Louisiana Law Review

Volume 64
Number 4 *Normalization of National Security Law: A Symposium*
Summer 2004

Article 3

8-1-2004

The Role of Military Intelligence in Homeland Security

Stephen Dycus

The Role of Military Intelligence in Homeland Security

*Stephen Dycus**

I. INTRODUCTION

If, God forbid, the American homeland is struck by another major terrorist attack, military forces will very likely be involved in the response. There can be little doubt, for example, that if pneumonic plague bacilli are released in Chicago and infections result,[1] the entire city will have to be quarantined as soon as the contagion is detected. Nor is there any doubt that troops will be used to enforce the quarantine. Only the Pentagon and National Guard units have the personnel, equipment, and training to do the job.

Military forces also may be able to help prevent another attack or at least reduce its impact. On September 11, 2001, for instance, Air Force and Air National Guard jets were sent aloft in an unsuccessful effort to intercept and perhaps shoot down the civilian airliners that had been commandeered by terrorists.[2]

Whether in the response to a terrorist attack or in its interdiction, military intelligence services will directly support the military's use of force at home, just as they provide information and analysis for other military activities around the world. But these same military intelligence services appear poised to assume a much broader responsibility for domestic counterterrorism. A recent Pentagon report on the military's role in homeland security notes that while

---

* The author is a Professor at Vermont Law School. Special thanks are due to Edward Demetriou, Emily Wetherell, Matthew Einstein, and Byron Kirkpatrick, all students at Vermont School, for their assistance with research for this article.

1. This scenario was posited in an exercise called TOPOFF 2, sponsored by the Departments of State and Homeland Security in May 2003. *See* Dep't of Homeland Security, Top Officials (TOPOFF) Exercise Series: TOPOFF 2 – After Action Summary Report (Dec. 19, 2003). Because it was planned and advertised well in advance, it may have lacked much of the spontaneity and reality of an earlier, unannounced exercise entitled TOPOFF, which imagined a similar release in Denver. *See* Thomas Inglesby, Rita Grossman & Tara O'Toole, *A Plague on Your City: Observations from TOPOFF,* 32 Clinical Infectious Diseases 436 (2001), *available at http://www.journals.uchicago.edu/CID/journal/issues/v32n3/001347/001347.html*; National Response Team, Exercise TOPOFF 2000 and National Capital Region (NCR): After-Action Report (Aug. 2001).

2. The sequence of events is spelled out in The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States 16-46 (2004). *See also* Eric Schmitt & Eric Lichtblau, *In 149 Minutes, Transformation to Terror Age*, N.Y. Times, June 18, 2004, at A1.

"terrorism that targets the homeland is fundamentally a law enforcement matter that is best addressed by domestic law enforcement entities with DoD in a supporting role during crises, the Department has a responsibility to protect its forces, capabilities, and infrastructure within the United States."[3] It then goes on to suggest, however, that "Service and DoD law enforcement/counterintelligence organizations and NORTHCOM . . . have leading roles in collecting and analyzing information and intelligence, and in conducting investigations and operations to prevent or preempt terrorist attacks."[4] This view reflects a dramatic change in what we have understood—at least for the last three decades—to be the "normal" relationship between the military and the rest of American society.

Before we agree that military intelligence services should play a more expansive role in our domestic life, several practical questions need to be addressed. One of the most important questions is whether such a change would actually make us more secure. Would a more aggressive use of military intelligence at home make a uniquely valuable contribution to current counterterrorism efforts of the FBI, local law enforcement, and other civilian agencies? Or would it be merely redundant, wasteful, and perhaps even counterproductive?

Another key question is how more expansive military intelligence activities would affect Americans' privacy and related liberties. If sacrifices were required, would improvements in security make those sacrifices worthwhile? If the balance did not clearly favor security, should the military intelligence services perhaps be barred from actions that do not directly support the use of military force? If they are not barred, are there clear legal limits on their activities inside the United States? Should there be?

These questions are presented in the midst of an unprecedented effort to organize and harmonize this nation's homeland security activities. They also arise against the background of a deep-seated American tradition of avoiding military entanglement in civilian affairs.

A little history and a brief look at recent developments may help to provide some answers. In this article we first briefly review the deeply enshrined antipathy toward involvement of the military in any aspect of American life. Then we consider the domestic use of military intelligence services from the American Revolution to the Vietnam era, when their extensive deployment for political purposes

---

3. Dep't of Defense, Report to Congress on the Role of the Department of Defense in Supporting Homeland Security (Sept. 2003), at 9, *available at* http://www.dtra.mil/press_resources/publications/deskbook/full_text/Agencies_Documents/index.cfm [hereinafter Supporting Homeland Security].

4. *Id.* NORTHCOM is a new military command with primary responsibility for homeland defense. *See infra*, text at notes 133–146.

provoked a public outcry and congressional, as well as executive, actions to curb them. Next we review legal authorities bearing on this use, and we trace the development since the mid-1990s of special measures to prevent or respond to a terrorist attack on the American homeland. We then consider several current initiatives, responsive to the ongoing terrorist threat, that may invite or at least permit new military intelligence intrusions into domestic affairs. Finally, we take up a modest proposal for new measures that could help strike the right balance between liberty and security—leaving military intelligence services free to support the Pentagon's homeland defense mission, but consigning other aspects of domestic counterterrorism to non-military parts of the law enforcement and intelligence communities.[5]

II. THE DOMESTIC USE OF MILITARY INTELLIGENCE: A VERY CONCISE HISTORY

A. The Military in American Society: A Cautious Embrace

In a 1972 case, the Supreme Court referred to the "traditional and strong resistance of Americans to any military intrusion into civilian affairs."[6] Since the earliest days of the Republic, in fact, Americans have worried about the risks associated with maintaining a standing army and more generally with giving the military a prominent role in civilian life. These concerns were summed up in a 1985 judicial decision:

> Civilian rule is basic to our system of government . . . . [M]ilitary enforcement of the civil law leaves the protection of vital Fourth and Fifth Amendment rights in the hands of persons who are not trained to uphold these rights. It may also chill the exercise of fundamental rights, such as the rights to speak freely and to vote, and create the atmosphere of fear and hostility which exists in territories occupied by enemy forces.
>
> The interest of limiting military involvement in civilian affairs has a long tradition beginning with the Declaration of

5. The Department of Defense distinguishes between "homeland security," a national effort to prevent or reduce United States vulnerability to terrorist attacks, or to assist in the recovery from such an attack, and "homeland defense," the military protection of United States territory, population, and infrastructure against external threats and aggression. *See* Steve Bowman, Homeland Security: The Department of Defense's Role 1–2 (Cong. Res. Serv. Rep. 31-615, 2003). DOD plays a supporting role in the former, a primary role in the latter. *Id. See also* Supporting Homeland Security, *supra* note 3, at 1.

6. Laird v. Tatum, 408 U.S. 1, 15, 92 S. Ct. 2318, 2326 (1972).

> Independence and continued in the Constitution, certain acts of Congress, and decisions of the Supreme Court. The Declaration of Independence states among the grounds for severing ties with Great Britain that the King "has kept among us, in times of peace, Standing Armies without Consent of our Legislature . . . [and] has affected to render the Military independent of and superior to the Civil power." These concerns were later raised at the Constitutional Convention. Luther Martin of Maryland said, "when a government wishes to deprive its citizens of freedom, and reduce them to slavery, it generally makes use of a standing army."[7]

To avoid the military excesses spelled out in the Declaration of Independence, the Framers took care to place overall control of military forces in the hands of a civilian Commander in Chief. Yet at the end of the Civil War the Supreme Court warned that even this precaution might not always suffice:

> This nation . . . has no right to expect that it will always have wise and humane rulers, sincerely attached to the principles of the Constitution. Wicked men, ambitious of power, with hatred of liberty and contempt of law, may fill the place once occupied by Washington and Lincoln; and if this right is conceded, and the calamities of war again befall us, the dangers to human liberty are frightful to contemplate.[8]

The intervention of the judiciary was needed, the Court said, to preserve a proper balance between the political branches and to protect the values set out in the Bill of Rights from improper domestic uses of the military.[9]

B. Domestic Use of Military Intelligence from the Founding to the Modern Era

Despite all these misgivings, military forces, and in particular military intelligence personnel, have been actively involved in homeland security from the very beginning. General George Washington was America's first spymaster. He made extensive use of espionage, counterintelligence, surveillance, and cryptography during the Revolutionary War.[10] These efforts led, for example, to

---

7. Bissonette v. Haig, 776 F.2d 1384, 1387, *aff'd*, 800 F.2d 812 (8th Cir. 1985), *aff'd*, 485 U.S. 264, 108 S. Ct. 1253 (1988).

8. Ex parte Milligan, 71 U.S. (4 Wall.) 2, 125 (1866).

9. *Id.* at 118–24.

10. Joan M. Jensen, Army Surveillance in America, 1775–1980 (1991), at 7–11.

the unmasking of General Benedict Arnold.[11] President Lincoln also relied heavily on military intelligence during the Civil War.[12]

Throughout Reconstruction and afterward, military intelligence gathering continued at home. Such efforts were not for homeland defense in the traditional sense, however, but for law enforcement and political purposes. During the Hayes administration, for example, Army Signal Corps weather observers collected information on labor agitators.[13] In World War I the military conducted extensive domestic surveillance, ostensibly in search of German spies and saboteurs, although ordinary citizens who objected to wartime policies or to the war itself were also targeted.[14] Later the focus shifted to communists, socialists, and pacifists, while the military gradually began to share its domestic surveillance responsibilities with the FBI.[15]

C. Keeping an Eye on Things During the Cold War

The National Security Act of 1947 spelled out, among other things, a structure for overall civilian control of the intelligence community,[16] of which units controlled by the Pentagon comprise by far the largest part. The Director of Central Intelligence (DCI) was named head of the intelligence community and directed to "establish the requirements and priorities to govern the collection of national intelligence."[17] He exercises direct authority only over the CIA, however.[18] Congress was careful to state that the DCI should be a civilian or, if a member of the military, that he would be removed from the control of his parent service.[19]

Separately, the 1947 Act provides that the Secretary of Defense exercises "civilian control" over the military.[20] In consultation with

---

11. *Id.* at 7–9. This earliest history is also recounted in Michael S. Prather, George Washington, America's First Director of Military Intelligence (2002) (unpublished masters thesis, Marine Corps Univ.) (on file with author).

12. Jensen, *supra* note 10, at 25–28; Christopher H. Pyle, Military Surveillance of Civilian Politics, 1967–1970 (1986), at 16–17.

13. Pyle, *supra* note 12, at 18.

14. Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, Final Report, S. Rep. No. 94-755 (1976), *available at* http://www.aarclibrary.org/publib/church/reports/book2/contents.htm [hereinafter Church Committee].

15. *Id.*; Jensen, *supra* note 10, at 201–15.

16. Pub. L. No. 80-253, 61 Stat. 495 (1947) (codified as amended in scattered sections of 10 & 50 U.S.C.).

17. 50 U.S.C. §§ 403(a)(1), 403-3(c)(2) (2000).

18. *Id.* § 403-3(d).

19. *Id.* § 403(c).

20. *Id.* § 401.

the DCI, she manages the operations of DOD intelligence components.[21] These include the National Security Agency, National Geospatial-Intelligence Agency (formerly National Imagery and Mapping Agency), National Reconnaissance Office, Defense Intelligence Agency, and the intelligence elements of the three service branches.[22]

During the 1950s and 60s, federal troops and federalized National Guard forces, accompanied by military intelligence personnel, were deployed to help integrate Southern schools[23] and to help deal with civil disorders in Detroit in 1967 and other cities the following year after the assassination of Dr. Martin Luther King Jr.[24] Throughout this period military intelligence units also continued to collect data on Americans at home who were suspected of involvement in subversive activities.[25] In the late 1960s, the Pentagon compiled personal information on more than 100,000 politically active Americans in an effort to quell civil rights and anti-Vietnam War demonstrations and to discredit protestors.[26] The Army used 1,500 plainclothes agents to watch demonstrations, infiltrate organizations, and spread disinformation.[27] According to one report, the Army had at least one observer at every demonstration of more than twenty people.[28]

The Army's activities were summed up by Senator Sam Ervin:

> Allegedly for the purpose of predicting and preventing civil disturbances which might develop beyond the control of state and local officials, Army agents were sent throughout the country to keep surveillance over the way the civilian population expressed their sentiments about government policies. In churches, on campuses, in classrooms, in public meetings, they took notes, tape-recorded, and photographed people who dissented in thought, word, or deed. This

---

21. *Id.* § 403-5(a).

22. *Id.* § 403-5(b). The operations of these defense intelligence services are spelled out in James E. Meason, *Military Intelligence and the American Citizen,* 12 Harv. J.L. & Pub. Pol'y 541, 547–54 (1989).

23. Jensen, *supra* note 10, at 237–39.

24. Meason, *supra* note 22, at 542–43 n.4.

25. This history is set out in considerable detail in *Improper Surveillance of Private Citizens by the Military*, part of the report of the Church Committee, *supra* note 14, at 785–825, and Pyle, *supra* note 12. *See also* Jensen, *supra* note 10, at 237–47; Meason, *supra* note 22, at 542–43.

26. Church Committee, *supra* note 14, at 789; *see also* Meason, *supra* note 22, at 543.

27. *Military Surveillance: Hearings Before the Subcomm. on Constitutional Rights, Senate Comm. on the Judiciary*, 93d Cong., 2d Sess. 2 (1974) [hereinafter *Military Surveillance Hearings*].

28. Pyle, *supra* note 12, at 186–87.

> included clergymen, editors, public officials, and anyone who sympathized with the dissenters.
>
> With very few, if any, directives to guide their activities, they monitored the membership and policies of peaceful organizations who were concerned with the war in Southeast Asia, the draft, racial and labor problems, and community welfare. Out of this surveillance the Army created blacklists of organizations and personalities which were circulated to many federal, state, and local agencies, who were all requested to supplement the data provided. . . .
>
> The Army did not just collect and share this information. Analysts were assigned the task of evaluating and labeling these people on the basis of reports on their attitudes, remarks, and activities. They were then coded for entry into computers or microfilm data banks.[29]

The Defense Department now describes what happened in the 1960s and 70s as

> a classic example of what we would today call "mission creep." What had begun as a simple requirement to provide basic intelligence to commanders charged with assisting in the maintenance and restoration of order, had become a monumentally intrusive effort. This resulted in the monitoring of activities of innocent persons involved in the constitutionally protected expression of their views on civil rights or anti-war activities. The information collected on the persons targeted by Defense intelligence personnel was entered into a national data bank and made available to civilian law enforcement authorities. This produced a chilling effect on political expression by those who were legally working for political change in domestic and foreign policies.[30]

These activities were not widely known until an Army intelligence officer spelled them out in a dramatic 1970 magazine

---

29. Sam J. Ervin, Jr., *The First Amendment: A Living Thought in the Computer Age*, 4 Colum. Hum. Rts. L. Rev. 13, 37–38 (1972). *See also* Church Committee, *supra* note 14, at 791, 793–94; Meason, *supra* note 22, at 542–43.

30. Office of the Asst. to the Sec. of Defense (Intelligence Oversight), *Mission and History* (n.d.), *available at* http://www.dtic.mil/atsdio/mission.html [hereinafter *Mission and History*], *quoted in* Kate Martin, *Domestic Intelligence and Civil Liberties*, 24 SAIS Rev. 7, 9 (2004).

article.[31] The article provoked several congressional investigations,[32] as well as modest reforms outlined below.

It also precipitated an ACLU class-action suit to stop domestic intelligence collection by the military. The plaintiffs, political activists, claimed that their First Amendment rights of free expression and association were "chilled" by Army surveillance and record collection. They expressed fear that the improper use of information gathered about their political activities could jeopardize their jobs and reputations. They also worried that a far larger number of persons might simply decide not to speak out, to meet with politically active persons, or even to subscribe to political publications. When the case reached the Supreme Court in 1972, the Court ruled that the plaintiffs lacked standing to sue, because "[a]llegations of a subjective 'chill' are not an adequate substitute for a claim of specific present objective harm or a threat of specific future harm."[33]

As a practical matter, of course, if an activist lost her job or was denied a security clearance, she might never learn the reason why. Personal information in military intelligence files was almost impossible to obtain in advance of 1974 amendments to the Freedom of Information Act[34] or the passage of the Privacy Act the same year,[35] unless it was used in a criminal prosecution.

In 1976, the Church Committee, looking into a variety of intelligence community abuses, called the Army program "the worst intrusion that military intelligence has ever made into the civilian

---

31. Christopher H. Pyle, *Conus Intelligence: The Army Watches Civilian Politics,* 1 Wash. Monthly 4 (1970).

32. *Federal Data Banks, Computers, and the Bill of Rights: Hearings Before the Subcomm. on Constitutional Rights, Senate Comm. on the Judiciary,* 92d Cong., 1st Sess. (1971); Staff of the Subcomm. on Constitutional Rights, Comm. on the Judiciary, United States Senate, Army Surveillance of Civilians: A Documentary Analysis, 92d Cong, 2d Sess. (Comm. Print 1972); Report of the Subcomm. on Constitutional Rights, Comm. on the Judiciary, United States Senate, Military Surveillance of Civilian Politics, 93d Cong, 1st Sess. (Comm. Print 1973); *Military Surveillance Hearings, supra* note 27.

33. Laird v. Tatum, 408 U.S. 1, 13–14, 92 S. Ct. 2318, 2325–26 (1972). Newly-appointed Justice William H. Rehnquist cast a deciding vote in the 5–4 decision. As Assistant Attorney General, he had argued before a Senate Judiciary subcommittee the year before that the same suit, then pending in the Court of Appeals, should be dismissed on standing grounds. Frank Askin, *Rehnquist's Story: Chief Justice Has History of Siding with "Big Brother,"* Legal Times, July 15, 2002. Asked by Senator Sam Ervin whether "you feel there are any serious constitutional problems with respect to collecting data on or keeping under surveillance persons who are merely exercising their right of peaceful assembly or petition to redress a grievance," Rehnquist answered, "No." *Id.*

34. Freedom of Information Act and Amendments of 1974, Pub. L. No. 93-502, 88 Stat. 1561 (1974).

35. Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (codified as amended at 5 U.S.C. § 552a (2000 & Supp. I 2001)).

community."[36] It proposed a "precisely drawn legislative charter" that would, *inter alia*, "limit military investigations to activities in the civilian community which are necessary and pertinent to the military mission, and which cannot feasibly be accomplished by civilian agencies."[37] Nearly three decades later, however, no such charter has been adopted.

III. EXECUTIVE AND CONGRESSIONAL RESPONSES TO THE "WORST INTRUSION"

The end of the Vietnam War marked a significant change in the relationship of trust that had long existed between the executive branch, Congress, and the American people. Publication of the Pentagon Papers, the Watergate scandal, and revelations about illegal domestic spying and disruption of political organizations all added to concerns over the military intelligence abuses outlined above. Congress reacted by passing several constraints on domestic (and foreign) intelligence activities. The President then adopted even broader regulations in an effort to forestall further legislative activism. These developments are described briefly below, along with the Pentagon's own relevant regulations and an important background principle that has shaped thinking in this area—the Posse Comitatus Act. Our objective here is to consider whether these statutory and executive initiatives are likely to prevent the kinds of military intelligence abuses that the Church Committee complained about.

A. Legislative Limits on Domestic Intelligence Collection

In 1974, Congress addressed domestic intelligence excesses, both military and civilian, by passing the Privacy Act.[38] In 1978, it passed the Foreign Intelligence Surveillance Act (FISA),[39] which now describes the "exclusive means" for electronic surveillance (if not for other kinds of intelligence collection) by any government agency if a Title III warrant is not obtained.[40] The efficacy of these statutes in

---

36. Church Committee, *supra* note 14, at 792.

37. *Id.* at 310–11.

38. 5 U.S.C. § 552a (2000 & Supp. I 2001). The workings of the Act are spelled out in United States Dept. of Justice, Office of Information and Privacy, Freedom of Information Act Guide and Privacy Act Overview 775–949 (2002); Litigation Under the Federal Open Government Laws 303–344, 417–437 (Harry A. Hammitt, David L. Sobel & Mark S. Zaid, eds., 21st ed. 2002).

39. 50 U.S.C. §§ 1801–1829 (2000 & Supp. I 2001).

40. 18 U.S.C. § 2511(2)(f) (2000). "Title III" refers to the Omnibus Crime Control and Safe Streets Act, id. §§ 2510–2520 (2000), which sets out the

discouraging the improper collection and use of information about individuals and organizations by the military is, however, far from clear.[41]

The Privacy Act generally forbids the maintenance by an agency of any record "describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or . . . unless pertinent to and within the scope of an authorized law enforcement activity."[42] "Individual" for this purpose means a United States citizen or an alien "lawfully admitted for permanent residence."[43] Similar provisions in FISA bar electronic surveillance or physical searches of a United States person "solely upon the basis of activities protected by the first amendment."[44] It might be argued, however, that military intelligence services could legally listen in on a private conversation about the National Rifle Association or the environmental group Greenpeace on grounds that the collection was not "solely" based on the exercise of First Amendment rights.

The Privacy Act also bars the maintenance of personal information by an agency unless it is "relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President."[45] Military intelligence agencies are plainly charged by Executive Order No. 12,333 with collection of information concerning foreign intelligence and counterintelligence,[46] and they are impliedly authorized by FISA to do the same. FISA does require agencies to follow procedures to "minimize the acquisition and retention, and prohibit the dissemination" of nonpublic information about United States persons,[47] except that evidence of a crime may be disseminated for law enforcement purposes.[48] The minimization procedures are

---

procedure for judicial authorization of electronic surveillance for the investigation, prevention, and prosecution of serious crimes.

41. Regarding application of the Privacy Act to military intelligence activities in this country, *see generally* Paul M. Peterson, *Civilian Demonstrations Near the Military Installation: Restraints on Military Surveillance and Other Intelligence Activities,* 140 Mil. L. Rev. 113, 130–44 (1993). Uncertainty about implementation of FISA generally is traced in William C. Banks & M.E. Bowman, *Executive Authority for National Security Surveillance,* 50 Am. U. L. Rev. 1 (2001).

42. 5 U.S.C. § 552a(e)(7) (2000). The history of this provision and controversy surrounding it are described in Steven W. Becker, *Maintaining Secret Government Dossiers on the First Amendment Activities of American Citizens: The Law Enforcement Activity Exception to the Privacy Act,* 50 DePaul L. Rev. 675 (2000).

43. 5 U.S.C. § 552a(a)(2) (2000).

44. 50 U.S.C. §§ 1805(a)(3)(A), 1824(a)(3)(A) (2000).

45. *Id.* § 552a(e)(1).

46. 46 Fed. Reg. 59,941 (1981).

47. 50 U.S.C. §§ 1801(h), 1805(a)(4), 1805(b)(2) (2000).

48. *Id.* § 1801(h)(3).

classified, however, so it is not possible to know precisely what kinds of personal data may be collected, retained, or shared pursuant to a FISA order.[49]

Another Privacy Act provision that is relevant here prohibits the transfer of personal information to other agencies without the consent of the subject, except, *inter alia,* for a "routine use" by the transferee agency that is "compatible with the purpose for which it was collected."[50] Thus, military intelligence services should not expect to receive data that were collected by other agencies for reasons having no bearing on DOD's homeland defense mission. But the Church Committee in 1976 thought the Privacy Act did not bar the military from directly gathering intelligence that is not "relevant" in order to supply it to other agencies.[51]

Individuals about whom information is collected generally have a right under the Privacy Act to inspect agency files and correct any errors about them in those files,[52] and to review any record of disclosures,[53] unless, *inter alia,* the information is properly classified.[54] Yet it may be exceedingly difficult to determine whether such information is in fact properly classified or, for that matter, whether it even exists.[55]

The Privacy Act does require that intelligence agents collecting personal data from human sources identify themselves to potential informants, state the authority for the collection, and describe the uses to which the data will be put.[56] A provision of the Intelligence Authorization Act for Fiscal Year 2005 that would have amended the Privacy Act to allow military intelligence personnel to work undercover was defeated.[57]

The E-Government Act of 2002 requires federal government agencies to prepare "privacy impact assessments" before they develop or procure new information technology or initiate any new collections of personally identifiable information.[58] An assessment must address what information is to be collected, how it will be collected, its intended use, with whom the information will be shared, and what notice, if any, will be provided to individuals described in the

---

49. *See* Banks & Bowman, *supra* note 41, at 89.
50. 5 U.S.C. §§ 552a(b)(3), (a)(7) (2000).
51. Church Committee, *supra* note 14, at 834.
52. 5 U.S.C. § 552a(d).
53. *Id.* § 552a(c)(3).
54. *Id.* § 552a(k)(1).
55. Those difficulties are outlined in Litigation Under the Federal Open Government Laws, *supra* note 38.
56. 5 U.S.C. § 552a(e)(3) (2000).
57. S. 2386, 108th Cong. § 502 (2004).
58. Pub. L. No. 107-347, § 208(b)(1), 116 Stat. 2899, 2921 (2002).

information.[59] Hope that this new law might bring a measure of transparency to the compilation of personalized computer data must be tempered by the fact that impact assessments need only be made public "if practicable,"[60] and that even this requirement may be "modified or waived for security reasons, or to protect classified, sensitive, or private information contained in an assessment."[61] The terms "practicable," "security," and "sensitive" are not defined.

If the collection, use, or transfer of some personal information cannot be revealed because disclosure of either the process or the information itself would jeopardize national security, compliance with the law should at least be subject to non-public oversight procedures. In 1980, Congress amended the National Security Act of 1947 to require the DCI and heads of all entities involved in intelligence activities, including the Defense Department, to keep the House and Senate Select Committees on Intelligence "fully and currently informed" of these activities.[62] In 1991, in response to the Iran-Contra Affair, the President was given the same responsibility.[63] The two congressional committees provide the only systematic oversight outside of the executive branch.

Will these different legislative initiatives reliably curb the kind of abuses by military intelligence witnessed during the Vietnam era? Maybe. Will they prevent unnecessary abridgements of civil liberties by military intelligence using computer technology that members of the Church Committee could not even have imagined thirty years ago? Probably not. Nor, it appears, will executive measures necessarily do so.

B. Executive Measures to Guide Domestic Intelligence Collection

Amid growing efforts by Congress to curb executive excesses and to play a more active role in intelligence, the Reagan administration in 1981 issued Executive Order No. 12,333.[64] In 2004, it is still the basic executive charter for United States intelligence activities. It includes a broad directive to collect intelligence "needed by" the Secretary of Defense "for the performance of [his] duties and responsibilities."[65] The Secretary of Defense is specifically

59. *Id.* § 208(b)(2)(B)(ii).
60. *Id.* § 208(b)(1)(B)(iii).
61. *Id.* § 208(b)(1)(C).
62. Intelligence Oversight Act of 1980, Pub. L. No. 96-450, § 407(b), 94 Stat. 1975, 1981 (1980) (amended 1991).
63. Intelligence Authorization Act, Fiscal Year 1991, Pub. L. No. 102-88, § 602, 105 Stat. 429, 441 (1991) (codified at 50 U.S.C. § 413(a)(1) (2000)).
64. 46 Fed. Reg. 59,941 (1981).
65. *Id.* § 1.4(a).

authorized to collect national foreign intelligence and to conduct counterintelligence at home in cooperation with the FBI,[66] but not "for the purpose of acquiring information concerning the domestic activities of United States persons."[67] On the other hand, the Order permits the collection, retention, and dissemination of "[i]nformation needed to protect the safety of any persons or organizations."[68] Concerning collection techniques, military intelligence services may conduct electronic surveillance but generally not physical searches of United States persons inside the United States.[69] Thus, Executive Order 12,333 is an uncertain guide for military intelligence activities that purports to authorize much but forbid little. Still, it expressly disclaims any authority for acts that would violate the Constitution or statutes, including, presumably, the Posse Comitatus Act, described below.[70]

Within the executive branch, oversight is conducted by the Intelligence Oversight Board[71] for the entire intelligence community and by Inspectors General for most elements of the community.[72] The Pentagon also has an Assistant to the Secretary of Defense for Intelligence Oversight, whose job is to monitor intelligence activities worldwide and investigate questions of their legality or propriety.[73]

After the terrorist bombing of the Alfred P. Murrah Federal Building in Oklahoma City in 1995, President Clinton issued several executive orders dealing with counterterrorism and critical infrastructure protection.[74] These were drawn together and restated

---

66. *Id.* § 1.11(a), (d).

67. *Id.* § 2.3(b).

68. *Id.* § 2.3(d).

69. *Id.* § 2.4. Physical searches may, however, be conducted of military personnel. *Id.* § 2.4(b).

70. *Id.* § 2.8.

71. The Intelligence Oversight Board is a part of the Executive Office of the President. *See* Executive Order No. 12,863, 58 Fed. Reg. 48,441 (1993); Executive Order No. 13,301, 68 Fed. Reg. 26,981 (2003).

72. *See, e.g.*, 5 U.S.C. App. §§ 1–7, 8H, 11 (2000 & Supp. I 2001) (Defense Intelligence Agency).

73. Department of Defense Directive 5148.11, *Assistant to the Secretary of Defense for Intelligence Oversight,* ¶ 4 (May 21, 2004), *available at* http://www.fas.org/irp/doddir/dod/5148_11.pdf; Remarks by George B. Lotz II, Asst. to the Sec. of Defense (Intelligence Oversight) to the Technology and Privacy Advisory Comm., July 22, 2003, *available at* www.sainc.com/tapac/bios/GeorgeLotz.pdf. This office was established in response to the domestic abuses by Army Intelligence during the 1960s. *See Mission and History, supra* note 30.

74. Presidential Decision Directive 39 (June 21, 1995), *available at* http://www.fas.org/irp/offdocs/pdd39.htm (heavily redacted) (official summary available at http://cns.miis.edu/research/cbw/pdd-39.htm) (setting out United States counterterrorism policy in broad terms); Presidential Decision Directive 62 (1998) (Fact Sheet available at http://www.fas.org/irp/offdocs/pdd-62.htm) (describing

in 2000 in the United States Government Interagency Domestic Concept of Operations Plan (CONPLAN),[75] giving lead agency responsibility to the FBI and Federal Emergency Management Agency (FEMA), respectively, for crisis and consequence management.[76] DOD (including, presumably, its intelligence components) is slated for a supporting role in each instance; it may also assist in threat assessment and provide operational and tactical support.[77] FEMA's Federal Response Plan likewise describes the Pentagon as playing a supporting role,[78] as do the Defense Department's own regulations for responding to civil disturbances.[79]

More recently, the 2002 National Strategy for Homeland Security indicated that military support to civil authorities may take the form of "providing technical support and assistance to law enforcement; assisting in the restoration of law and order; loaning specialized equipment; and assisting in consequence management."[80] Presidential Directive/HSPD-5,[81] issued in 2003, and a new National Response Plan,[82] currently under development by the Department of Homeland Security, generally continue this alignment.[83]

---

leadership of counterterrorism efforts); Presidential Decision Directive 63 (May 22, 1998), *available at* http://www.fas.org/irp/offdocs/pdd-63.htm (setting out policy for protection of nation's critical infrastructure).

75. United States Government Interagency Domestic Terrorism Concept of Operations Plan (2000), *available at* http://www.fema.gov/pdf/rrr/conplan/conplan.pdf [hereinafter CONPLAN].

76. "Crisis management is predominantly a law enforcement function" concerned with anticipating, preventing, or resolving a terrorist threat or act. *Id.* at 7. "Consequence management is predominantly an emergency management function . . . to protect public health and safety, restore essential government services, and provide emergency relief." *Id.* at 8. Confusion about overlapping agency responsibilities led to abandonment of these functional distinctions after the 9/11 attacks. *See* Office of Homeland Security, National Strategy for Homeland Security 42 (July 2002) [hereinafter National Strategy].

77. CONPLAN, *supra* note 75, at 4. *See also* Jeffrey Brake, Terrorism and the Military's Role in Domestic Crisis Management: Background and Issues for Congress (Cong. Res. Serv. Rep. 30-938, 2001).

78. FEMA, Federal Response Plan, *Terrorism Incident Annex, available at* http://www.fema.gov/rrr/frp/ ("the Department of Defense (DOD) will activate technical operations capabilities to support the Federal response to threats or acts of WMD terrorism.").

79. *See infra,* text at notes 93–105.

80. National Strategy, *supra* note 76, at 44.

81. Homeland Security Presidential Directive/HSPD-5, *Management of Domestic Incidents* (Feb. 28, 2003), *available at* http://www.fema.gov/pdf/reg-ii/hspd_5.pdf [hereinafter HSPD-5].

82. *See* U.S. Dep't of Homeland Security, Initial National Response Plan (Sept. 30, 2003), *available at* http://www.dhs.gov/interweb/assetlibrary/Initial_NRP_100903.pdf [hereinafter Initial National Response Plan].

83. HSPD-5, *supra* note 81, at ¶(9); Initial National Response Plan, *supra* note

Yet some have argued that in a great crisis the President ought to be prepared to deploy military forces at home in a lead role.[84] Either way, military intelligence services will necessarily be involved.

Does this welter of executive measures provide sufficient clarity and adequate flexibility to respond to the threat of global terrorism? Do provisions for military intelligence activities at home strike a proper balance between security and liberty? Do they provide sufficient transparency and accountability to ensure compliance with them? Uncertainty about the answers to these questions makes us less secure and, possibly, less free.

C. The Posse Comitatus Act as a Background Principle

The 1878 Posse Comitatus Act expressly forbids the use of military forces to "execute the laws," except when expressly authorized by the Constitution or a statute.[85] It has long been thought to limit most military involvement in civilian law enforcement.[86] The Church Committee concluded in 1976 that the Act "would probably prevent the military from conducting criminal investigations of civilians, but . . . would not bear upon other types of investigations."[87] Since that time, however, Congress has enacted an exception to the Act that allows the Secretary of Defense to provide law enforcement officials with "any information collected during the normal course of military training or operations that may be relevant to a violation of any Federal or State law," and to take the needs of such officials into

---

82, at 2.

84. *See, e.g.*, National Comm'n on Terrorism (Bremer Comm'n), Countering the Changing Threat of International Terrorism 39 (2000) ("[I]n extraordinary circumstances, when a catastrophe is beyond the capabilities of local, state, and other federal agencies . . . the President may want to designate DoD as a lead federal agency."); Ashton B. Carter, John M. Deutch & Philip D. Zelikow, *Catastrophic Terrorism: Elements of a National Policy* (Preventive Defense Project Occasional Paper, vol. 1, no. 6, 1998), *available at* http://www.ksg.harvard.edu/visions/terrorism.htm (DOD primacy inevitable). *But see* Advisory Panel to Assess Domestic Response Capabilities to Terrorism Involving Weapons of Mass Destruction (Gilmore Comm'n), Second Annual Report, *Toward a National Strategy for Combating Terrorism* 28 (2000), *available at* http://www.rand.org/nsrd/terrpanel/terror2.pdf (President should "always designate a Federal civilian agency other than the Department of Defense (DoD) as the Lead Federal Agency").

85. 18 U.S.C. § 1385 (2000).

86. The Act and its application are described in Sean J. Kelly, *Reexamining the Posse Comitatus Act: Toward a Right to Civil Law Enforcement,* 21 Yale L. & Pol'y Rev. 383 (2003); Matthew Carlton Hammond, Note, *The Posse Comitatus Act: A Principle in Need of Renewal,* 75 Wash. U. L.Q. 953 (1997); Charles Doyle, The Posse Comitatus Act & Related Matters: The Use of the Military to Execute Civilian Law (Cong. Res. Serv. Rep. 95-964, 1995).

87. Church Committee, *supra* note 14, at 833.

account "to the maximum extent practicable" in the planning and execution of military training or operations.[88] The Secretary may also furnish equipment to law enforcement agencies, along with personnel to operate it, for cases involving foreign or domestic counterterrorism or violation of "[a]ny law, foreign or domestic, prohibiting terrorist activities."[89]

Other statutory exceptions to the Act are potentially much broader. The Stafford Act, for example, gives the President authority to use the armed services in an emergency to perform work "essential for the preservation of life and property."[90] The Insurrection statutes at 10 U.S.C. §§ 331–335 give the President wide latitude to use troops for almost any purpose, including law enforcement, in responding to an actual or threatened terrorist attack. Another statute allows military forces to assist the Justice Department in collecting intelligence or in searches and seizures when it is "necessary for the immediate protection of human life."[91]

These statutory exceptions, designed to furnish maximum flexibility to the executive branch in an emergency, are most striking for their failure to include any meaningful limits—temporal, geographical, or situational—or any means for challenging their invocation. Taken together, they appear to remove any significant Posse Comitatus Act constraints on domestic military intelligence activities. Yet the applicability of the Act has been a source of some confusion, and President Bush, in his 2002 National Strategy for Homeland Security, called for a "thorough review of the laws permitting the military to act within the United States.[92]

D. The Pentagon's Own Regulations

What does the Pentagon believe to be the scope and limits of its domestic intelligence authority? The official answer is contained in

---

88. 10 U.S.C. § 371 (2000).

89. 10 U.S.C. §§ 372, 374 (2000). A related statute barring military personnel from participation in a "search, seizure, arrest, or similar activity unless . . . otherwise authorized by law," 10 U.S.C. § 375 (2000), has been held by one court not to prevent the Naval Intelligence Service from sharing with civilian police information collected in its surveillance of criminal drug activity. Hayes v. Hawes, 921 F.2d 100 (7th Cir. 1990).

90. 42 U.S.C. § 5170b(c) (2000). If the Stafford Act is not, in the strictest sense, an exception to the Posse Comitatus Act, *see* Operational Law Handbook (2004) (Joseph E. Berger, Derek Grimes & Eric T. Jensen eds., 2003), at 369, *available at* https://www.jagcnet.army.mil/laawsxxi/cds.nsf [hereinafter Operational Law Handbook], it is drawn in terms sufficiently broad to allow virtually any action that otherwise would be prohibited.

91. 10 U.S.C. § 382 (2000).

92. National Strategy, *supra* note 76, at 48.

several DOD directives, some of them written long before the threat of international terrorism became a top priority for the defense community.[93]

Two in particular are important here. One directive orders that all DOD intelligence activities "be carried out in strict conformity with the U.S. Constitution, applicable law, E.O. 12,333 [and] other DoD Directives, with special emphasis given to the protection of the constitutional rights and privacy of U.S. persons."[94]

A second, DOD Directive 5240.1-R, sets out fifteen procedures for domestic surveillance of U.S. persons by military intelligence components. It is described in the Army Judge Advocates' Operational Law Handbook as "the *sole authority* for DoD intelligence components to collect, retain, and disseminate intelligence concerning U.S. persons."[95] One of these procedures provides that covert collection is permitted only if "significant" foreign intelligence is sought, the head of the military agency approves, the information is not reasonably obtainable through overt means, and collection is coordinated with the FBI.[96] In addition, the information collected must not concern the "domestic activities" of any United States person,[97] here defined as activities that "do not involve a significant connection with a foreign power, organization, or person."[98] Other procedures contain very broad authorization for retention and dissemination of data.[99] Electronic surveillance, as well as "concealed monitoring," must follow Executive Order 12,333,[100] while physical searches are authorized only against current military personnel.[101] Human intelligence collection may be carried out only against prospective, current, or former military personnel or contractors.[102] Undisclosed collection from a domestic organization

93. Dep't of Defense Directive 3025.15, *Military Assistance to Civil Authorities* (Feb. 27, 1997); Dep't of Defense Directive 5240.1, *DoD Intelligence Activities* (Apr. 25, 1988) [hereinafter DOD Directive 5240.1]; Dep't of Defense Directive 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons* (Dec. 1982) [hereinafter DOD Directive 5240.1-R]; Dep't of Defense Directive 5200.27, *Acquisition of Information Concerning Persons and Organizations Not Affiliated with the Department of Defense* (Jan. 7, 1980). These directives are available at http://www.dtic.mil/whs/directives/corres/dir1.html or http://www.dtic.mil/whs/directives/corres/dir2.html.

94. DOD Directive 5240.1, *supra* note 93, at ¶ 4.1.

95. Operational Law Handbook, *supra* note 90, at 262 (emphasis in original).

96. DOD Directive 5240.1-R, *supra* note 93, at Proc. 2, ¶ E.

97. *Id.* at Proc. 2, ¶ E.1.

98. *Id.* at Proc. 2, ¶ B.3.

99. *Id.* at Procs. 3 and 4.

100. *Id.* at Procs. 5 and 6.

101. *Id.* at Proc. 7.

102. *Id.* at Proc. 9, ¶ C.1.

is barred,[103] while cooperation with law enforcement officials is permitted in the investigation of international terrorist activities.[104]

These procedures appear to limit the collection of United States person data in some instances beyond even what other authorities might permit. Still, they provide neither transparency nor accountability to anyone outside the military.[105]

IV. AN EVOLVING DOMESTIC ROLE FOR MILITARY INTELLIGENCE

The terrorist attacks of September 11, 2001, have led to the development of new strategies for protecting the American homeland. Military forces, including their intelligence components, are heavily involved in some of them. For example, the Pentagon reports that the recently established

> Defense Intelligence Agency's (DIA) Joint Intelligence Task Force–Combating Terrorism (JITF-CT) is DoD's lead national-level intelligence organization for indications and warning, the production of timely all-source intelligence, integration of national-level analytic efforts on all aspects of the terrorist threat, and development and maintenance of an accurate, up-to-date knowledge base on terrorism-related information. The Director, JITF-CT also serves as the DoD focal point and senior Defense Intelligence representative within the Intelligence Community (IC) for terrorist threat warning, proposing and coordinating within the IC promulgation of such warnings to appropriate DoD organizations and combatant commands. The JITF-CT mission continues to evolve in consonance with other organizations involved in homeland defense/security, including NORTHCOM and the Department of Homeland Security, as an appropriate division of labor is worked out and as working relationships and data-sharing arrangements are established.[106]

That evolving division of labor and those working relationships and data-sharing arrangements are the subject of this section.

---

103. *Id.* at Proc. 10, ¶ C.1.b.

104. *Id.* at Proc. 12, ¶ B.1.a.

105. Procedure 15 of DOD Directive 5240.1-R directs Inspectors General and General Counsels of the various intelligence components to seek out and investigate "questionable activities," but it offers no protection for whistleblowers. *Id.* at Proc. 15.

106. Supporting Homeland Security, *supra* note 3, at 9–10. *See also* Dep't of Defense Directive 2000.12, *DoD Antiterrorism (AT) Program* (Aug. 18, 2003), at Encl. 4, *available at* http://www.dtic.mil/whs/directives/corres/html2/d200012x.htm.

Here we review the Pentagon's domestic collaboration with two new counterterrorism institutions, one statutory and one created by executive fiat, along with a new DOD command structure devoted to homeland defense. We also consider DOD's role in the creation of new technology that could help thwart another terrorist attack. Finally, we look at a recent change in the management of military intelligence components. Our job here, as earlier, is to consider whether these developments are likely to make us safer without unnecessarily compromising core American values of privacy.

A. The Pentagon's Relation to the Department of Homeland Security

The Homeland Security Act of 2002 creates a new program, the Directorate for Information Analysis and Infrastructure Protection (IAIP),[107] that is "singularly focused on the protection of the American homeland against terrorist attack."[108] Its mission is to "access, receive, and analyze law enforcement information, intelligence information, and other information from agencies of the Federal Government, State and local government agencies . . . and private sector entities," to integrate that information, and then to disseminate it to the same agencies and entities.[109] Those agencies—both collectors and consumers of information—include the military intelligence services.[110]

The Act authorizes the Secretary of Homeland Security to enter into cooperative agreements with heads of other agencies, such as DIA, to detail personnel to the IAIP Directorate to perform "analytic

---

107. Pub. L. No. 107–296, §201, 116 Stat. 2135, 2145–2147 (2002).

108. Letter from Thomas J. Ridge, Secretary, Dep't of Homeland Security et al. to Senators Susan M. Collins and Carl Levin (Apr. 13, 2004), *available at* http://levin.senate.gov/newsroom/supporting/2004/041304TTICresponse.pdf [hereinafter Letter from Thomas J. Ridge].

109. Pub. L. No. 107–296, §201(d), 116 Stat. 2135, 2145–2148 (2002). Some details of IAIP's operations are set forth in *The Department of Homeland Security's Information Analysis and Infrastructure Protection Budget Proposal for Fiscal Year 2005: Joint Hearing Before the Subcomm. on Infrastructure and Border Security and the Subcomm. on Intelligence and Counterterrorism of the House Select Comm. on Homeland Security,* 108th Cong. (Mar. 4, 2004) (testimony of Frank Libutti, Under Secretary of Homeland Security for Information Analysis and Infrastructure Protection). A critique of the Directorate may be found at Democratic Members of the House Select Comm. on Homeland Security, America at Risk: Closing the Security Gap 1-11 (Feb. 2004).

110. Not all data will be shared with every contributing entity. Classified information and sources, for example, cannot be revealed to state and local law enforcement agencies or first responders, and such data should not be given to other federal officials who have no legitimate need for it. *See* Bowman, *supra* note 5, at 3.

functions and related duties."[111] Thus, military personnel may furnish as well as receive a variety of information while serving with the IAIP.

The Defense Science Board has urged DOD to share with DHS (and also with the Justice Department and the CIA) "the entire repository of information" available to it, not just "traditionally shared intelligence."[112] It reasons that "DoD has information other than traditional foreign intelligence that is essential for others engaged in homeland security,"[113] although it does not indicate what that information might be. It also suggests that "DoD requires information from others, such as providers of domestic intelligence, in order to execute its homeland defense and homeland security responsibilities," but it proposes no limits on the scope of information received.[114]

While the Homeland Security Act expresses the "sense of Congress" that nothing in it "should be construed to alter the applicability" of the Posse Comitatus Act,[115] there is no other reference in the 2002 legislation to any limits on the military's domestic collection and use of personal information.

In a move to clarify and implement the statute, Homeland Security Presidential Directive/HSPD-5, issued in 2003, provides that the Secretary of Homeland Security is to be the "principal Federal official for domestic incident management" and is to coordinate the actions of other agencies involved.[116] The directive also specifies that the Attorney General is to have "lead responsibility for criminal investigations of terrorist acts or . . . threats,"[117] while the Secretary of Defense is directed to furnish support to civil authorities for domestic incidents.[118] DHS is currently developing a National Response Plan to replace the earlier Federal Response Plan and CONPLAN.[119]

DHS is unique among agencies in having statutorily mandated oversight offices for privacy and for civil rights and civil liberties.[120] These offices may provide a public window into at least some of DOD's intelligence services as they interact with the new department.

---

111. Pub. L. No. 107-296, § 201(f), 116 Stat. 2135, 2148 (2002).
112. Defense Science Board, DoD Roles and Missions in Homeland Security 9–10 (Nov. 2003).
113. *Id.* at 10.
114. *Id.*
115. Pub. L. No. 107-296, § 886, 116 Stat. 2135, 2248 (2002).
116. HSPD-5, *supra* note 81, at ¶ (4).
117. *Id.* at ¶ (8).
118. *Id.* at ¶ (9).
119. Initial National Response Plan, *supra* note 82.
120. Pub. L. No. 107-296, §§ 222 and 705, 116 Stat. 2135, 2155 and 2219 (2002), respectively.

B. TTIC: Too Many Cooks in the Kitchen?

The Terrorist Threat Integration Center (TTIC), announced in President Bush's 2003 State of the Union message, is supposed to help avoid the apparent breakdown in information-sharing among agencies that preceded 9/11.[121] It has "the primary responsibility in the [U.S. government] for terrorism analysis (except information relating to purely domestic terrorism) and is responsible for the day-to-day terrorism analysis provided to the President and other senior policymakers."[122] It is intended to "close the 'seam' between analysis of foreign and domestic intelligence on terrorism"[123] and to serve as the government's "hub for all terrorist threat-related analytic work."[124] TTIC does not actively gather intelligence but instead compiles what is collected by various members of the intelligence community and disseminates it again to those members. It may, however, direct the collection of information by other agencies.[125] According to its Director, "TTIC has the primary responsibility for terrorism analysis at the national level. Each of the other elements has responsibility for doing analysis in support of their respective missions and operational requirements."[126] It also maintains a database of known and suspected terrorists that is available to federal and non-federal officials.[127]

Because it looks at foreign as well as domestic terrorist threats, TTIC may have a broader "customer base" than the Department of Homeland Security's Directorate of Information Analysis and Infrastructure Protection (IAIP), described above. Regarding domestic threats from foreign sources, however, TTIC may be largely redundant (although it expands the domestic intelligence

---

121. *See* News Release, The White House, Fact Sheet: Strengthening Intelligence to Better Protect America (Jan. 28, 2003), *available at* http://www.whitehouse.gov/news/releases/2003/01/20030128-12.html [hereinafter White House News Release]. TTIC is described in considerable detail in Letter from John O. Brennan, Director, Terrorist Threat Integration Center, to Rep. John Conyers, Jr. 10–11 (Dec. 4, 2003), *available at* http://www.fas.org/irp/agency/ttic/qfr120403.pdf [hereinafter Letter from John O. Brennan].

122. Letter from Thomas J. Ridge, *supra* note 108, at 1.

123. White House News Release, *supra* note 121.

124. *White House Offers New Details on Terrorism Threat Integration Center,* Inside the Pentagon, Feb. 20, 2003.

125. Letter from John O. Brennan, *supra* note 121, at 40.

126. *Law Enforcement and the Intelligence Community: Panel II of the Tenth Hearing before Nat'l Comm'n on Terrorist Attacks Upon the United States* (Apr. 14, 2004) (statement of John O. Brennan), *available at* http://www.9-11commission.gov/archive/hearing10/9-11Commission_Hearing_2004-04-14.pdf.

127. Letter from John O. Brennan, *supra* note 121, at 42.

role of the DCI), and it may actually have hampered the establishment of IAIP as the main entity to "connect the dots."[128] More troubling, "there is still confusion within the federal government and among state and local governments about the respective roles of the TTIC, TSC [the FBI's Terrorist Screening Center], and the Information Analysis (IA) component of IAIP."[129]

A Senate committee complained recently that

> [a]lthough TTIC was established to bring intelligence data from across the Intelligence Community together at one location, many analysts at TTIC are still burdened by the same information restrictions that inhibited their work at their parent agency—working under a collage of minimization procedures, parent organization legal authorities and policy barriers, and perceived limitations that still inhibit real all-source intelligence analysis.[130]

The committee may have been referring to the military intelligence services, with which TTIC interacts strongly. About one-quarter of TTIC's staff will be furnished by DOD, including representatives from the Defense Intelligence Agency, National-Geospatial Intelligence Agency, and National Security Agency working in its offices.[131]

Military intelligence personnel are both suppliers and recipients of information in this setting, and they may become involved in the traffic of personal data that have no relevance to the military's homeland defense mission. Aside from DOD's own regulations, there may be no constraints on this traffic, since TTIC lacks legislative limits, an oversight machinery of its own, or a charter that would impose such constraints.[132]

---

128. Democratic Members of the House Select Comm. on Homeland Security, *supra* note 109, at 2; *but cf.* Letter from John O. Brennan, *supra* note 121, at 18.

129. Office of Inspector General, Dept. of Homeland Security, Review of the Status of Department of Homeland Security Efforts to Address Its Major Management Challenges 23 (Mar. 2004). *See also* Democratic Members of the House Select Comm. on Homeland Security, *supra* note 109, at 1–2.

130. S. Rep. No. 108-258 (2004), *available at* http://www.fas.org/irp/congress/2004_rpt/s108-258.html.

131. Letter from John O. Brennan, *supra* note 121, at 10–11. *See also* Supporting Homeland Security, *supra* note 3, at 11.

132. *See The Terrorist Threat Integration Center (TTIC) and Its Relationship with the Departments of Justice and Homeland Security: Hearing Before the House Comm. on the Judiciary and House Select Comm. on Homeland Security,* 108th Cong. (2003) (statement of Jerry Berman, Pres., Center for Democracy & Technology), *available at* http://www.house.gov/judiciary/berman072203.pdf; Letter from John O. Brennan, *supra* note 121, at 41.

C. NORTHCOM: Reorganizing for Homeland Security

When the Pentagon announced in early 2002 that it was creating a new Northern Command (NORTHCOM) based in Colorado[133] to assist in homeland defense, it said its mission would be restricted to protecting America from foreign adversaries and assisting civilian authorities in recovering from another terrorist attack at home.[134] While that mission gives it "a strong rationale for access to information collected by various intelligence and law enforcement agencies,"[135] it also raises questions about safeguards on the use of that information.

In fact, NORTHCOM has its own extensive domestic intelligence operation. NORTHCOM intends to collect and "fuse intelligence and law enforcement information" and then disseminate it to "a wide spectrum of users that consist of folks from first responders all the way up the national command authority."[136] To this end, personnel from the FBI, CIA, NSA, DIA, and other intelligence agencies maintain offices at NORTHCOM and receive daily briefings on potential terrorist threats.[137] In at least some respects, this function of NORTHCOM appears to substantially duplicate the activities of both TTIC and the Department of Homeland Security's IAIP.[138]

NORTHCOM is also involved in direct intelligence collection. General Ralph Eberhart, NORTHCOM's commander, has stated, "we are not going to be out there spying on people," but added, "we get information from people who do."[139] He may have been referring to a new Pentagon organization called Counterintelligence Field Activity (CIFA).[140] CIFA is charged to maintain "a domestic law enforcement

---

133. Some information about the new command may be found at http://www.northcom.mil.

134. *See* U.S. Northern Command, *Who We Are—Mission* (n.d.), *at* http://www.northcom.mil/index.cfm?fuseaction=s.who_mission.

135. Christopher Bolkcom et al., Homeland Security: Establishment and Implementation of Northern Command 5 (Cong. Res. Serv. Rep. RS21322, 2003), *available at* http://www.fas.org/man/crs/RS21322.pdf.

136. *Homeland Defense: Old Force Structures for New Missions: Hearing Before the Subcomm. on National Security, Veterans' Affairs, and Int'l Relations of the House Comm. on Govt. Reform*, 108th Cong. (2003) (statement of Edward Anderson III, Dep. Comm., U.S. Northern Command, Northern Aerospace Defense Command), *available at* 2003 WL 2008258 (F.D.C.H.). *See also* Jim McGee & Caitlin Harrington, *In the Mountains of Colorado, the Pentagon Grows a Big New Homeland Intelligence Center*, CQ.com, Oct. 22, 2003.

137. Kaye Spector, *Military Commander Aims to Stay Steps Ahead of Potential Terrorism*, The Plain Dealer (Cleveland), Apr. 6, 2004, at A8.

138. *See supra*, text at notes 108–119 and 121–127.

139. Interview by Dan Sagalyn with Ralph Eberhart, on "The News Hour," PBS (Sept. 27, 2002), *available at* http://www.pbs.org/newshour/terrorism/ata/eberhart.html.

140. CIFA was established by Dep't of Defense Dir. 5105.67, *DoD Counterintelligence Field Activity* (Feb. 19, 2002), *available at*

database that includes information related to potential terrorist threats directed against the Department of Defense."[141] It also has a "clear-cut intelligence analysis responsibility, which includes the fusion of intelligence, law enforcement, and other domestic (e.g., medical) information into all-source, predictive, and actionable threat assessments."[142] CIFA is engaged in "close collaboration and partnering with other organizations in the national intelligence and investigative community," for example, by furnishing a counterintelligence support team to the FBI.[143] Moreover, it has been directed to develop a data mining capability that may resemble the much maligned Total Information Awareness program, described below.[144]

In March 2004, the Wall Street Journal reported that a CIFA agent sought a videotape of a University of Texas Law School conference attended by "three Middle Eastern men" who had made "suspicious remarks."[145] The Army later called that request "inappropriate."[146] What the Army has not yet done is to spell out clearly what kinds of data can appropriately be collected by CIFA, how they will be collected, and the uses to which they will be put.

D. Total Information Awareness and Its Progeny

Many were wary when John Poindexter[147] appeared in 2002 as head of a new program at the Pentagon's Defense Advanced Research Projects Agency (DARPA) called Total Information Awareness

---

http://www.fas.org/irp/doddir/dod/d5105_67.htm.

141. Dep't of Defense Dir. 2000.12, *DoD Antiterrorism (AT) Program*, Encl. 6, ¶ E6.1.2 (Aug. 18, 2003), *available at* http://www.dtic.mil/whs/directives/corres/html/200012.htm.

142. Supporting Homeland Security, *supra* note 3, at 11.

143. *Id.* at 10.

144. *Id.* at ¶ E6.1.5.

145. Robert Block & Gary Fields, *Is Military Creeping Into Domestic Spying and Enforcement?*, Wall St. J., Mar. 9, 2004, at B1.

146. *See* Press Release, U.S. Army Intelligence and Security Command, INSCOM Concludes Review of Events at University of Texas Law School (Mar. 12, 2004), *available at* http://www.fas.org/irp/news/2004/03/inscom031204.pdf.

147. Poindexter was the National Security Adviser in the Reagan administration who appeared to be at the center of the Iran-Contra Affair. His conviction for obstruction of a congressional inquiry, false statements, and destruction of documents was overturned on appeal on grounds that it might have been based on immunized testimony given to a joint congressional committee investigating the affair. United States v. Poindexter, 951 F.2d 369 (D.C. Cir. 1991). The entire affair is traced in Theodore Draper, A Very Thin Line: The Iran-Contra Affairs (1991); Stephen Dycus et al., National Security Law 473–522 (3d ed. 2002); and Lawrence E. Walsh, Final Report of the Independent Counsel for Iran/Contra Matters (1993).

(TIA).[148] Developed in collaboration with the Army's Intelligence and Security Command, TIA was officially described as

> a research and development program that will integrate advanced collaborative and decision support tools; language translation; and data search, pattern recognition, and privacy protection technologies into an experimental prototype network focused on combating terrorism through better analysis and decision making.[149]

In practical terms, it was supposed to enable intelligence officials to "data-mine an indefinitely expandable universe of databases" in order to "analyze, detect, classify, and identify foreign terrorists."[150] Collecting data from government as well as public and private sources, TIA programs would automatically recognize patterns of behavior, like the purchase of bomb-making materials, or improbable medical activity, such as treatment for anthrax symptoms, that might suggest terrorist activity. These programs would also use biometric recognition technologies to identify individuals by, for example, their facial features or walking gait. And they would do all this on a continuing, real-time basis in order to provide prompt warnings of potential terrorist threats.

DARPA is not an intelligence agency, and it does not collect intelligence. Products developed by DARPA are used not only by the military, but also by other agencies and consumers outside the government. (For example, DARPA, not Al Gore, invented the Internet.) Moreover, data-mining technologies are in use or under development in at least six other agencies.[151] Still, the Defense Department's association with a program to compile extensive electronic records on the American public—telephone calls, social

---

148. The program is described in Dep't of Defense Advanced Research Projects Agency, Report to Congress Regarding the Terrorism Information Awareness Program: In Response to Consolidated Appropriations Resolution, 2003, Pub. L. No. 108-7, Div. M, § 111(b) (May 20, 2003), *available at* http://www.epic.org/privacy/profiling/tia/may03_report.pdf [hereinafter Report to Congress on TIA]; Gina Marie Stevens, Privacy: Total Information Awareness Programs and Related Information Access, Collection, and Protection Laws 1 (Cong. Res. Serv. Rep. 31-730, 2003); Dep't of Defense Advanced Research Projects Agency, Overview of the Information Awareness Office (Aug. 2, 2002), *available at* http://www.fas.org/irp/agency/dod/poindexter.html; and Dep't of Defense Advanced Research Projects Agency, DARPA's Information Technology Initiative on Countering Terrorism (n.d.), *available at* http://www.sainc.com/tapac/library/TerrorismInformationOverview.pdf.

149. Report to Congress on TIA, *supra* note 148, Executive Summary at 1.

150. Stevens, *supra* note 148, at 1. Confusion about the goals of TIA is described in Technology and Privacy Advisory Committee (TAPAC), Safeguarding Privacy in the Fight Against Terrorism 15–20 (Mar. 2004) [hereinafter TAPAC].

151. Stevens, *supra* note 148, at 3.

interactions, bank transactions, medical data, credit card purchases, and more—struck some as particularly threatening. Others expressed concern that the contemplated use of the technology for domestic law enforcement seemed inconsistent with the Posse Comitatus Act.[152]

In an effort to allay public fears, DARPA renamed the program Terrorism Information Awareness. But without clear limits on targeting or on sharing of information (DARPA said the program would rely on existing laws and developing technology to protect privacy and civil liberties), Congress barred its deployment in early 2003, at least against United States persons inside the United States, pending a report to Congress on how it balanced security against privacy.[153] Then in the FY 2004 DOD Appropriations Act Congress eliminated funding for the majority of TIA's program components.[154]

Yet in December 2003 a number of DOD commands and intelligence services were continuing to develop and test TIA technologies.[155] TIA also appears to live on in programs like Novel Intelligence from Massive Data (NIMD), another device for analyzing giant databases now resident in an obscure agency housed at NSA headquarters called Intelligence Community Advanced Research and Development Activity (ARDA).[156] NIMD is supposed to be capable of processing a "petabyte" or more of data, an amount equal to forty pages of text for every member of the human race.[157]

A different agency controlled by the Pentagon, the National Geospatial-Intelligence Agency (formerly National Imagery and Mapping Agency), is currently using satellite surveillance to conduct what it calls an "urban data inventory" that describes physical features throughout the country down to the house level.[158] If home ownership or residency records were integrated into the mapping database, together with data about national origin and political affiliation, it could help to keep track of the movements of individuals for reasons having nothing to do with either homeland defense or homeland security.

---

152. *See, e.g.*, Letter from Sen. Chuck Hagel to Joseph E. Schmitz, Inspector General, Dept. of Defense (Dec. 2, 2002), *reproduced in* Department of Defense, Office of the Inspector General, Information Technology Management: Terrorism Information Awareness Program (Dec. 12, 2003) [hereinafter Information Technology Management].

153. Pub. L. No. 108-7, Div. M, § 111(b), 117 Stat. 11, 534–36 (2003).

154. Pub. L. No. 108-87, § 8131, 117 Stat. 1054, 1102 (2003). A useful critique may be found in Information Technology Management, *supra* note 152.

155. Information Technology Management, *supra* note 152, at 2.

156. *See* Advanced Research and Development Activity, *Novel Intelligence from Massive Data, at* http://ic-arda.org/Novel_Intelligence/index.html.

157. Michael J. Sniffen, *Controversial Terror Research Lives On,* Associated Press, Feb. 23, 2004.

158. William M. Arkin, *Mission Creep Hits Home,* L.A. Times, Nov. 23, 2003, at M2. *See also* Supporting Homeland Security, *supra* note 3, at 10–11.

Whenever a military agency uses military technology (or any other kind, for that matter) to control the collection and use of data, it may be possible automatically to prevent the acquisition of information that is not relevant to the military's homeland defense mission. Any data collected might have personally identifiable information suppressed, unless and until an apparent terrorist threat is detected.[159] Then, some say, intelligence personnel should obtain a Title III warrant or FISA order to discover the identity of persons concerned.[160] There is wide agreement that such programs ought to create tamper-proof audit trails and be subjected to vigorous oversight.[161] Nevertheless, there is no indication that data mining programs currently in use by military intelligence components do any of these things.

E. A New DOD Intelligence Secretariat

The 2003 DOD Authorization Act created a new Under Secretary of Defense for Intelligence.[162] He or she is responsible for coordination and management of all the Pentagon's intelligence services, including the Defense Intelligence Agency, National Security Agency, National Reconnaissance Office, National Geospatial-Intelligence Agency, and the intelligence divisions of the service branches and unified commands, as well as support for homeland defense.[163] The new Under Secretary is also supposed to ensure that the Defense Department has an "effective working relationship" with the Director of Central Intelligence.[164]

Some believe that DOD sought this new position to prevent the loss of control over these agencies to an Intelligence Czar (presumably the DCI), who would operate all intelligence services not strictly military.[165] Others speculate that it will enable the Pentagon

159. This recommendation is set forth in TAPAC, *supra* note 150, at 50; Paul Rosenzweig, *Proposals for Implementing the Total Information Awareness System* 2, 14 (Heritage Fdn. Legal Memorandum No. 8, Aug. 7, 2003).

160. TAPAC, *supra* note 150, at 52; Rosenzweig, *supra* note 159, at 15–16.

161. TAPAC, *supra* note 150, at 50, 52–53, 55; Rosenzweig, *supra* note 159, at 19–22.

162. Pub. L. No. 107-314, § 901, 116 Stat. 2458, 2465 (2002).

163. *See* Deputy Sec. of Defense Paul Wolfowitz, Excerpt of Memorandum: Implementation Guidance on Restructuring Defense Intelligence – and Related Matters (May 8, 2003), *available at* http://www.intelligence.gov/0-usdi_memo.shtml; Supporting Homeland Security, *supra* note 3, at 3.

164. Supporting Homeland Security, *supra* note 3, at 3.

165. *See, e.g.*, Linda Robinson, *In the Intelligence Wars, A Pre-emptive Strike by the Pentagon Surprises Many in Congress*, U.S. News & World Rep., Aug. 12, 2002, at 18. *See also* Chris Strohm, *Defense Officials Oppose Overhaul of Intelligence Community*, GovExec.com, Apr. 7, 2004, *at*

to exert greater influence than previously over a large segment of the intelligence community.[166]

Recent congressional testimony by the current Under Secretary, Stephen A. Cambone, described a "horizontal integration" strategy that includes

> a planned "system-of-systems" that integrates surveillance capabilities across the various human and technical disciplines and national, theater, tactical, and commercial programs. This provides the mechanism to share information across the enterprise—increasing the likelihood that events can be correlated and fused to increase the accuracy, timeliness, and value of intelligence.[167]

Whether the "horizontal integration" and "system-of-systems" will include increased domestic collection and exchange of data by military intelligence services is unclear.

The FY 2003 DOD Authorization Act also created a new Assistant Secretary of Defense for Homeland Defense. This official is responsible for overall supervision of the department's homeland security activities, and she is to serve as the Pentagon's liaison with the Department of Homeland Security and National Security Council.[168] The division of responsibilities between the two new secretariats regarding domestic counterterrorism intelligence has not yet been revealed, however.

VI. CONCLUSION: "GOVERNMENTS LONG ESTABLISHED SHOULD NOT BE CHANGED FOR LIGHT AND TRANSIENT CAUSES"[169]

We have no direct evidence that the military intelligence services today are listening in on Americans' phone conversations, reading our email, tracking our contributions to charities, or infiltrating activist organizations. But in the current climate of fear spawned by the attacks of September 11, and given the Defense Department's commitment to keep us safe from another attack, it could happen again.[170] It would simply be naïve to ignore the lessons of the 1960s.

---

http://www.govexec.com/dailyfed/0404/040704c1.htm.

166. *See* Vernon Loeb, *New Intelligence Post Consolidates Rumsfeld's Clout,* Wash. Post, Nov. 18, 2002.

167. *Intelligence, Surveillance & Reconnaissance: Hearing Before the Strategic Forces Subcomm. of the Senate Armed Services Comm.,* 108th Cong. (2004) (statement of Stephen A. Cambone, Under Secretary of Defense for Intelligence).

168. Pub. L. No. 107-314, § 902(a), 116 Stat. 2458, 2621 (2002). *See* Supporting Homeland Security, *supra* note 3, at 2–3.

169. The Declaration of Independence para. 2 (U.S. 1776).

170. Some potential dangers are described in Richard H. Kohn, *Using the*

There is nothing "light and transient" about the threat of another terrorist attack, of course. Maybe an adjustment in our thinking about the appropriate domestic role of military intelligence is needed. If so, it should follow a determination that strengthening and refining the civilian intelligence agencies will not accomplish the same purpose. We should also be satisfied that the Department of Homeland Security's IAIP or TTIC could not furnish all the data needed for domestic military operations. Any such adjustment should be the product of a robust public debate, probably culminating in legislation.

If we do accept such a change, we must also adopt reliable controls and measures to provide accountability. We might, for example, want to require the approval of a neutral magistrate, say one specially trained in security matters, for military investigations where a Title III warrant or FISA order would not be required. We might want to strictly limit the dissemination of military intelligence information based on particular defined needs, or to limit the acquisition of data by military intelligence components to matters bearing directly on homeland defense. And we might require a periodic review of such data in military intelligence agency files in order to expunge whatever is not accurate and currently relevant to the agency's mission. Finally, we ought to have some clear idea about when we can expect to abandon these changes and return to earlier understandings.

Even if no important changes are adopted, we urgently need to clarify our current understandings about how military intelligence activities at home should affect the balance between security and liberty. A recent Congressional Research Service report argues that the "main stumbling block" to better coordination and response between the FBI and the military is the "numerous and often confusing statutory and regulatory authorities that govern the use of the military in a domestic situation."[171] Clarifying these authorities, it says, could allow a more effective use of military forces while ensuring respect for civil liberties and law enforcement concerns.[172] The same could be said for almost every law, directive, executive order, and regulation touching the domestic work of military intelligence. If we fail to clearly articulate and harmonize these various authorities we will be more vulnerable than we need to be to another terrorist attack. We will also invite well-meaning compromises to some of our most treasured American values.

Military at Home: Yesterday, Today, and Tomorrow, 4 Chi. J. Int'l L. 165 (2003).

171. Brake, *supra* note 77, at 20.

172. *Id.*