the office was slated to open.[86] Perhaps not coincidentally, DHS's announcement came while Congress was on its August recess.[87] When Congress reconvened in September, Representative Bennie Thompson, the Chairman for the House Committee on Homeland Security, immediately commenced hearings to discuss the NAO.[88] Thompson made clear that despite the nearly two-year effort to establish the NAO, no one within either DHS or the DNI's office had ever informed the Committee on Homeland Security about the

84. Memorandum from Michael Chertoff, DHS Secretary, to Ambassador John D. Negroponte, DNI (Mar. 14, 2001), http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB229/41.pdf. It is hard to overlook how much DHS stood to gain from this arrangement. Not only did the establishment of the DAO require transfer of the CAC's functions (and staff) from the DNI to DHS, the study group had also recommended that the DNI continue to fund the program. CAC BLUE RIBBON STUDY, *supra* note 6, at 4. It can be argued that at least part of the reason for that proposal was that it would have permitted the DAO/NAO to remain somewhat more independent. The fact remains, though, that DHS appeared to have little to lose with this venture, which may explain the haste (and concomitant lack of foresight) with which the program proceeded.

85. *See* DEP'T OF HOMELAND SEC. OFFICE OF INSPECTOR GENERAL, LETTER REPORT: DHS NATIONAL APPLICATIONS OFFICE PRIVACY STEWARDSHIP (REDACTED) OIG REPORT 08-35, at 2 (2008), http://www.dhs.gov/xoig/assets/mgmtrpts/OIGr_08-35_Apr08.pdf. Though there is evidently no public information regarding the name change, the explanation for it does not require much imagination. News of the NSA's Terrorist Surveillance Program, which was more colloquially known as the "domestic spying program," broke in December of 2005. *See* James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1. The change from *Domestic* Applications Office to *National* Applications Office likely ensued so as to avoid any perceived affiliation between the two programs.

86. *See* Press Release, U.S. Dep't of Homeland Sec., Fact Sheet: National Applications Office (Aug. 15, 2007), http://www.dhs.gov/xnews/releases/pr_1187188414685.shtm.

87. *Hearing*, *supra* note 9, at 1.

88. *Id.*

program.[89] Indeed, he chided the senior DHS representative during the hearings for the fact that the committee had to learn about the NAO from the *Wall Street Journal* and noted that "there was no briefing, no hearing, no phone call from anyone [within DHS] to inform any member of this committee of why, how, or when satellite imagery would be shared" with civil agencies.[90]

1. DHS notice to Congress

To put it mildly, the hearings were a disaster for the NAO. The fact that DHS had not informed the committee about the program was the first source of contention. One congressman noted, for example, that "if we are to be an effective oversight committee . . . it is essential that we be brought in at the start, not find out about [such programs] from press reports after the fact."[91] Less generously, another committee member compared the NAO to the National Security Agency's Terrorist Surveillance Program.[92] "[W]e are dealing in context here," said Representative Jane Harman, "[a]nd the context is . . . that this administration, post 9/11, rolled out the terrorist surveillance program, decided unilaterally . . . and has been making security policy in the executive branch without full regard for the laws that Congress has passed."[93] Later, she stated that though she and the rest of Congress had been "rolled" on the terrorist surveillance program, she did not intend "to get rolled again."[94]

2. Failure in planning

More substantively, DHS representatives faced intense criticism for failing to fully consider the legal ramifications of the NAO before its launch. One of the major sources of concern was that the NAO planned to expand the use of domestic satellite imaging to include

89. *Id.*

90. *Id.*

91. *Id.* at 3 (statement of Hon. Peter T. King, Ranking Member, H. Comm. on Homeland Sec.).

92. *Id.* at 23 (statement of Hon. Jane Harman, Member, H. Comm. on Homeland Sec.).

93. *Id.*

94. *Id.* at 59. Likewise, a witness adverse to the creation of the NAO noted that Congress should indeed have been offended that after two years of DHS work to establish the program, "and on the eve of its implementation," the *press* had to "discover this revolutionary plan." *Id.* at 56 (statement of Lisa Graves, Center for Nat'l Sec. Studies Deputy Director).

not only civil applications, such as disaster planning and relief, but also national security and law enforcement collection. From the perspective of most committee members, this posed significant problems related to the Posse Comitatus Act (PCA)[95] and the Fourth Amendment.[96]

a. The Posse Comitatus Act. In general terms, the PCA prohibits the U.S. military from *directly* participating in law enforcement activities, except in certain exceptional circumstances.[97] The Act reflects a "long tradition of suspicion and hostility toward the use of military forces for domestic purposes."[98] In the leading case concerning the PCA, *United States v. Red Feather*, the court explained that impermissible direct participation in law enforcement includes such activities as "arrest; seizure of evidence; search of a person; search of a building; investigation of crime; interviewing witnesses; pursuit of an escaped civilian prisoner; search of an area for a suspect and other like activities."[99] By contrast, permissible passive involvement includes such activities as aerial reconnaissance, offering advice about operational planning, and delivery of military equipment and supplies for training purposes.[100]

As pertaining to the NAO, certain members of the Committee for Homeland Security apparently believed that "[u]sing [the] Department of Defense" in any manner for NAO law enforcement operations would, in and of itself, be a violation of the PCA.[101] This perception was perhaps perpetuated by the testimony of a witness adverse to the NAO who noted that "[t]hese are the Department of Defense satellites. These offices are within the Department of

95. 18 U.S.C. §1385; *see*, *e.g.*, *Hearing*, *supra* note 9, at 23, 35, 41–42, 46–47, 50, 55–61.

96. U.S. CONST. amend. IV.

97. 18 U.S.C. § 1385; *see also* The Posse Comitatus Act, U.S. N. Command, http://www.northcom.mil/About/history_education/posse.html (last visited Jan. 14, 2011). While the Act itself encompasses only the Army and Air Force, DoD directives have made the prohibition applicable to the Navy and Marine Corps. *See* JENNIFER K. ELSEA, THE POSSE COMITATUS ACT AND RELATED MATTERS: A SKETCH, CONGRESSIONAL RESEARCH SERVICE REPORT RS20590 (June 6, 2005), at CRS-4.

98. Bisonette v. Haig, 776 F.2d 1384, 1389 (8th Cir. 1985).

99. 392 F. Supp. 916, 925 (D.C. S.D. 1975).

100. *Id.*

101. *Hearing*, *supra* note 9, at 42 (statement of Hon. Sheila Jackson Lee, Member, H. Comm. on Homeland Sec.).

Defense. This is the military."[102] When asked about the implications of the PCA on the operations of the NAO, DHS officials suggested that there would be no violation because "NGA can provide *indirect* support."[103] The committee members, however, remained unpersuaded, with one suggesting bluntly that she did not find the government's response to the PCA issues at all satisfactory.[104]

b. The Fourth Amendment. In addition to the PCA issues, the committee had a fundamental problem with the fact that the NAO's operations, especially those related to law enforcement, would potentially violate the Fourth Amendment.[105] The Fourth Amendment provides, in relevant part, that "[t]he 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."[106] During the hearings, one witness explained that the domestic use of satellite imagery was such an unreasonable search that it was essentially "like Big Brother in the Sky."[107] As for the committee, one member noted that the "[F]ourth [A]mendment really is a kind of cornerstone, if you will, for the home being the castle. If we allow the unfettered access by way of satellite technology, which is unchartered space for us, we really don't know exactly where this will end."[108] Another committee member pointed out that the Supreme Court had suggested in dicta that satellite surveillance might be unconstitutional without a warrant.[109] Though the DHS witnesses

102. *Id.* at 44 (statement of Barry Steinhardt, Director of the American Civil Liberties Union Program on Technology and Liberty). Another witness went further, suggesting that the *Red Feather* decision interpreted the PCA too narrowly. In her estimation, the PCA was designed not only to prohibit aggressive assistance by the armed forces, but all military intervention in domestic affairs. *Id.* at 55 (statement of Lisa Graves, Center for Nat'l Sec. Studies Deputy Director).

103. *Id.* at 42 (statement of Hugo Teufel, III, Chief Privacy Officer, U.S. Dep't of Homeland Sec.) (emphasis added).

104. *Id.* at 24 (statement of Hon. Jane Harman, Member, H. Comm. on Homeland Sec.).

105. *Id.* at 26 (statement of Hon. Al Green, Member, H. Comm. on Homeland Sec.).

106. U.S. CONST. amend. IV.

107. *Hearing*, *supra* note 9, at 50 (statement of Lisa Graves, Center for Nat'l Sec. Studies Deputy Director).

108. *Id.* at 26 (statement of Hon. Al Green, Member, H. Comm. on Homeland Sec.).

109. *Id.* at 28 (statement of Hon. Daniel E. Lungren, Member, H. Comm. on Homeland Sec.) (citing Dow Chemical Co. v. United States, 476 U.S. 227, 238 (1986) ("[S]urveillance of private property by using highly sophisticated surveillance equipment not

were able to certify that the NAO would not permit penetration of buildings and homes,[110] when specifically asked if there were any U.S. Supreme Court cases directly pertaining to the NAO's planned operations, they could only respond that they were still "coordinating [their] thoughts" on the matter.[111]

c. Statutory schemes and congressional oversight. In an attempt to alleviate some of the committee's concern, DHS officials testified that reconnaissance satellite imagery had "been used for decades lawfully and appropriately to support a variety of domestic uses by the U.S. Government's scientific, security, and law enforcement agencies."[112] They asserted that the NAO would actually provide more oversight for such collection, because approval authority would no longer be concentrated within NGA.[113] Specifically, though NGA would continue to play an integral role in the approval process, they explained that the NAO would also be "subject to direct oversight by privacy and civil liberties offices within both" DHS and ODNI.[114] Additionally, the NAO would even "have its own legal advisor."[115] DHS witnesses further explained that the process would be subject to the House and Senate Intelligence Oversight Committees and that it would comply with all applicable laws.[116] Ultimately, DHS saw the development of the NAO as nothing more than an expansion of

generally available to the public, such as satellite technology, might be constitutionally prescribed [sic] absent a warrant.")).

110. *See id.* at 29 (statement of Charles Allen, Chief Intelligence Officer, Office of Intelligence and Analysis, U.S. Dep't of Homeland Sec.).

111. *Id.* at 21 (statement of Daniel W. Sutherland, Officer, U.S. Dep't of Homeland Sec. Office of Civil Rights and Civil Liberties).

112. *Id.* at 5 (statement of Charles Allen, Chief Intelligence Officer, Office of Intelligence and Analysis, U.S. Dep't of Homeland Sec.).

113. *Id.* at 15 (statement of Hugo Teufel, III, Chief Privacy Officer, U.S. Dep't of Homeland Sec.).

114. *Id.* at 9 (statement of Charles Allen, Chief Intelligence Officer, Office of Intelligence and Analysis, U.S. Dep't of Homeland Sec.).

115. *Id.* (statement of Charles Allen, Chief Intelligence Officer, Office of Intelligence and Analysis, U.S. Dep't of Homeland Sec.).

116. *Id.* These included "the National Security Act of 1947, Executive Order 12333, the Homeland Security Act of 2002, and . . . the Privacy Act." *Id.* at 19. Exec. Order N. 12,333, 46 Fed. Reg. 59,941 (Dec. 8, 1981) (revoking Exec. Order 12,036); Exec. Order No. 12,036, 43 Fed. Reg. 3,674 (Jan. 24, 1978) (superseding Exec. Order 11,905).

its then-existing customer base and a means of streamlining an otherwise ad hoc process.[117]

In response, the committee pressed for more details, which simply were not forthcoming. Representative Harman, for instance, stated that "just telling us that [existing laws] cover this program is not telling me anything."[118] Instead, she "want[ed] to see the legal document[s] that put[] the clear, bright legal framework around" the NAO.[119] Another committee member, Representative Al Green, expressed concern that too much power related to satellite imagery had been concentrated in the executive branch.[120] "The [C]onstitution requires a broader remedy that envisions the judiciary being a part of something as pervasive as what we are capable of doing with the satellites."[121] Indeed, Green was not even persuaded that previous activities related to domestic collection were constitutional.[122] He raised the question of why "something comparable to what FISA was envisioned to be" could not be used as a clearinghouse for domestic collection requests.[123]

d. The beginning of the end. Though one committee member expressed that the NAO was merely consolidating "what has been done in an ad hoc way in a variety of ways over the past 30 years," such statements of support were rare.[124] In the end, the committee called for a moratorium on the opening of the NAO until DHS could show that adequate legal frameworks were in place to ensure

117. *Id.* at 20 (statement of Charles Allen, Chief Intelligence Officer, Office of Intelligence and Analysis, U.S. Dep't of Homeland Sec.).

118. *Id.* at 23 (statement of Hon. Jane Harman, Member, H. Comm. on Homeland Sec.).

119. *Id.*

120. *Id.* at 26 (statement of Hon. Al Green, Member, H. Comm. on Homeland Sec.).

121. *Id.*

122. *Id.*

123. *Id.* at 27. FISA is the Foreign Intelligence Surveillance Act, which was enacted in 1978 as an attempt to balance Fourth Amendment rights against the need to conduct domestic national security intelligence collection. FISA required that the executive branch (more precisely, the president, acting through the attorney general) obtain an order from the Foreign Intelligence Surveillance Court (FISC) before conducting a search against U.S. persons for foreign intelligence purposes. 50 U.S.C. §§ 1804–05 (1978). By its terms, FISA originally only applied to electronic surveillance, though it has since been extended to physical searches for foreign intelligence purposes. 50 U.S.C. §§ 1801–12 (1978); 50 U.S.C. § 1822 (2008).

124. *Hearing*, *supra* note 9, at 3–4 (statement of Hon. Peter T. King, Ranking Member, H. Comm. on Homeland Sec.).

that "military spy satellites do not become the 'Big Brother in the Sky' that some in the privacy and civil liberties community have described."[125] Subsequently, Congress passed legislation prohibiting "funds from being made available to commence operations of the NAO" until DHS certified that the program would be compliant with existing laws, and until that certification was thereafter reviewed by the Government Accountability Office (GAO).[126] While DHS certified the program to Congress in April of 2008, the GAO review released in November of 2008 was likely the death knell for the office.[127] In its very first finding, the GAO review succinctly reported that DHS "has not yet fully addressed all outstanding issues regarding how the planned operations of the NAO . . . are to comply with legal requirements."[128] In June of 2009, DHS Secretary Janet Napolitano announced the closure of the NAO.[129]

B. Failing to Learn from the NAO Experience

Admittedly, much of the anxiety surrounding the NAO was based on the DHS's plan to extend domestic satellite collection to national security and law enforcement applications. Nevertheless, as Representative Green pointed out during the NAO hearings, the events surrounding the NAO debacle also exposed fundamental and persistent concerns regarding the domestic use of reconnaissance satellites and raised questions about the legitimacy of using them even for civil users within FEMA and state and local governments. Indeed, as plans to establish the NAO evolved, the CAC study group's observation regarding the unsettled "legal regime governing

125. BEST & ELSEA, *supra* note 26, at CRS-10 (quoting letter from Hon. Bennie G. Thompson, Chairman, H. Comm. on Homeland Sec., to Hon. David E. Price, Chairman, Subcomm. on Homeland Sec., Comm. on Appropriations and Hon. Harold Rogers, Ranking Member, Subcomm. on Homeland Sec., Comm. on Appropriations) (Sept. 26, 2007). *See also* Letter from Hon. Bennie G. Thompson, Chairman, H. Comm. on Homeland Sec., to Hon. Michael Chertoff, DHS Secretary, and Charles Allen, Chief Intelligence Officer, Office of Intelligence and Analysis, U.S. Dep't of Homeland Sec. (Sept. 6, 2007), http://hsc.house.gov/SiteDocuments/20070907154522-02923.pdf.

126. U.S. GOVERNMENT ACCOUNTABILITY OFFICE, NATIONAL APPLICATIONS OFFICE CERTIFICATION REVIEW, GAO-09-105R (Nov. 6, 2008), at 2.

127. *See id.* at 3.

128. *Id.*

129. *See* Press Release, U.S. Dep't of Homeland Sec., Secretary Napolitano Announces Decision to End National Applications Office Program (June 23, 2009), http://www.dhs.gov/ynews/releases/pr_1245785980174.shtm.

the use of [Intelligence Community] capabilities domestically" seemed especially prescient.[130]

These problems arguably had their root in the origins of the program and the fact that it was created, not by any legislative action, but rather by intra-executive memoranda and policy directives. As outlined above, this legal framework—such as it was—raised flags from the beginning as to the legitimacy of the effort.[131] Moreover, while the imagery itself was understandably safeguarded from public disclosure, the lack of transparency as to the policies and procedures governing domestic imaging made analogies to the NSA's Terrorist Surveillance Program all too easy to adopt. It also likely contributed to an incomplete understanding, both within the Intelligence Community and Congress, as to how the program fit within larger constitutional and statutory schemes such as the Fourth Amendment and the Posse Comitatus Act. Finally, the lack of clear legal guidance related to domestic imagery reinforced the culture of secrecy within the Intelligence Community and made analysts even more risk averse in decisions about releasing imagery for fear that they would be exceeding legal authorization. Given this context, it was no surprise that Congress so adamantly opposed efforts to establish the NAO.

But while efforts to create the office were perhaps appropriately stymied, the unfortunate result has been that since its closure, the government has simply returned to the status quo. Shortly after the NAO hearings, Representative Thompson sent a letter to DHS Secretary Michael Chertoff explaining that "[b]ifurcating the NAO into 'easy to do' domains and a 'hard to do' law enforcement domain is not an option."[132] Thompson believed the legal framework for all domestic imagery collection, whether for disaster planning or law enforcement, "should be completed as a seamless package so privacy and civil liberties are approached holistically and not haphazardly."[133] While there is certainly merit to this argument,[134]

130. *See supra* notes 75–76 and accompanying text.

131. *See supra* notes 56–59 and accompanying text.

132. Letter from Hon. Bennie G. Thompson, Chairman, H. Comm. on Homeland Sec., to Hon. Michael Chertoff, DHS Secretary (Apr. 7, 2008), http://homeland.house.gov/SiteDocuments/20080407134422-36588.PDF.

133. *Id.*

134. In addition to facilitating a comprehensive strategy for domestic imagery collection, for example, it would minimize the duplication of effort inherent in a bifurcated system. *See, e.g.*, CAC BLUE RIBBON STUDY, *supra* note 6, at 45.

the government's inability to effectively address the "hard to do" aspects of the NAO led to abandonment of efforts to clarify legal standards for even the "easy to do" domestic collections. Consequently, the energy poured into exposing the problems with the domestic satellite collection program—from the independent study group to the congressional hearings—has essentially been wasted. The program is, therefore, once again on a course encouraging missed "opportunities to better protect the nation."[135]

V. PROPOSED REFORMS

Several reforms are necessary to interrupt this pattern of wasted opportunities. First, in order to avoid abuses while still taking full advantage of satellite capabilities, Congress should develop an adequate governance structure under which a domestic collection program can operate. Further, this structure must be built on a more rigorous statutory framework outlining the parameters by which domestic imagery can be collected. Also, given the inherent lack of public transparency with certain aspects of this program, Congress must ensure that it is properly fulfilling its intelligence oversight responsibilities. Each of these proposals is discussed in turn.

A. Governance of the Domestic Imaging Program

Despite Representative Thompson's suggestion that bifurcation of the domestic satellite collection program into two domains or offices was not an option, such a structure in reality seems to be the most prudent course of action. More specifically, to the extent that they can be conducted lawfully at all, law enforcement operations ought to be managed in an office separate and distinct from the office managing collections for disaster planning and response. The primary rationale for this is that once the DoD engages in satellite collection for law enforcement purposes, the potential for Posse Comitatus Act and Fourth Amendment violations increases exponentially. On the other hand, when imagery collection is limited to civil applications, these issues, as Thompson suggested, are simply easier to address.

135. CAC BLUE RIBBON STUDY, *supra* note 6, at 4.

1. The Posse Comitatus Act

Though some members of Congress appear to have been confused about the dictates of the PCA, careful analysis of the Act suggests that bifurcation is necessary to comply with its prescribed dictates. More to the point, there does not appear to be a PCA violation for domestic imagery confined strictly to disaster preparation and response. Conversely, involving the military in domestic satellite collection for law enforcement purposes may indeed present a violation.

First, the PCA would clearly not be implicated if domestic satellite collection were strictly constrained to disaster planning and response. By its terms, the PCA only limits *military* participation in *law enforcement* activities.[136] While it is conceivable that federal troops could be requested for such law enforcement activities as quelling post-disaster riots or looting, scholars have suggested that these sorts of activities are usually less pervasive than reports might otherwise suggest.[137] Moreover, even if riots and looting were in fact to occur, given the relatively isolated and sporadic nature of such incidences, satellite imagery would not likely be helpful in subduing them. Even in the unlikely event that the military did rely on satellite imagery for such law enforcement operations, *Red Feather* suggests that any related PCA violation in this scenario would be for the manner in which the *troops* were used, rather than for use of DoD imagery.[138]

The calculus might change, however, if a unified collection strategy, including those related to law enforcement operations, were pursued. *Red Feather* clearly established that the PCA only prohibits the military from *directly* participating in law enforcement activities.[139] Thus, while using DoD assets to collect the imagery would not, in and of itself, violate the PCA, there are arguably

136. 18 U.S.C. § 1385 (2010).

137. *See*, *e.g.*, Thomas E. Drabek & David A. McEntire, *Emergent Phenomena and the Sociology of Disaster: Lessons, Trends and Opportunities from the Research Literature*, 12 DISASTER PREVENTION & MGMT. 97, 98–99 (2003).

138. It might be possible to extend this argument to a suggestion that since it would be the DoD providing satellite imagery to these military personnel, the PCA is in fact implicated. While this is explored in more detail in the following paragraph, suffice it to say that complications in such an unlikely scenario only appear to arise if military analysts are interpreting the imagery in an effort to seize evidence or conduct a search.

139. United States v. Red Feather, 392 F. Supp. 916, 925 (D.C.S.D. 1975).

related activities that might. For example, were military analysts to *interpret* imagery collected for law enforcement operations, there may in fact be a PCA violation.[140] The disposition of such a case would depend on whether a court viewed this effort simply as aerial reconnaissance—which *Red Feather* deemed indirect activity—or as a search for or seizure of evidence—which *Red Feather* said constituted direct involvement.[141] Clearly if the court saw satellite imagery collection as a seizure of evidence or a search, the activity would violate the PCA.[142]

2. The Fourth Amendment

Raising the issue of searches also brings to the forefront concerns related to the Fourth Amendment. As with the PCA, thorough scrutiny of the Fourth Amendment's application to domestic imagery collection in the disaster context suggests that bifurcation of the nation's domestic satellite collection strategy is necessary. In particular, while there are arguably no violations when reconnaissance satellites are used for disaster related missions, their use in the law enforcement context presents potential violations that may be entirely insurmountable.

Though such a case has never been adjudicated, it seems unlikely that domestic imagery collection confined strictly to disaster planning and response would be deemed a violation of the Fourth Amendment. This assertion rests on the fact that the U.S. Supreme Court has established that "the traditional requirement of a warrant based on probable cause is not well-suited to searches for purposes"

140. This is not simply an academic exercise. Though data related to NGA's workforce is classified, the agency is known to have "sizable numbers of active duty military personnel assigned" to it. BEST & ELSEA, *supra* note 26, at CRS-13. Moreover, similar issues may even apply to *non-military* analysts. This is because DoD directives indicate that even civilian employees of the DoD are subject to the PCA if they are "under the direct command and control of a military officer." Dep't of Defense Directive 5525.5 ¶ E4.2.3 (Dec. 20, 1989), *available at* http://www.dtic.mil/whs/directives/corres/pdf/552505p.pdf. Though the phrase "direct command" is obviously subject to interpretation, it is significant that since its creation in 1996, NGA has only had one civilian director. THE NAT'L GEOSPATIAL-INTELLIGENCE AGENCY, HISTORICAL HANDBOOK OF NGA LEADERS: OFFICE OF THE NGA HISTORIAN 58 (2008), https://www1.nga.mil/About/OurHistory/Documents/leaders.pdf.

141. *See Red Feather*, 392 F. Supp. at 925.

142. For a more thorough discussion as to whether satellite imagery collection for law enforcement purposes constitutes a search, see *infra* notes 148–51 and accompanying text.

such as public safety.[143] Instead, in such "special needs" cases,[144] the Court relies on a reasonableness test that balances the interests at stake to determine what precautions are appropriate.[145] As specifically applied to domestic disaster related reconnaissance imagery, an adjudicating court would thus weigh the value to be gained by using the imagery against any privacy interest that could potentially be invaded. Given that any personal invasion that might occur would be minimal, a court is likely to determine that it is dwarfed by the public safety interest. A court would, therefore, probably determine that only minimal safeguards are required for such strictly defined operations.[146] Since the government evidently already has safeguards and minimization procedures in place,[147] a court would likely reach the conclusion that domestic imagery collection for disasters does not violate the Fourth Amendment.

Conversely, using reconnaissance satellites for domestic imagery collection related to law enforcement and national security missions falls into the "hard to do" domain mentioned by Representative Thompson. This is essentially because "if the purpose of the search is simply to obtain evidence for purposes of criminal law enforcement, then probable cause and a warrant are presumptively required."[148] While the executive would likely argue that satellite imagery collection does not constitute a search, the U.S. Supreme Court has intimated otherwise. Specifically, in *Dow Chemical v. United States*, the Court noted that the use of "highly sophisticated surveillance equipment not generally available to the public, *such as satellite technology*, might be constitutionally proscribed absent a warrant."[149] And more generally, the Court held in *Kyllo v. United States* that the

143. STEPHEN A. SALTZBURG & DANIEL J. CAPRA, AMERICAN CRIMINAL PROCEDURE: INVESTIGATIVE, CASES AND COMMENTARY 382 (2007). This argument presupposes that satellite collection would constitute a search. The next paragraph addresses this issue more thoroughly.

144. Special needs cases are essentially those not focused on criminal law enforcement. *See id.*

145. *Id.*

146. Ultimately, the analysis and result of such a case may end up looking something akin to an administrative search. *See id.*

147. *See supra* note 55–56 and accompanying text. "Minimization efforts" are rules to ensure potential privacy invasions are limited and any evidence related thereto is destroyed. While there are apparently certain minimization processes currently in place, these should arguably be strengthened in any new statutory scheme that Congress adopts.

148. SALTZBURG & CAPRA, *supra* note 143, at 382.

149. 476 U.S. 227, 238 (1986) (emphasis added).

use of a thermal imaging device to detect heat emissions from a suspect's house was unconstitutional absent a warrant.[150] Importantly, the *Kyllo* holding rested largely on the fact that such thermal imaging tools were not generally in public use,[151] so an individual's expectation of privacy was higher than it might have been with other possible law enforcement techniques. Applying *Dow Chemical* and *Kyllo* to satellite technology, a court would likely determine that since satellites are not widely available to the general public, an individual's expectation of privacy against a satellite search would be high.[152]

3. Bifurcated organizational structure

In light of these PCA and Fourth Amendment issues, then, bifurcating the domestic imagery program into distinct law enforcement and disaster related operations seems to be precisely the correct approach. As explained, current constitutional and statutory provisions likely limit—if not altogether prevent—the ability to use reconnaissance satellite imagery domestically for law enforcement purposes. That fact, however, should not prevent or impede its use in disaster planning and response, though that is exactly what has happened. To the extent, therefore, that the government still believes domestic collection for law enforcement ought to be pursued, those efforts should continue independent of efforts to establish a more coherent domestic imagery strategy for disasters.[153]

150. 533 U.S. 27, 40 (2001).

151. *Id.*

152. These cases assert that if law enforcement officers were to obtain a warrant, the use of satellite technology would perhaps be permissible. The conundrum, however, is that the very purpose of using satellite imagery would likely be to *establish* probable cause, which is the standard of proof required to obtain a warrant in the first place. In other words, if law enforcement officers were able to establish the level of proof required to obtain a warrant to use satellite technology, they would likely not need to use it, since they could instead simply procure a warrant to search a house. SALTZBURG & CAPRA, *supra* note 143, at 72. Thus, just as the "Court's holding in *Kyllo* put[ ] an end to the law enforcement use of thermal imaging devices to scan homes," the same result would likely flow from any case regarding satellite imagery collection for law enforcement purposes. *Id.*

153. On this point, it bears mentioning that in the DHS press release announcing the closure of the NAO, DHS indicated that the office was being shut down because of changing priorities. This was perhaps driven by the fact that law enforcement officials themselves indicated that they had other issues more pressing than the NAO. *See* Press Release, U.S. Dep't of Homeland Sec., Secretary Napolitano Announces Decision to End National Applications Office Program (June 23, 2009), http://www.dhs.gov/ynews/releases/pr_1245785980174.shtm.

In the meantime, in order to provide adequate governance and long-term stability to the domestic imaging program, the government should establish an office responsible for fielding domestic imaging requests for disaster planning. While some might contend that the CAC performs this function already, its ad hoc operating structure and the numerous indicia of missed collection opportunities belie that argument. Moreover, the 2005 CAC independent study noted that "a committee structure was not the most efficient process and that without multi-department level support and dedicated resources it would not be sustainable."[154]

As for the best placement of such an organization within the government, the plans to situate the NAO within DHS seem prudent since FEMA is housed within DHS. There are several features that make placing the NAO within FEMA a particularly logical organizational choice. First, the agency already has a Mapping and Analysis Center that uses imagery products to prepare for and respond to disasters.[155] In fact, even when NGA assets have been used in the past to support domestic disasters, they have been provided only after a request from FEMA.[156] Beyond that, placement within FEMA seems appropriate given that improving readiness for, response to, and recovery from disasters is one of DHS's top five priorities.[157] While it might be more organizationally efficient to house the domestic imaging program within NGA—since it already manages the bulk of imagery collection and interpretation—such a proposal could perpetuate the perception that the government is spying on U.S. persons.[158] Moreover, part of the current problem is that NGA already holds a great deal of unilateral authority over the imagery collection process. Placement of the domestic imaging program within FEMA would defuse many of the civil liberties concerns surrounding domestic imagery collection since FEMA's focus has traditionally been on disaster response rather than law

154. CAC BLUE RIBBON STUDY, *supra* note 6, at 43.

155. *See* FEMA, http://www.gismaps.fema.gov/rs.shtm (last visited Jan. 14, 2011).

156. *See*, *e.g.*, Press Release, Nat'l Geospatial-Intelligence Agency, NGA Supports Federal Response to California Wildfires (Oct. 26, 2007), http://www.nga.mil/NGASiteContent/StaticFiles/OCR/nga0712.pdf; Press Release, Nat'l Geospatial-Intelligence Agency, NGA Makes Imagery of Midwest Flooding Available to the Public (June 20, 2008), http://www.nga.mil/NGASiteContent/StaticFiles/OCR/nga0806.pdf.

157. U.S. Dep't of Homeland Sec., Department Responsibilities, http://www.dhs.gov/xabout/responsibilities.shtm#four (last visited Jan. 14, 2011).

158. *See* CAC BLUE RIBBON STUDY, *supra* note 6, at 44.

enforcement missions. Finally, housing the domestic imagery collection program within FEMA would allow it to benefit from the oversight of DHS's Office for Civil Rights and Civil Liberties.[159]

B. Codification of Imaging Policy

Even if this governance proposal seems too challenging, the government should at least pursue the CAC study group's recommendation to pursue a comprehensive review of the laws, policies, and practices governing domestic reconnaissance satellite imagery collection.[160] As the study group noted, the executive agreements and policies used to sustain the program to this point have created an indecipherable "complex web of law" that contributes to the underutilization of this resource.[161] And while Congress has thus far evidently acquiesced to this situation, congressional input is critical to creating a more comprehensive and clearly defined domestic imaging strategy.

There are a variety of possible approaches to solving this problem. First, since there are arguably no constitutional violations for domestic satellite collection limited to disasters, Congress could simply develop and enact clear laws codifying—and therefore legitimizing—existing intra-executive memoranda, directives, and practices. To the extent that this effort would create a unified framework around the domestic imagery collection program, it would serve to unravel the current complexities related to these efforts. During this process, Congress could also strengthen these laws and policies to ensure that appropriate minimization efforts, remedies, and sanctions for violations are included.[162] While this proposal might first appear to waste effort and energy (in that it would essentially only reinforce the status quo), the congressional "stamp-of-approval" is necessary to alleviate the confusion and concern currently surrounding the domestic use of reconnaissance

159. The Office for Civil Rights and Civil Liberties is responsible for "ensuring respect for civil rights and civil liberties in policy decisions and implementation of those decisions" within DHS. Dep't of Homeland Sec., About the Office for Civil Rights and Civil Liberties, http://www.dhs.gov/xabout/structure/editorial_0371.shtm (last visited Jan. 14, 2011).

160. *See* CAC BLUE RIBBON STUDY, *supra* note 6, at 5.

161. *Id.* at 33.

162. *See supra* note 147.

satellites and to counter the culture of secrecy within the Intelligence Community.[163]

With this effort being driven by Congress rather than the executive, the codification process and outcome will potentially be more transparent, potentially assuaging public concerns of executive domestic spying. Moreover, Congress's involvement in drafting these laws would also better posture it to engage in oversight activities related to these operations.[164] Finally, by clarifying existing policies and directives with codified statutes, Congress would empower members of the Intelligence Community to engage in wider information sharing without having to "hedge against uncertainty" as to the permissibility of releasing such imagery.[165]

Representative Green proposed another possible—and far more drastic—approach during the NAO hearings. Concerned that the current domestic satellite imaging program vests too much power in the executive, he passionately suggested that something akin to FISA be implemented, since doing so would ensure that the judiciary review and approve the legitimacy of each domestic imagery request. Specifically, in directing his comments to the DHS witnesses, he stated, "Listen, I am imploring, I beseech you, I beg that you please give some consideration to the notion that we need a third branch of government or another branch of government involved."[166]

While a comprehensive exploration of this proposal is beyond the scope of this paper, there are a few especially significant points worth noting. First, it is important to highlight that as presently constituted, FISA only applies, as its name suggests, to domestic collections made for the purposes of gathering *foreign intelligence* matters.[167] Thus, although a strict FISA-like scheme may have very limited application to collections designed to prevent disasters caused

163. In codifying the nation's domestic imagery policy, Congress can perhaps delegate some of this authority rather than delve into all of the particulars. However, given the fact that the executive already created the current, confused structure, Congress arguably needs to at least establish the basic parameters and broad framework for the program. This may include laws establishing such fundamental issues as what general types of imaging are appropriate (disaster- related collection but not law enforcement, for example), minimization efforts that are necessary to comply with the Fourth Amendment, and penalties that will be imposed for abuses.

164. Oversight issues are discussed more thoroughly below. *See infra* Part V.C.

165. *See* CAC BLUE RIBBON STUDY, *supra* note 6, at 34.

166. *Hearing*, *supra* note 9, at 28 (statement of Hon. Al Green, Member, H. Comm. on Homeland Sec.).

167. 50 U.S.C. § 1801 (2006).

by terrorist attacks,[168] it would not seem to address judicial review for imagery collection related to other types of manmade or natural disasters.[169] Another central question Congress would have to address if it were to pursue this option is whether the Foreign Intelligence Surveillance Court (FISC)—the body that currently adjudicates FISA matters—would be the proper court to review the legality of satellite imagery requests, or if standard Article III courts could do so.[170] Additionally, Congress would even have to decide how to frame the proceedings. More specifically, any new legislation on this front would have to address whether the proceedings would be non-adversarial, as the FISC is now,[171] or whether amici curiae would be appointed to oppose the government's collection requests. Because time is of the essence during disaster response, Congress would ultimately also need to consider whether the value of these procedures outweighs the opportunities that would inevitably be lost by delays in the adjudicative process.

Clearly, these are only the more obvious issues requiring consideration should Congress choose to adopt a policy of judicial review for domestic satellite imagery requests. Frankly, given congressional inaction related to the program to this point, it seems unlikely that Congress will pursue such a complex course of action. Nor, in fact, does such a dramatic proposal even seem necessary to address the challenges currently plaguing domestic imagery collection. Instead, clarifying and codifying existing policies and practices seems to be the more realistic and effective approach. Doing so would remove much of the uncertainty among analysts as to precisely what can be released to domestic users like FEMA and state and local disaster responders. Moreover, with clarified legal guidance, these domestic users will be more informed about the

168. Strict adherence to FISA would require the individual subject to surveillance be an agent of a foreign power. *Id.* at § 1801(b).

169. This of course is not meant to suggest that judicial review would not be appropriate for natural-disaster-related requests; rather, it is intended merely to establish that the parameters of any new statutory construct of this sort would have to extend beyond the scope of issues currently covered by FISA.

170. Each option offers unique advantages; the FISC is already familiar with many intelligence issues, but regular Article III courts would arguably be better resourced to handle the additional demand.

171. *See* Kristian W. Murray, *National Security Veiled in Secrecy: An Analysis of the State Secrets Privilege in National Security Agency Wiretapping Litigation*, 199 MIL. L. REV. 1, 46 n.239 ("FISC hearings are non-adversarial proceedings where the government presents applications to conduct surveillance.").

requests they can make to better carry out their missions. But whatever legislative course Congress eventually pursues, its role should not end with the enactment of statutes.

C. Oversight

Indeed, in developing the statutory scheme to address the confusion surrounding domestic imagery collection, Congress must also ensure that there is a corresponding oversight regime to deter and uncover any abuses.[172] The CAC's current approach is one of self-policing, where agencies making domestic imagery requests certify *themselves* that their collections comply with applicable law. While CAC members and NGA officials apparently review these certifications, the fact remains that all assessment is currently intra-executive. Though these mechanisms are certainly important, as one commentator has observed, they ultimately amount to the executive telling Congress and the public to "trust us; we can handle all of this powerful technology, and we will handle it in a manner that is consistent with our principles" and with the law.[173] The fact that the Committee for Homeland Security learned of the NAO from the press, however, does not bode well for the reliability of such promises. Further, given prior legal concerns raised by other domestic Intelligence Community programs, the importance of independent oversight is difficult to overstate.[174]

172. Perhaps somewhat unwittingly, Congress has already taken a major step in this direction. In the Intelligence Authorization Act of 2010, Congress amended the Inspector General Act of 1978 to include the NRO and NGA as "designated federal entities." S. REP. NO. 111-223, at 59 (2010). With such designation, these offices "will be required by statute to administratively appoint inspectors general." *Id*. While each agency had in fact previously established its own Inspector General (IG) office, because they were not previously within the Inspector General Act of 1978, they lacked the degree of authority and independence necessary to effectively perform their functions. *Id*. Given this new amendment, however, NRO and NGA IGs will now have greater authority to access information, perform audits, and independently report their findings to the DoD IG and the GAO. *Id*. While such investigations will obviously still be conducted entirely within the executive branch, this change nevertheless provides another level of oversight to deter and/or discover potential abuses related to the domestic imaging program.

173. *Hearing*, *supra* note 9, at 43 (statement of Barry Steinhardt, Director of the ACLU Program on Technology and Liberty).

174. As noted above, the CAC itself sprang from investigations into domestic spying by the CIA. *See supra* notes 44–48 and accompanying text. Other examples of questionable Intelligence Community programs include the NSA's Terrorist Surveillance Program and the Defense Advanced Research Projects Agency's Total Information Awareness program. *See* Risen & Lichtblau, *supra* note 85; GINA MARIE STEVENS ET AL., PRIVACY: TOTAL

Congress must, therefore, address intelligence oversight issues within its own body. As an indication of just how critical this is, the 9/11 Commission called its proposal to strengthen congressional intelligence oversight one of its most important propositions.[175] The Commission's recommendation was based on the observation that the then-existing intelligence oversight structure was "dysfunctional," and that "intelligence committees lack the power, influence, and sustained capability" to protect American interests.[176] Presciently, however, the commission also noted that "[f]ew things are more difficult to change in Washington than congressional committee jurisdiction and prerogatives."[177] And, in fact, little progress has been made since the release of the commission's report.

Today, for instance, neither chamber of Congress has a standing committee focused specifically on intelligence issues.[178] Instead, both the House and Senate vest authority for intelligence in select committees, which are nominally only temporary bodies, without the authority "to receive and report out proposed legislation."[179] Though these select committees focus exclusively on intelligence issues, no fewer than fifteen standing committees oversee some aspect of intelligence,[180] and many of these committees have overlapping jurisdiction.[181] Such a complex and fragmented system

INFORMATION AWARENESS PROGRAMS AND RELATED INFORMATION ACCESS, COLLECTION, AND PROTECTION LAWS, CONGRESSIONAL RESEARCH SERVICE REPORT RL31730 (Mar. 21, 2003), at CRS-4.

175. NAT'L COMM'N ON TERRORIST ATTACKS UPON THE UNITED STATES, THE 9/11 COMMISSION REPORT 419 (2004).

176. *Id*. at 420.

177. *Id*. at 419.

178. Anne Joseph O'Connell, *The Architecture of Smart Intelligence: Structuring and Overseeing Agencies in the Post-9/11 World*, 94 CAL. L. REV. 1655, 1662 (2006).

179. *Id*. at 1662 n.27.

180. *Id*. at 1662. In the House, these are the Appropriations, Armed Services, Budget, Energy and Commerce, Government Reform, Homeland Security, International Relations, and Judiciary Committees. In the Senate, these are the Appropriations, Armed Services, Budget, Energy and Natural Resources, Foreign Relations, Homeland Security and Governmental Affairs, and Judiciary Committees. *Id*.

181. The NAO, for example, would likely have been subject to oversight by the select intelligence committees, as well as the Appropriations, Homeland Security, Homeland Security and Governmental Affairs, and possibly the Armed Services Committees. For a better idea of the scope of this problem, it is worth noting one group's finding that "no less that 88 committees and subcommittees in the House and the Senate had responsibility for oversight of homeland security." CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES, UNTANGLING THE WEB: CONGRESSIONAL OVERSIGHT AND THE DEPARTMENT OF HOMELAND SECURITY 2 (2004) http://csis.org/files/media/csis/events/041210_dhs_tf_whitepaper.pdf.

creates turf-wars that make effective oversight nearly impossible.[182] In fact, in a recent report judging the status of 9/11 Commission recommendations, intelligence oversight reforms received only a "D" grade.[183] The report specifically noted that "the ability of the intelligence committees to perform oversight of the intelligence agencies and account for their performance is still undermined by the power" of other committees and subcommittees.[184]

Congress must address these oversight issues in order to prevent potential executive abuses and to ensure the domestic imagery program operates within the confines of the legal framework it develops. Several proposals have been offered, including one by the 9/11 Commission to create a joint intelligence committee made up of members from both the House and Senate.[185] Less drastically, Congress could reform the overlapping jurisdictional issues currently impeding effective oversight operations by more clearly establishing the responsibilities and authorities of each committee.[186] Further, transforming the intelligence committees into standing committees with greater ability to influence intelligence related legislation would strengthen the committees.[187] Finally, since one of Congress's greatest tools is the power of the purse, the appropriations and intelligence committees could be structured to promote better cooperation and ensure that funding is only applied to programs that are consistent with the nation's priorities and legal frameworks.[188]

VI. CONCLUSION

The capabilities of reconnaissance satellite imagery make it a significant tool in efforts to prepare for and respond to disasters. Unfortunately, however, opportunities to use this capability are being squandered in light of complex and confusing guidance surrounding the legality of its use within the United States. This lack of clarity serves to perpetuate secrecy within an already cautious

182. *See* O'Connell, *supra* note 178, at 1663.

183. 9/11 PUBLIC DISCOURSE PROJECT, FINAL REPORT ON 9/11 COMMISSION RECOMMENDATIONS 3 (2005), http://www.9-11pdp.org/press/2005-12-05_report.pdf.

184. *Id*.

185. NAT'L COMM'N ON TERRORIST ATTACKS UPON THE UNITED STATES, *supra* note 175, at 420.

186. *See* O'Connell *supra* note 178, at 1733.

187. *Id*. at 1672.

188. *See id*. at 1673.

intelligence community and thus stymies the application of imagery even where operations are plainly legal. Further, the disjointed nature of the current legal framework also fosters fear within the public that "Big Brother" is watching.

Such concerns can and ought to be eliminated. Though current policies are complex and confusing, they at least do not appear to be in violation of applicable laws. As explained, this is arguably not the case regarding recent efforts to expand the domestic imagery program to law enforcement and national security collection. Accordingly, such efforts should either be abandoned, or at least separated from the government's disaster-related collection framework. Further, to eliminate confusion surrounding the use of reconnaissance satellites for disaster issues, Congress should enact clear legislation designed to codify the government's domestic collection strategy. After such laws are enacted, Congress must continue to monitor the domestic use of satellite imagery by actively overseeing the executive agencies engaged in the imagery program. By engaging in such continued monitoring, Congress will ensure that the appropriate balance is struck between protecting personal privacy and allowing the government to utilize capabilities that will protect its citizens. Because the next disaster will not wait until this legal framework is developed, now is the time to act.

Carla Crandall[*]

* J.D. Candidate, 2011, J. Reuben Clark Law School, Brigham Young University. The author would like to thank Professor Lisa Grow Sun for her helpful suggestions regarding previous drafts of this Comment. The author also expresses gratitude to the editors of the BYU Law Review for their diligent editing. Although the author was previously employed by the National Geospatial-Intelligence Agency, nothing in this article contains classified information obtained as a result of that employment. The views expressed herein are entirely those of the author.

TABLE OF ACRONYMS

CAC: Civil Application Committee
CIA: Central Intelligence Agency
DAO: Domestic Applications Office
DCI: Director of Central Intelligence
DHS: Department of Homeland Security
DIA: Defense Intelligence Agency
DNI: Director of National Intelligence
DoD: Department of Defense
DOI: Department of the Interior
EPA: Environmental Protection Agency
FEMA: Federal Emergency Management Agency
FISA: Foreign Intelligence Surveillance Act
FISC: Foreign Intelligence Surveillance Court
GAO: Government Accountability Office
GEOINT: Geospatial-Intelligence
IG: Inspector General
NAO: National Applications Office
NASA: National Aeronautics and Space Administration
NGA: National Geospatial-Intelligence Agency
NIMA: National Imagery and Mapping Agency
NPIC: National Photographic Interpretation Center
NRO: National Reconnaissance Office
NSA: National Security Agency
NSF: National Science Foundation
ODNI: Office of the Director of National Intelligence
OEP: Office of Emergency Preparedness
OMB: Office of Management and Budget
PCA: Posse Comitatus Act
PUM: Proper Use Memorandum
USACE: United States Army Corps of Engineers
USGS: United States Geological Survey