WATCHING THE WATCHERS: SURVEILLANCE, TRANSPARENCY, AND POLITICAL FREEDOM IN THE WAR ON TERROR

Seth F. Kreimer[*]

> Like other totalitarian movements, the terrorists seek to impose a grim vision in which dissent is crushed, and every man and woman must think and live in colorless conformity.[1]

INTRODUCTION: "TEAR DOWN THE WALLS"

If one insight apparently transcends the current partisan rancor, it is that the effort to secure America against terrorist attacks requires better intelligence. And if one consensus candidate emerges as the prerequisite for that improvement, it is that the intelligence services should gather more information and share it more widely. The Senate Select Committee on Intelligence Joint Investigation Inquiry into September 11 identified the failure to share intelligence as a systematic flaw that exposed the United States to terrorist attacks.[2] The Attorney General regularly inveighs against the "impediments to communication and information sharing among the men and women charged with keeping America safe."[3] The non-partisan Markle Foundation Task Force has advocated improved sharing of information as the precondition to more effective homeland security,[4] a rec-

[*] Kenneth W. Gemmill Professor of Law, University of Pennsylvania. This paper was originally delivered at the "Homeland Security and Civil Liberties" conference jointly hosted on June 18, 2004 by the University of Pennsylvania Law School and the Army War College. It has benefited from the comments of the participants at that conference, as well as the perceptive analysis of M.E. Bowman, Lara Flint, Jonathan Fredman, Mitch Marcus, Kim Scheppele, and Polk Wagner, and the superb research assistance of Mihir Kshirsigar. They have my deep thanks, while I retain all responsibility for errors or omissions that remain.

[1] President George W. Bush, Remarks at the United States Air Force Academy Graduation Ceremony (June 2, 2004), http://www.whitehouse.gov/news/releases/2004/06/20040602.html.

[2] *E.g.*, *September 11 Intelligence Failures: Hearing Before the J. S. & House Select Intelligence Comm.*, 107th Cong. (2002) (statement of Eleanor Hill, Staff Director, Joint Inquiry Staff), http://www.fas.org/irp/congress/2002_hr/100102hill.pdf.

[3] *E.g.*, U.S. Attorney General John Ashcroft, Remarks Regarding the Intelligence Sharing Initiative at the Department of Justice (May 14, 2004) (transcript available from the Federal News Service at http://www.fnsg.com).

[4] MARKLE FOUND. TASK FORCE, CREATING A TRUSTED NETWORK FOR HOMELAND SECURITY 2 (2003) [hereinafter MARKLE REPORT] (stressing the importance of information sharing and analysis), http://www.markletaskforce.org/Report2_Full_Report.pdf.

ommendation joined by the Defense Department's Technology and Privacy Advisory Committee.[5] The General Accounting Office similarly reports that "homeland security" requires increased interpretation of intelligence.[6]

This urge to share information has generated an efflorescence of efforts to gather, swap, and agglomerate data. In law enforcement, the USA PATRIOT Act and Justice Department rule-making have famously "torn down the walls" separating foreign intelligence and domestic law enforcement.[7] The Justice Department has established the framework for a National Criminal Intelligence Sharing Plan among state and local law enforcement agencies.[8] The FBI seeks to develop "a single, integrated information space, in which the default

[5] TECH. AND PRIVACY ADVISORY COMM., DEP'T OF DEFENSE, SAFEGUARDING PRIVACY IN THE FIGHT AGAINST TERRORISM 6 (2004) [hereinafter TAPAC REPORT] ("[W]e believe a uniform system of laws and technology measures to facilitate data mining and information sharing without compromising the privacy of U.S. persons is essential."), http://www.sainc.com/tapac/TAPAC_Report_Final_5-10-04.pdf.

[6] U.S. GEN. ACCOUNTING OFFICE, REP. NO. GAO-03-760, HOMELAND SECURITY: EFFORTS TO IMPROVE INFORMATION SHARING NEED TO BE STRENGTHENED 29–31 (2003) ("If [the Department of Homeland Security] does not effectively strengthen efforts to improve the information-sharing process, the nation's ability to detect or prepare for attacks may be undermined."), *available at* http://www.gao.gov/new.items/d03760.pdf (last visited Sept. 30, 2004).

[7] U.S. Attorney General John Ashcroft, Preserving Life and Liberty, Prepared Remarks at the American Enterprise Institute (Aug. 19, 2003) ("[I]n the Patriot Act, Congress began to tear down the walls that cut off communication between intelligence and law enforcement officials."), http://www.usdoj.gov/ag/speeches/2003/081903remarksataeifinal.htm.

[8] Ted Leventhal, *Officials Announce Plan to Share Terrorism Intelligence*, May 14, 2004, *at* http://govexec.com/dailyfed/0504/051404tdpm1.htm (last visited Sept. 17, 2004). *See* GLOBAL JUSTICE INFO. SHARING INITIATIVE INTELLIGENCE WORKING GROUP (GIWG), DEP'T OF JUSTICE, NATIONAL CRIMINAL INTELLIGENCE SHARING PLAN iii–viii (2004) [hereinafter SHARING PLAN] (summarizing the report's recommendations), *available at* http://it.ojp.gov/documents/National_Criminal_Intelligence_Sharing_Plan.pdf; Press Release, Dep't of Justice, Attorney General Ashcroft Announces Implementation of the National Criminal Intelligence Sharing Plan (May 14, 2004) (describing the initiative as designed to link federal, state, and local law enforcement agencies so that they can share intelligence information to prevent terrorism and crime), http://www.fbi.gov/dojpressrel/pressrel04/natlsharing051404.htm. For more information about current sharing initiatives, see the Global Justice Information Sharing Initiative Web site at http://it.ojp.gov/global.

The *National Criminal Intelligence Sharing Plan* contains recommendations to incorporate privacy guidelines developed by the National Criminal Justice Association. SHARING PLAN at vi. *See* NAT'L CRIMINAL JUSTICE ASSOC., JUSTICE INFORMATION PRIVACY GUIDELINE (2002), http://www.ncja.org/pdf/privacyguideline.pdf (last visited Sept. 30, 2004). The Sharing Plan also recommends compliance with the privacy protection mandates of 28 C.F.R. § 23 (2003). One difficulty here is that section 23 embodies a "reasonable suspicion" requirement, § 23.20(a), a direct relationship requirement for First Amendment related records, § 23.30(b), and "need to know" limitations, § 23.20(e), (g). The "protections" of civil liberties which the Attorney General touts as part of the Sharing Plan thus appear to include exactly the "roadblocks" he purports to seek to remove. On the other hand, the Sharing Plan suggests that section 23 "is currently pending revision" in light of "the speed of which technology changes, the nature of the new threat to public safety (exemplified by terrorism), and the critical need to facilitate information sharing among all levels of government." SHARING PLAN at 14.

will be to share with agencies,"[9] while the Justice Department is experimenting with a "database that will ultimately be accessible to all participating agencies via secure Internet" linking the databases of state, local, and federal law enforcement authorities.[10] A federally funded program based in Florida is trying to link state public records and private databases into the "Multistate Anti-Terrorism Information Exchange ("MATRIX")."[11]

On the military side, even after the demise of the Defense Advanced Research Projects Agency's ("DARPA") controversial "Total Information Awareness" ("TIA") program,[12] the Commander of

[9] OFFICE OF INSPECTOR GEN., DEP'T OF JUSTICE, REP. NO. 04-10, THE FEDERAL BUREAU OF INVESTIGATION'S EFFORTS TO IMPROVE THE SHARING OF INTELLIGENCE AND OTHER INFORMATION 47 (2003) [hereinafter OIG, FBI'S EFFORTS] (stating that the shared information space is one of the "guiding principles that the FBI expects to apply to its information sharing strategy" in its draft Integrated Information Sharing Plan), *available at* http://www.usdoj.gov/oig/audit/FBI/0410/final.pdf.

[10] Press Release, Dep't of Justice, Attorney General John Ashcroft Unveils Gateway Information Sharing Pilot Project in St. Louis, Missouri (Oct. 9, 2002), http://www.usdoj.gov/opa/pr/2002/October/02_ag_589.htm.

[11] The self-definition of MATRIX can be found at the program's Web site at http://www.matrix-at.org (last visited Sept. 15, 2004). It purports to be "a computerized research tool that electronically queries existing criminal justice records and public and commercial databases." Frequently Asked Questions, MATRIX, *at* http://www.matrix-at.org/faq.htm (last visited Sept. 15, 2004). There is evidence, however, that MATRIX has data mining capabilities. Press Release, Am. Civil Liberties Union, Documents Acquired by ACLU Prove That MATRIX is a Data Mining Program (Jan. 21, 2004), http://www.aclu.org/Privacy/.

The program is based in Florida, overseen by the Florida Department of Law Enforcement, and operated by Sesint, a private firm, which previously generated a list of 120,000 names based on a "terrorism index" comprised of "such factors as age, gender, ethnicity, credit history, 'investigational data,' information about pilot and driver licenses, and connections to 'dirty' addresses known to have been used by other suspects." Brian Bergstein, *Database Measured 'Terrorism Quotient'*, MY WAY, May 20, 2004, http://apnews.myway.com/article/20040520/D82M9B400.html. At this writing, eight of the original thirteen states have withdrawn their cooperation due to privacy concerns. *See* Ryan Singel, *New York, Wisconsin Unplug Matrix*, WIRED NEWS, Mar. 15, 2004, *at* http://www.wired.com/news/privacy/0,1848,62645,00.html (last visited Sept. 17, 2004). There is some indication that federal involvement extends beyond funding. Robert O'Harrow, *Anti-Terror Database Got Show at White House*, WASH. POST, May 21, 2004, at A12 (describing the MATRIX system as "capable of examining records of billions of people in seconds."). TAPAC reports that the Department of Homeland Security is a full MATRIX participant. TAPAC REPORT, *supra* note 5, at 4.

[12] The TIA project was part of the now-disbanded Information Awareness Office headed by retired Admiral John Poindexter. *See* William Safire, *You Are a Suspect*, N.Y. TIMES, Nov. 14, 2002, at A35 ("Attorney General Ashcroft tried his Terrorism and Prevention System (TIPS), but public outrage at the use of gossips and postal workers as snoops caused the house to shut it down."). The far reaching surveillance project sought to establish a capacity to capture the "information signature" of subjects so that the government could track potential terrorists and criminals. *See* Presolicitation Notice BAA02-08, Defense Advanced Research Projects Agency (DARPA) (Mar. 21, 2002) (describing the project and soliciting funding proposals), *at* http://www.darpa.mil/baa/baa02-08.htm. The project's ambitious plans called for creating a "virtual, centralized, grand database" filled with details about the personal lives of all Americans and non-citizens to enable data mining programs to find patterns and associations that might help gather intelligence to preempt terrorist acts. *Id.* The project, with an ominous logo and

Northcom, General Ralph Eberhart, has avowed that "[w]e need to change from the 'need to know' Cold War mentality to the 'need to share,'. . . in this global war on terrorism."[13] A series of initiatives in the military have sought to gather and integrate information about potential terrorist activities from both traditional intelligence sources and "raw non-validated" reports of "anomalous activities."[14] Indeed,

"knowledge is power" as its slogan, attracted a firestorm of criticism from advocacy groups, *e.g.*, Letter from Thirty Civil Liberties Groups to Senators Daschle and Lott (Nov. 18, 2002) (opposing the Total Information Awareness Project), http://www.epic.org/privacy/profiling/tia/tialetter11.18.02.html, and from technical experts who questioned the feasibility of the system, *e.g.*, Letter from U.S. Association for Computing Machinery to Senators Warner and Levin (Jan. 23, 2003) (expressing concerns regarding Total Information Awareness System), http://www.acm.org/usacm/Letters/tia_final.html. Congress reacted by first demanding a report from the office about the projected impact on civil liberties, *see* DARPA, REPORT TO CONGRESS REGARDING TOTAL INFORMATION AWARENESS PROGRAM IN RESPONSE TO CONSOLIDATED APPROPRIATIONS RESOLUTION OF 2003, PUB. L. NO. 108-7, 117 STAT. 11, § 111(B) (2003), and then subsequently by halting funding for the project. *See* Conf. Rep. on H.R. 2658, Department Of Defense Appropriations Act of 2004, H.R. Rep. No. 108-283, 108th Cong., at § 8131(A) (2003) ("Notwithstanding any other provision of law, none of the funds appropriated or otherwise made available in this or any other Act may be obligated for the Terrorism Information Awareness Program."). Meanwhile, the Secretary of Defense initiated a separate review in February 2003 to assess the civil liberties implications of the system, which resulted in the TAPAC Report. TAPAC REPORT, *supra* note 5, at iii. DARPA, however, is not likely to abandon research in data mining software, and the issues will no doubt resurface, even if not as dramatically as with TIA, since the Pentagon is certainly more sensitive to public perception of its activities. *Id.* at 5.

[13] Doug Sample, *Defending the Homeland Is a 'Must Win' Game*, AM. FORCES INFO. SERVICE, Feb. 26, 2004, *at* http://www.defenselink.mil/news/Feb2004/n02262004_200402263.html. This echoes the Northern Command's Chief Information Officer, who earlier announced that "[m]y mantra is that I need to change from a 'need to know' to a 'need to share' foundation." Molly Peterson, *Homeland Defense Commander Stresses 'Need to Share' Information*, Dec. 3, 2002, *at* http://www.govexec.com/dailyfed/1202/120302td1.htm. *See also* William M. Arkin, *U.S. Military: Mission Creep Hits Home*, L.A. TIMES, Nov. 23, 2003, at M2 (quoting General Eberhart as stating that "[w]e are not going to be out there spying on people . . . [w]e get information from people who do," and describing the "Counterintelligence Field Activity," which has been given the mission of data mining public records, credit card accounts, and intercepted communications); Robert Green, *NSA's Wolf Touts Innovation and "Need to Share,"* EFFECTIVE GOV'T IN ACTION, Oct. 31, 2003, *at* http://www.publicsectorinstitute.net/ELetters/EGovernment/v1n6/0097EGv1n6NSA.lsp; William New, *Computer Firm Helps Military Share its 'Trusted' Data*, Jan. 23, 2004 ("[S]ince the Sept. 11, 2001, terrorist attacks, the 'need to know' approach to information has become a 'need to share' philosophy."), *at* http://www.govexec.com/dailyfed/0104/0123oftdpm2.htm.

[14] Brian McWilliams, *DoD Logging Unverified Threats*, WIRED NEWS, June 25, 2003, *at* http://www.wired.com/news/politics/0,1283,59365,00.html. *See* Larry Kahaner, *A Businesslike Approach to Solving Crime*, INFO. WK., Apr. 5, 2004, at G23 (describing Air Force Office of Special Investigations use of "business-intelligence system" to update information "across several databases"); Lt. Joseph K. Kellogg, Jr. & Mark Powell, *Protecting America With Information Technology*, 2003 SIGNAL 35 (describing the development of the "Protect America System" which joins the databases of Northcom, the U.S. Customs Service, the Secret Service, the TSA, the FBI, and others, to share information among current government databases), *at* http://www.afcea.org/signal/articles/anmvier.asp?a=207 (last visited Sept. 16, 2004); *Office of Special Investigations (anti-terrorism efforts)*, *in* TIG BRIEF: THE INSPECTOR GENERAL, Sept 1, 2003, at 9 (describing the Air Force's "Threat and Local Observation Notice" (TALON) system which logs and shares data

parts of the former Total/Terrorism Information Awareness package appear to be funded to go forward under other "off the books" appropriations.[15]

The Intelligence Community is pursuing an initiative on "Novel Intelligence from Massive Data" through its "Advanced Research and Development Activity,"[16] and the Director of the CIA has been mandated to "assess the feasibility and advisability of permitting intelligence analysts of various elements of the intelligence community to access and analyze intelligence from the databases of other elements."[17] The National Aeronautic and Space Administration ("NASA") is seeking to develop a "Data mining and Aviation Security" system that integrates "'the Internet and classified intelligence data' with information from two flight-safety databases,"[18] while immigration and air safety initiatives already are seeking to link a variety of publicly and privately held databases to screen air passengers and immigrants.[19] As the Technology and Privacy Advisory Committee re-

including private reports of "suspicious persons out of place" filed under the Air Force's "Eagle Eyes" private informant program).

[15] Associated Press, *US Still Mining Terror Data*, WIRED NEWS, Feb. 23, 2004 ("Congressional officials declined to say which Poindexter programs were killed and which were transferred, but people with direct knowledge of contracts told AP that the surviving programs included some of 18 data-mining projects known as Evidence Extraction and Link Discovery in Poindexter's research."), *at* http://www.wired.com/news/conflict/0,2100,62390,00.html. *See* TAPAC REPORT, *supra* note 5, at vii (maintaining that data mining tools may be used only outside the United States).

[16] Novel Intelligence from Massive Data, Advanced Res. & Dev. Activity (ARDA) [hereinafter ARDA], *at* http://www.ic-arda.org/Novel_Intelligence/index.html (last visited Sept. 16, 2004).

[17] Intelligence Authorization Act for Fiscal Year 2004, Pub. L. No. 108-177, § 314, 1117 Stat. 2599, 2610, *available at* http://www.fas.org/irp/congress/2003_cr/s1025.html (last visited Sept. 27, 2004).

[18] Noah Shachtman, *NASA's New Antiterrorism Mission*, WIRED NEWS, Jan. 21, 2004, *at* http://www.wired.com/news/privacy/0,1848,61987,00.html.

[19] *See* U.S. GEN. ACCOUNTING OFFICE, REP. NO. GAO-04-385, AVIATION SECURITY: COMPUTER ASSISTED PASSENGER PRESCREENING SYSTEM [CAPPS] FACES SIGNIFICANT IMPLEMENTATION CHALLENGES (2003) (detailing efforts to exempt CAPPS II from Privacy Act protections of relevance and accessibility and failure to establish either accuracy or privacy of screening mechanisms), *available at* http://www.gao.gov/new.items/d04385.pdf (last visited Sept. 30, 2004); Ryan Singel, *Profiling System Takeoff Delayed*, WIRED NEWS, Dec. 12, 2003, *at* http://www.wired.com/news/privacy/0,1848,61553,00.html; Press Release, Dep't of Homeland Security, CAPPS II: Myths and Facts (Feb. 13, 2003) (describing the scope of the air passenger risk assessment scheme that would employ both commercial and government databases), http://www.dhs.gov/dhspublic/display?content=3163.

Implementation of CAPPS II has been scuttled by operational difficulties and the opposition of privacy advocates, but the Transportation Safety Administration has announced that it intends to pursue similar initiatives. Ryan Singel, *Life After Death for CAPPS II?*, WIRED NEWS, July 16, 2004 ("The government's controversial plan to screen passengers before they board a plane is dead—but it may return in a new form."), *at* http://www.wired.com/news/privacy/0,1848,64240,00.html. A similar program to track non-citizens on arrival in the United States is, however, very much alive. Travel and Transportation: US-VISIT, Dep't of Homeland Security (providing information about the screening program that uses biometric technology coupled

cently observed, "TIA was not the tip of the iceberg, but rather one small specimen in a sea of icebergs."[20]

I. A PAGE OF HISTORY

A. *Domestic Surveillance Over Time*

This is not the first time that the American government, faced with the threat of internal disorder, has sought to gather information about American residents. During the Civil War, the executive branch deployed a series of agents to track opposition to its war aims, as well as active Confederate espionage and subversion.[21] While the Posse Comitatus Act of 1878[22] barred the Army from domestic law enforcement and the Anti-Pinkerton Act of 1893[23] limited the federal executive's capacity to employ private undercover agents, during World War I the military again developed a substantial internal surveillance and security apparatus in conjunction with the semi-private American Protective League.[24] The Justice Department established its own Bureau of Investigation to undertake domestic surveillance.[25] Though the domestic military intelligence apparatus was pruned in

with public and private databases for identification and risk assessment of visitors to the United States), *at* http://www.dhs.gov/us-visit (last visited Sept. 16, 2004).

[20] TAPAC REPORT, *supra* note 5, at 5. *See* U.S. GEN. ACCOUNTING OFFICE, REP. NO. GAO-04-548, DATA MINING: FEDERAL EFFORTS COVER A WIDE RANGE OF USES (2004) [hereinafter GAO, DATA MINING] (identifying 199 separate data mining projects by federal agencies, 54 of which use private sector data including DIA and DHS terrorism projects), *available at* http://www.gao.gov/new.items/d04548.pdf (last visited Sept. 30, 2004).

[21] *See, e.g.*, Totten v. United States, 92 U.S. 105, 106 (1875) (noting that the President was "undoubtedly authorized during the war, as commander-in-chief of the armies of the United States, to employ secret agents to enter the rebel lines and obtain information respecting the strength, resources, and movements of the enemy"); *Ex parte* Vallandigham, 68 U.S. 243 (1864) (recounting arrest and conviction of critic of Civil War policies by military tribunal); JOAN M. JENSEN, ARMY SURVEILLANCE IN AMERICA, 1775–1980, at 24–30 (1991) (giving an account of military and civilian initiatives); CHRISTOPHER H. PYLE, MILITARY SURVEILLANCE OF CIVILIAN POLITICS 16–18 (1986) (describing Vallandigham's arrest being carried out by two army captains in civilian clothes).

[22] 18 U.S.C. § 1385 (2000).

[23] 5 U.S.C. § 3108 (2000).

[24] *See* FRANK J. DONNER, THE AGE OF SURVEILLANCE 33 (1980) ("The [Justice] Department's Bureau of Investigation worked closely during the [World War I] years with private patrioteering groups, principally the American Protective League (APL), officially designed . . . for ferreting out spies, slackers, and saboteurs."); JENSEN, *supra* note 21, at 131–32, 147–49 ("The APL developed a quasi-military organization to operate secretly within industries.").

[25] JENSEN, *supra* note 21, at 123, 164–65; Major Paul M. Peterson, *Civilian Demonstrations Near the Military Installation: Restraints on Military Surveillance and Other Intelligence Activities*, 140 MIL. L. REV. 113, 116 (1993) ("World War I, however, brought on the first extensive domestic intelligence operations.").

the aftermath of scandals in the 1920s,[26] both military and civilian authorities maintained at least "passive" surveillance of radicals thereafter.[27] Incipient disruption in the depths of the Depression led the FBI to expand its surveillance of "subversives" and its investigation of "potential crimes" involving national security.[28] With the onset of European hostilities, the looming threats accompanying World War II produced further surveillance to protect critical military resources and allowed the military to reestablish a full-blown internal surveillance program which lasted through the war.[29] The Cold War, in turn, generated an overlapping series of military, civilian and private investigation, and surveillance agencies seeking to uncover and combat Communist infiltration—surveillance that extended to include civil rights groups perceived to be allied with or infiltrated by Communists.[30]

A generation ago, our nation again found itself grappling with the challenge of providing "homeland security" in the face of what was perceived as a rising tide of disorder, subversion, and sabotage.[31] Between 1967 and 1968, the National Guard was mobilized eighty-three times and the Army was called out four times to suppress domestic riots.[32] The Army was mobilized in 1969 and 1970 to control protesters

[26] BRUCE W. BIDWELL, HISTORY OF THE MILITARY INTELLIGENCE DIVISION DEPARTMENT OF THE ARMY GENERAL STAFF: 1775–1941, at 277–79 (1986) (describing domestic military intelligence after 1920); JENSEN, *supra* note 21, at 196–98 (discussing the activities of the Military Intelligence Division); GEORGE J.A. O'TOOLE, HONORABLE TREACHERY 4, 319 (1991) (recounting adverse reaction to surveillance of labor organizers in the state of Washington); David M. Crane, *Divided We Stand: Counterintelligence Coordination Within the Intelligence Community of the United States*, 1995 ARMY LAW. 26, 31 ("The War Department stopped conducting domestic surveillance of alleged radicals after disclosure that the Army was using military intelligence reservists to conduct unofficial intelligence gathering against United States citizens.").

[27] JENSEN, *supra* note 21, at 199–205; Peterson, *supra* note 25, at 116 ("Because stateside counterintelligence agents tended to be underemployed throughout these periods, most were readily available to perform political surveillance. Significantly, the civilian hierarchy that controlled the military often was ignorant about the extent and nature of domestic intelligence gathering.").

[28] DONNER, *supra* note 24, at 52–64.

[29] S. REP. NO. 94-755, bk. II (1976) (describing how the domestic intelligence activities were reinstituted, expanded, and institutionalized during the wartime under FBI director J. Edgar Hoover to include subversives, potential criminals, and even political opponents of the President), *available at* http://old.lib.ucdavis.edu/govdoc/Intelligence/76S9632.pdf (last visited Sept. 30, 2004); JENSEN, *supra* note 21, at 211–29.

[30] S. REP. NO. 94-755, at bk. II; JENSEN, *supra* note 21, at 230–39.

[31] Peterson, *supra* note 25, at 117 (describing disorders and the development by the military of "two parallel and redundant intelligence collecting apparatus . . . with an estimated 1500 intelligence operatives.").

[32] Tatum v. Laird, 444 F.2d 947, 952 (D.C. Cir. 1971) ("In recent years the Army and the National Guard have been called upon to act to preserve peace against violent protests against civil disorders."), *rev'd*, 408 U.S. 1 (1972); *see also id.* at 963 n.6 (MacKinnon, J., dissenting) (quoting Brief of Appellee) ("[D]uring the month of April 1968 alone, there were 237 civil disorders, 27,000 arrests, 43 deaths, over 58 million dollars in property damages, and over 58,000

converging on Washington to protest the Vietnam War.[33] Factions of antiwar radicals moved from draft resistance and civil disobedience, illegal in themselves but posing no physical danger, to active violent attacks on government facilities. In 1969, news media reported over five hundred bombings in the continental United States; the number doubled in 1970.[34] The rate doubled again early in 1971.[35]

In response, the military sought to establish a domestic surveillance mechanism to provide warning and operational intelligence in the event of internal disturbances.[36] It shared the fruits of civilian inquiry and went on to use its own resources to monitor and infiltrate political activities it viewed as potentially threatening and to illegally monitor domestic radio signals.[37] As the Defense Department recounts the story,

> [w]hat had occurred was 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.[38]

National Guard and Army troops had to be used 25 times to quell the civil disturbances."); PYLE, *supra* note 21, at 34–35 (estimating a total of 300,000 soldiers deployed to preserve domestic order between January 1965 and December 1969).

[33] *See* PYLE, *supra* note 21, at 252–53 (describing deployment of twenty thousand federal troops in November 1969); TOM WELLS, THE WAR WITHIN: AMERICA'S BATTLE OVER VIETNAM 512 (1994) ("[May Day] had taken an immense mobilization of armed might and twelve thousand arrests to keep Washington open.").

[34] United States v. U.S. Dist. Ct. (Keith), 444 F.2d 651, 674 n.1 (6th Cir. 1971) (Weick, J., dissenting) ("1096 bombings and 176 attempts were reported in the United States in 1970, against 549 bombings in 1969."), *aff'd*, 407 U.S. 297 (1972).

[35] 407 U.S. at 312 n.12 ("The Government asserts that there were 1,562 bombing incidents in the United States from January 1, 1971, to July 1, 1971, most of which involved Government related facilities.").

By way of comparison, in 2000, the Bureau of Alcohol Tobacco and Firearms (ATF) reported 807 actual or attempted bombings; in 2001, 763; in 2002, 711; and in 2003, 386. Arson & Explosives National Repository, ATF, *at* http://www.atf.gov/aexis2/statistics.htm (last visited Sept. 16, 2004).

[36] *See* S. REP. NO. 94-755, bk. III (1976) (detailing events leading to establishment and expansion of internal surveillance programs), *available at* http://old.lib.ucdavis.edu/govdoc/Intelligence/76S9633.pdf (last visited Sept. 30, 2004).

[37] ATHAN G. THEOHARIS, SPYING ON AMERICANS: POLITICAL SURVEILLANCE FROM HOOVER TO THE HUSTON PLAN 121–22 (1978) (describing illegal monitoring of radio signals).

[38] Mission and History, Assistant to the Secretary of Defense (Intelligence Oversight), Dep't of Defense, *at* http://www.dod.mil/atsdio/mission.html (last visited Sept. 19, 2004).

On the civilian side, the NSA, the CIA, and the FBI deployed conventional investigative techniques against a variety of domestic critics and potential opponents, but engaged as well in break-ins, mail openings, warrantless wiretaps, and covert efforts to discredit groups viewed as potential sources of disruption.[39] The Nixon Administration sought to marshal all of these agencies as well as the Internal Revenue Service ("IRS") and the Defense Intelligence Agency ("DIA") against groups it viewed as threats to "internal security,"[40] claiming as well the right to engage in extraconstitutional searches and seizures.[41]

The Army's Military Intelligence website puts the matter somewhat more succinctly:

"Question: Why do we have intelligence oversight?

Answer: Because MI messed up a while back."

History, Intelligence Oversight, *at* http://www.dami.army.pentagon.mil/offices/damich/io/faq/history.html (last visited Sept. 30, 2004); *see* S. REP. NO. 94-755, at bk. III (giving an account of surveillance activities including covert penetration of the Poor Peoples' March to Washington; attendance at a Halloween party for elementary school children in Washington, D.C., where Army agents suspected a local "dissident" might be present; and maintenance of files on over 100,000 citizens, including Reverend William Sloane Coffin, Congressman Abner Mikva, and Senator Adlai Stevenson, III); JENSEN, *supra* note 21, at 240–47 (recounting military surveillance during Vietnam protests).

[39] Thus, the CIA intercepted all international mail to and from individuals and organizations on a New York City "watch list" over a twenty-year period. REPORT TO THE PRESIDENT BY THE COMMISSION ON CIA ACTIVITIES WITHIN THE UNITED STATES 111–12 (1975) [hereinafter ROCKEFELLER COMMISSION REPORT], *available at* http://history-matters.com/archive/church/rockcomm/contents.htm (last visited Sept. 30, 2004). It also deployed its resources against the anti-war movement under the rubric "Operation CHAOS," accumulating files containing the names of 300,000 persons and organizations. *Id.* at 146.

The FBI engaged in a campaign of wiretapping, surveillance, penetration, and harassment against a variety of dissident groups under the "COINTELPRO" programs. *See* Hobson v. Wilson, 737 F.2d 1 (D.C. Cir 1984) (describing operation of FBI harassment); JAMES KIRKPATRICK DAVIS, SPYING ON AMERICA: THE FBI'S DOMESTIC COUNTERINTELLIGENCE PROGRAM 2 (1992) (discussing the COINTELPRO programs beginning in 1956); THEOHARIS, *supra* note 37, at 135–55 (describing COINTELPRO).

The NSA surveilled a variety of dissidents under its MINARET program. *Id.* at 122–23. The IRS was mobilized to target "dissident" and "extremist" individuals and organizations for audits. *Id.* at 188–90.

[40] THEOHARIS, *supra* note 37, at 16–17 (describing efforts in 1969 to mobilize intelligence agencies). The high water mark of this effort was the Huston Plan developed during the summer of 1970. That White House initiative was approved by President Nixon, though the approval was later revoked, and attempted to create a permanent interagency committee on domestic protest which would distribute disinformation, engage in electronic surveillance, kidnapping, infiltration, break-ins, pilfering, and opening of mail. *See* S. REP. NO. 94-755, bk. II (1976), *available at* http://old.lib.ucdavis.edu/govdoc/Intelligence/76S9632.pdf (last visited Sept. 30, 2004); John W. Dean, III, *Watergate: What Was It?*, 51 HASTINGS L.J. 609, 614–15 (2000) (recounting that his reaction to the Huston Plan when presented to him as the President's counsel was that "[t]he potential scope of illegal activity by the government was truly frightening"); THEOHARIS, *supra* note 37, at 13–39.

[41] *E.g.*, United States v. Ehrlichman, 546 F.2d 910, 924–28 (D.C. Cir. 1976) (rejecting defendant's claim of presidential authority to burglarize the office of Daniel Ellsberg's psychiatrist to protect national security interests); Dellinger v. Mitchell, 442 F.2d 782, 784 (D.C. Cir 1971) (noting "[t]he Government answer asserted that the electronic surveillance was lawful even in

B. *Political Surveillance in the Supreme Court*

Both military and civilian efforts were ultimately subjected to legal challenges that made their way to the Supreme Court.

1. *Military Surveillance:* Laird v. Tatum

In January of 1970, a former military intelligence officer published a description of the extensive domestic political surveillance files that the Army had developed during the 1960s.[42] Although the Defense Department initially denied most of the allegations, the ACLU filed a class action on February 17, 1970 seeking a declaratory judgment that the program was unconstitutional, an injunction preventing continuation of the program, and the destruction of the intelligence files. In April 1970, the trial court dismissed the case on the ground that the acquisition and filing of information constituted "no threat to [the plaintiffs'] rights."[43] Despite its refusal to allow the plaintiffs to present evidence or obtain discovery on the nature of the infiltration undertaken by Army agents, the trial court rested its dismissal on the proposition that the Army merely kept "the type of information that is available to all news media in this country."[44]

A year later, in April 1971, the District of Columbia Circuit reversed by a vote of two to one, remanding for discovery and proof as to the nature and scope of the Army's domestic intelligence system and its effect on dissent.[45] The majority opinion acknowledged that the plaintiffs faced "some difficulty in establishing visible injury, at least on this incomplete record."[46] Nonetheless, the majority was willing to acknowledge that the Army's files resulted in an actionable "inhibition of lawful behavior and of First Amendment rights,"[47] in light of the "long-established tradition against military involvement in civilian politics,"[48] and of the fact that the military's commanders were

the absence of judicial authorization since the President, acting through the Attorney General, has constitutional power as the Chief Executive to utilize electronic surveillance [in domestic security cases] . . . free from any judicial supervision or statutory limitation.").

[42] Christopher H. Pyle, *CONUS Intelligence: The Army Watches Civilian Politics*, WASH. MONTHLY, Jan. 1970, at 4. A follow-up appeared in Christopher H. Pyle, *CONUS Revisited, The Army Covers Up*, WASH. MONTHLY, July 1970.

[43] Tatum v. Laird, 444 F.2d 947, 963 (D.C. Cir. 1971) (citing the trial court decision), *rev'd*, 408 U.S. 1 (1972).

[44] *Id.* at 962–63 (citing the trial court decision).

[45] *Id.*

[46] *Id.* at 953.

[47] *Id.* at 954.

[48] *Id.* at 956.

"trained as soldiers not lawyers" and were "not accustomed to operating within the restrictions of law and the processes of the courts."[49]

Rather than risking discovery directed at its domestic surveillance apparatus, the administration, in turn, sought Supreme Court review, which was granted in November 1971.[50] In the course of briefing, the Solicitor General highlighted the statements of the lower courts that the information-gathering activities of the military were based on publicly-available data, and hence, were analogous to newspaper clipping services,[51] and pressed the proposition that, in the absence of a showing of specific threat of governmental sanctions, the "visionary apprehensions" of future misuse of the data created no justiciable controversy.[52]

The ACLU and its allies, on the other hand, argued that legislative investigations[53] and parallel litigation[54] that followed the summary dismissal of *Laird* in the trial court had revealed an array of both legal and illegal military surveillance that went far beyond attendance at public meetings and clipping publications.[55] They advanced a series

[49] *Id.* at 958.

[50] Laird v. Tatum, 404 U.S. 955 (1971). The grant of review came five months after the rejection of the administration's claim of inherent power to obtain prior restraints against newspaper publications in the name of national security in *New York Times v. United States*, 403 U.S. 713 (1971).

[51] Brief for Petitioners at 12, Laird v. Tatum, 408 U.S. 1 (1971) (No. 71-288) (discussing "type of information that is available to all news media in this country"); *id.* at 15 (stating that it is "essentially no different than what a good newspaper reporter would be able to gather by attendance at public meetings") (citing majority opinion).

[52] *Id.* at 20–21, 24, 26–27 n.24 ("[P]roper course is to await a case presenting concrete evidence of unlawful inhibitory action.").

[53] *See* Lawrence M. Baskir, *Reflections on the Senate Investigation of Army Surveillance*, 49 IND. L.J. 618, 619–37 (1974) (giving account of the evolution of the Ervin Committee hearings).

[54] The ACLU had filed a related case in Illinois, which proceeded through presentation of evidence in a preliminary injunction hearing before being dismissed. ACLU v. Westmoreland, No. 70-3191 (N.D. Ill. filed Dec. 21, 1970). *Westmoreland* was dismissed on January 5, 1971, a dismissal that was affirmed by *ACLU v. Laird*, 463 F.2d 499 (7th Cir. 1972), *cert. denied*, 409 U.S. 1116 (1973).

[55] Brief for Respondents at 15–21, *Laird* (No. 71-288) (referring to the record of *Westmoreland* and the Ervin hearings to highlight the continuing retention of political surveillance dossiers, the breadth of the political groups surveilled (including Americans for Democratic Action and the NAACP), the harmful dissemination of such information, and the covert surveillance and intrusion that generated the information); Amicus Brief of a Group of Former Army Intelligence Agents at 16–19, 24, *Laird* (No. 71-288) (highlighting scope of surveillance as described in hearing testimony, including undercover infiltration, "stake-outs" of the grave of Martin Luther King, impersonations of news media, illegal monitoring of radio transmissions, and leaking of information to other government agencies, press, private employers, and subversive hunters); *id.* at 26–29 (disputing the Justice Department's "errors and omissions of fact" concerning the limitations on military surveillance); Amicus Brief of Unitarian Universalist Ass'n at 11, *Laird* (No. 71-288) (attaching copies of hearings of Senate Judiciary Committee's Constitutional Rights Subcommittee, commenting on correspondence with the committee in which executive officials refuse to eliminate political surveillance data from governmental records).

of arguments from constitutional theory and social science, along with the recollection of the McCarthy era, to support the proposition that accumulation of political surveillance files is likely to chill political discussion and participation, and argued that this chill, in itself, was a cognizable injury.[56]

Chief Justice Burger, writing for a five-member majority, held for the defendants. His opinion acknowledged the "traditional and strong resistance of Americans to any military intrusion into civilian affairs," and offered assurance that no "actual or threatened injury by reason of unlawful activities of the military" would go unredressed.[57] The majority opinion determined, however, that the plaintiffs' allegations made out no such injury. Somewhat disingenuously, the opinion repeated the statement of the Court of Appeals that "[s]o far as is yet shown, the information gathered is nothing more than a good newspaper reporter would be able to gather by attendance at public meetings and the clipping of articles from publications available on any newsstand."[58] The existence of such files, the majority determined, did not make out a claim of "specific present objective harm or the threat of specific future harm" necessary to provide the plaintiffs with standing.[59] In the absence of an exercise of "regulatory, proscriptive or compulsory" power by the government, a "subjective chill" was insufficient.[60]

The Government urged the Court to take judicial notice of the existence of the legislative investigations, Brief for Petitioners at 33–34, *Laird* (No. 71-288), while relying on judicial characterization of the Army's activities that were at odds with the facts revealed by those hearings. *Cf.* Reply Brief for Petitioners at 7–10, *Laird* (No. 71-288) (urging the Court not to rely on material presented at the legislative hearings).

[56] Brief for Respondents at 15–21, *Laird* (No. 71-288).

[57] *Laird*, 408 U.S. at 15–16.

[58] *Id.* at 9 (citing 444 F.2d at 953). The crucial qualifier "[s]o far as is yet shown" made the statement technically accurate. The opinion's account of what had been "shown" in *Laird* ignored both the allegations of the complaint of illegal invasions of privacy and the showings of record in both the parallel *Westmoreland* litigation and the congressional hearings that occurred after the record was closed at trial in *Laird*.

Likewise, the opinion maintained that "the principal sources" of the information were news media and identified some information as coming from public meetings and civilian law enforcement agencies. *Id.* at 6–7. This statement may or may not have been true, depending on the definition of "principal"; it was untested factually, and at odds with the plaintiffs' allegations. Plaintiffs maintained that only five percent of the reports came from the news media, and that the sources of data included illegal electronic surveillance, confidential private sector records, and covert informers. *See* Petition for Rehearing at 7–8, *Laird* (No. 71-288).

[59] 408 U.S. at 14.

[60] *Id.* at 11, 13.

2. *"Domestic Security" and Presidential Prerogative:* United States v. United States District Court *(Keith)*

In January of 1971, as the ACLU lawyers were preparing to argue their case against military blacklists in the D.C. Circuit, another challenge to domestic political surveillance was beginning its journey to the Supreme Court. Radical lawyer William Kunstler, defending three members of the "White Panther Party" charged with conspiracy to dynamite the CIA office in Ann Arbor, Michigan, had moved to compel disclosure of the transcript logs of warrantless wiretaps deployed against his clients, which he argued, would taint their prosecution.[61] In response, the Justice Department acknowledged wiretapping one of the defendants without a warrant, but invoked what it regarded as inherent presidential authority over domestic security to maintain that the defendants had no right to examine the logs.[62] The Justice Department advanced the proposition that wiretaps authorized by the President or his designee, the Attorney General, to "protect the nation against hostile acts and to gather information concerning domestic organizations which seek to attack and subvert" the government were *ipso facto* legal.[63] The claim of inherent and extra-constitutional executive authority in domestic security cases was a regular feature of the efforts of the Nixon Administration's struggle against domestic radicals and opponents of the Vietnam war,[64] but the trial judge, Damon Keith, rejected it.[65] The Justice Department im-

[61] United States v. Sinclair, 321 F. Supp. 1074, 1076 (E.D. Mich. 1971), *aff'd sub nom.* United States v. U.S. Dist. Ct. (Keith), 444 F.2d 651 (6th Cir. 1971), *aff'd*, 407 U.S. 297 (1972).

[62] *Id.* at 1076–77.

[63] *Id.* at 1079 (quoting from the affidavit filed by the Attorney General).

[64] *See, e.g.*, United States v. Ehrlichman, 546 F.2d 910, 924–28 (D.C. Cir. 1976) (rejecting defendant's claim of presidential authority to burglarize office of Daniel Ellsberg's psychiatrist to protect national security interests); *In re* Dellinger, 461 F.2d 389 (7th Cir. 1972) (invoking executive authority to engage in warrantless wiretapping in the Chicago 8 case); Dellinger v. Mitchell, 442 F.2d 782, 784 (D.C. Cir 1971) (noting "the Government answer asserted that the electronic surveillance was lawful even in the absence of judicial authorization since the President, acting through the Attorney General, has constitutional power as the Chief Executive to utilize electronic surveillance [in domestic security cases] . . . free from constitutional or statutory limitations"); United States v. Clay, 430 F.2d 165 (5th Cir. 1970) (affirming that the defendant's conviction was not affected by five wiretapped conversations); United States v. Stone, 305 F. Supp. 75 (D.C. Cir. 1969) (determining that the Government did not have to disclose records of intercepted telephone conversations); United States v. O'Baugh, 304 F. Supp. 767, 768 (D.C. Cir. 1969) ("Since neither defendant's Fourth Amendment rights nor Section 605 of the Federal Communications Act of 1934 were violated, the wiretap used by the government to obtain foreign intelligence information was legal."); United States v. Smith, 321 F. Supp. 424, 429 (C.D. Cal. 1971) (concluding that in "wholly domestic situations there is no national security exemption from the warrant requirement"); United States v. O'Neal, No. KC-CR-1204 (D. Kan. Sept. 1, 1970); United States v. Brown, 317 F. Supp. 531 (E.D. La. 1970) (holding that the monitored telephone conversations by prison officials did not taint defendant's conviction).

[65] *Sinclair*, 321 F. Supp. 1074.

mediately filed a mandamus action to block implementation of Judge Keith's order to provide the transcripts (now styled *United States v. United States District Court (Keith)*), and on April 18, 1971 the Sixth Circuit affirmed.[66] The Supreme Court granted the Justice Department's petition for certiorari; *Keith* was argued a month before *Laird v. Tatum*, and decided a week earlier.[67]

Unlike *Laird*, there was no question of justiciability. In the Supreme Court, the government acknowledged that the wiretap in question was a "search" for purposes of the Fourth Amendment. But it took the position that searches ordered by the President or his designee for purposes of domestic security are "reasonable" searches even in the absence of a warrant unless the order is determined after the fact to be arbitrary and capricious.[68]

The government argued that in the midst of a rising wave of anti-government bombings, "the President must protect the government—and thereby the society for whose benefit it exists."[69] Where the President seeks to obtain information that will be used to prevent rather than prosecute attacks, the argument continued, the question of the reasonableness of searches diverges from the criminal justice model.[70] Given the "complicated facts and subtle inferences" involved in domestic intelligence investigations, the Justice Department concluded that "[a]llowing the Attorney General to authorize such surveillances without prior approval by a magistrate would centralize responsibility . . . facilitating close control of the use of this investigative technique."[71] "[T]he interest of privacy of the American citizen," claimed the government, "is better protected in limiting this authority in the area of electronic surveillance in counterintelligence cases, to one man—the Attorney General, acting for the President of the

[66] 444 F.2d 651.

[67] 407 U.S. 297. Justice Douglas's concurrence in *Keith* saw the two cases as linked elements of a "flood of cases" reflecting a concerted federal effort to "subject[] to scrutiny" "[t]hose who . . . dissent or who petition . . . for redress." *Id.* at 329 (Douglas, J., concurring). Citing those cases, the Ervin hearings and journalistic revelations, he discerned a pattern of surveillance, bugging, interrogation, infiltration, grand jury subpoenas, and efforts to discredit opposition. *Id.* at 329–33. At the time, Justice Douglas's rhetoric may have seemed overwrought. In retrospect he appears to have accurately identified the Nixon Administration's strategy.

[68] In the trial court, the Government had argued that the President's inherent authority was immune from all review. 321 F. Supp. at 1077 (prompting Judge Keith to make the observation that "[w]e are a country of laws and not of men.").

[69] Brief for the United States at 18, United States v. U.S. Dist. Ct. (Keith), 407 U.S. 297 (1972) (No. 70-153).

[70] *Id.*; *see also* Reply Brief for the United States at 2–3, *Keith* (No. 70-153).

[71] Brief for the United States at 7, 27–28, *Keith* (No. 70-153). The government argued, as well, that the Attorney General's judgment is reliable because he is "directly accountable to the President and through him to the electorate." Petition for Cert. at 8, *Keith* (No. 70-153).

United States—rather than to proliferate amongst all of the Federal sitting judges in the United States."[72]

Unlike *Laird*, the Court in *Keith* rejected the government's position without dissent.[73] Justice Powell's opinion acknowledged the president's "fundamental duty" to "protect, preserve and defend the Constitution of the United States," the record of "threats and acts of sabotage," and the "covertness and complexity of potential unlawful conduct" in domestic security cases.[74] But it noted as well that "national security cases often reflect a convergence of First and Fourth Amendment values":

> History abundantly documents the tendency of Government—however benevolent and benign its motives—to view with suspicion those who most fervently dispute its policies. Fourth Amendment protections become the more necessary when the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs. The danger to political dissent is acute where the Government attempts to act under so vague a concept as the power to protect "domestic security."[75]

In light of the "potential danger[s] posed by unreasonable surveillance to individual privacy and free expression,"[76] the opinion held, neither the demands of internal security nor the claims of executive authority justified the claim that wiretapping, even for "intelligence" purposes, could be constitutional in the absence of a warrant issued by a "neutral and detached magistrate."[77] "[U]nreviewed executive discretion," the court held, "may yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech."[78]

---

[72] Transcript of Oral Argument at *1046, *Keith* (No. 70-153).

[73] Justice Rehnquist, before his elevation to the bench, had been a key player in establishing both the parameters of civil and domestic surveillance for the Nixon Administration. *See* Jeffrey W. Stempel, *Rehnquist, Recusal, and Reform*, 53 BROOK. L. REV. 589, 592–93 (1987) (criticizing Justice Rehnquist's refusal to recuse himself in *Laird*); Note, *Justice Rehnquist's Decision to Participate in* Laird v. Tatum, 73 COLUM. L. REV. 106 (1973). He had not recused himself in *Laird* but elected to do so in *Keith*. 407 U.S. at 324. Justice Burger concurred in the result without opinion, *id.*, and Justice White concurred on statutory grounds. *Id.* at 335.

[74] *Id.* at 310–12.

[75] *Id.* at 313–14.

[76] *Id.* at 315.

[77] *Id.* at 318–21.

[78] *Id.* at 317–22. The *Keith* case left undecided the issue of whether the President could invoke powers unconstrained by the Fourth Amendment in the case of foreign threats. *See id.* at 308 ("[T]he instant case requires no judgment on the scope of the President's surveillance power with respect to the activities of foreign powers."). Lower courts divided on the issue. *Compare* United States v. Butenko, 494 F.2d 593, 604–05 (3d Cir.) (en banc) (finding that some Fourth Amendment protections, but not a prior judicial warrant, might be applicable even when the President was acting pursuant to his foreign affairs duties), *cert. denied*, 419 U.S. 881 (1974), *and* United States v. Brown, 484 F.2d 418, 426 (5th Cir. 1973) (holding that the President may constitutionally authorize warrantless wiretaps for the purpose of gathering foreign intelligence), *with* Zweibon v. Mitchell, 516 F.2d 594, 614 (D.C. Cir. 1975) (en banc) (holding

C. The Risks of Records

Keith rejected the claims of the Nixon Administration. In light of the risks that surveillance posed to privacy and free expression, it could not accept the position that the imperatives of domestic security suspended the provisions of the Fourth Amendment. When the government sought information by search or seizure, by physical intrusion, or by wiretapping, the Constitution required authorization from a neutral magistrate. On the other hand, under *Laird*, where no "regulatory, proscriptive, or compulsory" sanctions were deployed, gathering information was largely immune from constitutional challenge.[79] This division of constitutional labor meant that officials were not constitutionally precluded from compiling dossiers on sensitive political activities and dissent. So long as the information was not utilized in formal proceedings, the exclusionary rule could not be brought to bear even on information that was illegally obtained. Yet the course of the litigation, combined with contemporaneous investi-

that a warrant is always required when a domestic organization is targeted, even if the surveillance is initiated under the President's foreign intelligence gathering power), *cert. denied*, 425 U.S. 944 (1976). Likewise, the Court in *Keith* suggested that "security intelligence" seeking to "prevent unlawful activity" or "enhance government preparedness" might be grounds for Congress to alter the standards for issuance of the warrant. 407 U.S. at 322.

[79] Laird v. Tatum, 408 U.S. 1, 11 (1972). The distinction between "regulatory" actions, which were constrained by law, and actions involving the acquisition or dissemination of information, which were uncontrolled, was echoed in *Paul v. Davis*, 424 U.S. 693, 708–09 (1976) (holding that mere defamation through the state's publication of a flyer with the defendant listed as an active shoplifter without an "alteration in legal status" is insufficient to trigger due process requirements) and *Whalen v. Roe*, 429 U.S. 589, 603–04 (1977) (holding that neither the immediate nor the threatened impact of the patient-identification requirements on either the reputation or the independence of patients for whom certain drugs are medically indicated is sufficient to constitute an invasion of any right or liberty).

The *Laird* majority's disingenuous refusal to acknowledge the nature and scope of the Army's surveillance program, ironically, formed the basis for subsequent distinctions of *Laird* by some lower courts. *E.g.*, Anderson v. Davila, 125 F.3d 148 (3d Cir. 1997) (enjoining targeted surveillance in retaliation for filing Equal Employment Opportunity Commission (EEOC) complaint); Presbyterian Church (U.S.A.) v. United States, 870 F.2d 518 (9th Cir. 1989) (showing of membership loss by targeted organization confers standing); Olagues v. Russoniello, 797 F.2d 1511 (9th Cir. 1986) (explaining that being the targets of surveillance gives standing to sue for injunctive relief); Hall v. Pa. State Police, 570 F.2d 86 (3d Cir. 1978) (placing surveillance cameras based on race confers standing); Phila. Yearly Meeting of Religious Soc'y of Friends v. Tate, 519 F.2d 1335 (3d Cir. 1975) (disseminating information beyond law enforcement circles confers standing); Berlin Democratic Club v. Rumsfeld, 410 F. Supp. 144, 151 (D.D.C. 1976) (finding that illegal techniques of surveillance or dissemination of information confers standing); Alliance to End Repression v. Rochford, 407 F. Supp. 115, 117 (N.D. Ill. 1975) (finding that intrusive techniques of surveillance gave standing); Handschu v. Special Services Div., 349 F. Supp. 766 (S.D.N.Y. 1972) (finding that intrusive techniques gave standing). *But cf.* ACLU v. Laird, 463 F.2d 499 (7th Cir. 1972) (on request for rehearing) (relying on facts set forth in Justice Douglas's dissent in *Laird v. Tatum* to find that even broad, illegal, and intrusive surveillance would not confer standing).

gations, highlighted real dangers for civil liberties from the very compilation of dossiers.

1. *"You manage what you measure"*

As the old chestnut from organizational development handbooks has it, in any bureaucracy, "you manage what you measure."[80] A political establishment that systematically tracks the involvement of particular individuals in political support or opposition is a political establishment that can move to reward supporters and punish critics. During the Nixon era, intelligence information was put to precisely this use.

At its worst, a list of political opponents prefigures the danger of political purges and military coups. As Judge Wilkey, a moderate jurist not generally given to radical paranoia put the concern in the D.C. Circuit opinion in *Laird*:

> It is highly important for the safety of the country that to the extent consonant with the performance of the military's mission a separation of sensitive information and military power be maintained, as a separation of match and powder. . . . [T]o permit the military to exercise a totally unrestricted investigative function in regard to civilians, divorced from the normal restrictions of legal process and the courts, and necessarily coupling sensitive information with military power, could create a dangerous situation in the Republic.[81]

The files challenged in *Laird* were probably poorly adapted to actually implementing a coup. While "counterinsurgency" rhetoric was occasionally utilized by military planners, the ultimate goal was simply to provide advance warning of potential riots in which the Army would be called upon to provide backup for civilian authorities.[82] On the other hand, the accumulation of "blacklists" of potential agitators was well adapted to the use of extralegal mechanisms to suppress opponents of existing civil authorities.[83]

---

[80] *E.g.*, DONALD A. MARCHAND ET AL., MAKING THE INVISIBLE VISIBLE: HOW COMPANIES WIN WITH THE RIGHT INFORMATION, PEOPLE AND IT (2001); Bradley C. Karkkainen, *Information as Environmental Regulation: TRI and Performance Benchmarking, Precursor to a New Paradigm?*, 89 GEO. L.J. 257, 285–88 (2001); Louis Lowenstein, *Financial Transparency and Corporate Governance: You Manage What You Measure*, 96 COLUM. L. REV. 1335, 1342–43 (1996).

[81] Tatum v Laird, 444 F.2d 947, 958 (D.C. Cir. 1971), *rev'd*, 408 U.S. 1 (1971).

[82] PYLE, *supra* note 21, at 319–24; *see also id.* at 324–33 (noting that the official doctrine did not contemplate the imposition of martial law).

[83] The FBI conducted "tens of thousands of domestic intelligence investigations" to identify candidates for incarceration under the "Emergency Detention of Suspected Security Risks Provision" of the Internal Security Act of 1950, Pub. L. No. 81-831, § 103, 64 Stat. 987, 1021, which was repealed in September 1971, Pub. L. No. 92-128, 85 Stat. 347 (1971). W. Raymond Wannall, *Undermining Counter Intelligence Capability*, 15 INT'L J. INTELLIGENCE & COUNTERINTELLIGENCE 321–22 (Fall 2002) (lamenting the repeal of this provision); *see also* DONNER, *supra* note 24, at 162–69 (discussing "custodial detention programs"); THEOHARIS,

The Nixon Administration did not deploy death squads or disappearances against its critics. But the discretion of the modern administrative state is well adapted to low visibility retaliation. Some such interventions are blatantly illegal, like focusing IRS audits on political opponents—as was the custom with the Nixon enemies lists. Others fall into a gray area of patronage, selective prosecution, and "honest graft." Most such interventions are difficult to prove to the satisfaction of skeptical courts, so nominal legal protections may be thin armor against them. On the other hand, none can be effective unless the identities of opponents and supporters are revealed. A government that is limited in its ability to amass information about the political activities of citizens will be constrained in its efforts to target such activities for adverse exercises of administrative discretion.

2. *Blacklists, Blackmail, Blackened Reputation*

In addition to the prospect of governmental retaliation, the acquisition of information provides a level of power that can be exercised without going through official channels. During the McCarthy era, the threat of exposure was a substantial weapon in the hands of red-baiters. In an era when sixty-eight percent of the populace believed that Communists should be fired from jobs as sales clerks, and ninety-one percent believed that Communist teachers should be discharged, public registration as a member of the Communist party was economic suicide, and being named as an "uncooperative" witness was a pathway to ruin.[84] As the Court observed, when

> forced revelations concern matters that are unorthodox, unpopular, or even hateful to the general public, the reaction in the life of the witness may be disastrous. . . . Those who are identified by witnesses and thereby placed in the same glare of publicity are equally subject to public stigma, scorn and obloquy.[85]

In the COINTELPRO program, during the 1960s, the FBI deployed the prospect of embarrassing exposure against disfavored groups, and the motive for the illegal burglary of Daniel Ellsberg's

supra note 37, at 40–64 (describing the evolution of the FBI's "Custodial Detention Index" into the "Security Index" into the "Administrative Index" between 1930 and 1972). Likewise, the Army counterintelligence program in the 1960s maintained "blacklists" of agitators to be incarcerated in the event of civil disturbances. PYLE, *supra* note 21, 72–73, 344 (describing the series of mug books, known as "blacklists," which was a "file on individuals involved in underground activities against an army of occupation and is used by that army as a round-up list").

[84] *See* DONNER, *supra* note 24, at 178 (detailing FBI tactic of leaking alleged subversiveness of uncooperative witnesses to landlords and employers).

[85] Watkins v. United States, 354 U.S. 178, 197 (1957); *see, e.g.*, Sweezy v. New Hampshire, 354 U.S. 234, 248 (1957) ("The sanction emanating from legislative investigations is of a different kind than loss of employment. But the stain of the stamp of disloyalty is just as deep. The inhibiting effect in the flow of democratic expression . . . is equally grave.").

psychiatrist's office was an effort to find information that could discredit the release of the Pentagon Papers.[86]

3. *Chilling Effects: "I'll Be Watching You"*

Uncontrolled surveillance may be effective in repressing dissent even where dossiers are not deployed to achieve any concrete results. Opposition to the surveillance of the Nixon Administration was rooted in the observed effects of the red-hunting of the 1950s. In *Lamont v. Postmaster General*, the Court wrote in the shadow of its experience with McCarthyism of the "almost certain deterrent effect" of being listed in government files as one who requests "communist propaganda":

> Public officials, like schoolteachers who have no tenure, might think they would invite disaster if they read what the Federal Government says contains the seeds of treason. Apart from them, any addressee is likely to feel some inhibition in sending for literature which federal officials have condemned as "communist political propaganda."[87]

Vulnerability can arise not only from the observation of dissident activities, but from sufficiently penetrating documentation of non-political transgressions. Authorities who have sufficient knowledge of a fallible citizenry are in a position to cow dissent by the mere fact of their prosecutorial discretion. Justice Jackson observed:

> I cannot say that our country could have no central police without becoming totalitarian, but I can say with great conviction that it cannot be totalitarian without a centralized national police. . . . [A national police] will have enough on enough people, even if it does not elect to prosecute them, so that it will find no opposition to its policies.[88]

The very sense of exposure to view, moreover, encourages individuals to engage in actions that society desires. Unorthodox but protected activities are less likely to be undertaken when subject to examination. The author who must expose every draft to the public

---

[86] *See, e.g.*, United States v. Ehrlichman, 546 F.2d 910, 915 (D.C. Cir. 1976) (noting that even the Government brief conceded that the reasons for interest in Ellsberg's psychiatric records "were, at best mixed" and included creating a "negative press image" of Ellsberg); DAVIS, *supra* note 39 (1992) (detailing COINTELPRO tactics); DONNER, *supra* note 24, at 170–72 (detailing dissemination of files); *id.* at 177–237 (describing COINTELPRO tactics).

[87] 381 U.S. 301, 307 (1965); *see, e.g.*, Gibson v. Florida Legislative Comm., 372 U.S. 539, 544 (1963) ("Inviolability of privacy in group association [is] indispensable to [the] preservation of freedom of association, particularly where a group espouses dissident beliefs."); Shelton v. Tucker, 364 U.S. 479, 485–87 (1960) ("To compel a teacher to disclose his every associational tie is to impair that teacher's right of free association.") (citing NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 462 (1958)); *NAACP*, 357 U.S. at 462 ("[C]ompelled disclosure of affiliation with groups engaged in advocacy may constitute as effective a restraint on freedom of association as [taxes or punishments].").

[88] ROBERT H. JACKSON, THE SUPREME COURT IN THE AMERICAN SYSTEM OF GOVERNMENT 70–71 (1955).

is likely to turn out a more timid product than the one who can try out alternatives in private. The ability to experiment in the realm of the intimate is valuable not only for the society it builds, but for the citizens' sense of freedom and character. Unwanted observation by others is itself a limitation of autonomy, and the more intimate the observation, the greater the violation. To retain a sense of control over who can observe us nurtures our sense of independence; control over disclosure of intimate matters may be essential to our sense of identity. Conversely, the power of the state to inflict the sense of vulnerability is itself a sanction.

It was in recognition of these effects that Justice Powell emphasized in *Keith:*

> The price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power. Nor must the fear of unauthorized official eavesdropping deter vigorous citizen dissent and discussion of Government action in private conversation. For private dissent, no less than open public discourse, is essential to our free society.[89]

D. The Settlement of the 1970s

In the congressional hearings on military surveillance, then-Assistant Attorney General (and later Chief Justice) Rehnquist argued that it was "quite likely that self-discipline on the part of the executive branch will provide an answer to virtually all of the legitimate complaints against excesses of information-gathering."[90] Executive self-discipline in the administration for which he spoke at the time was manifestly underdeveloped. Yet, in the next seven years, the most effective responses to the dangers of databases did emerge from the political branches. Executive and legislative initiatives erected a web of constraints on political surveillance that imposed a measure of accountability on the programs left beyond judicial control by *Laird.*

The Ervin hearings on Army surveillance and the revelations of Watergate impelled Congress in 1974 to adopt the Federal Privacy Act, limiting both retention and use of information regarding private individuals by federal agencies.[91] In 1975, the Senate formed the

---

[89] United States v. U.S. Dist. Ct. (Keith), 407 U.S. 297, 314 (1972).

[90] Peter E. Quint, *The Separation of Powers Under Nixon: Reflections on Constitutional Liberties and the Rule of Law*, 1981 DUKE L.J. 1, 20 n.84 (quoting testimony of then-Assistant Attorney General William Rehnquist).

[91] In addition to structural limits, the Privacy Act specifically limits collection of political information:

> Each agency that maintains a system of records shall . . . maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity.

Church Committee and the House convened the Pike Committee to review and report on abuses by the intelligence community,[92] and in the next session they established permanent intelligence oversight committees in both the House and Senate.[93] In 1978, agencies were required to establish inspectors general,[94] and in the Foreign Intelligence Surveillance Act ("FISA"), Congress directly addressed the issue of foreign intelligence searches that the Court had pretermitted in *Keith*.[95]

In the executive branch, executive orders issued by Presidents Ford, Carter, and Reagan set constraints on the activities of the intelligence community.[96] The Defense Department established an Office

5 U.S.C. § 552a(e)(7) (2004). The protections of the Privacy Act, however, do not extend to data matching for national security and law enforcement purposes. *See* §§ 552a(b)(7), (a)(8)(B)(vi), and (j).

In 1974, Congress also strengthened and expanded the Freedom of Information Act ("FOIA"), Pub. L. No. 93-502, 88 Stat. 1561 (1974). *See also* 120 CONG. REC. H36,633 (1974) (showing a House veto override); 120 CONG. REC. S36,882 (1974) (showing a Senate veto override); Veto of Freedom of Information Act Amendments: The President's Message to the House of Representatives Returning H.R. 12,471 Without His Approval, 10 WEEKLY COMP. PRES. DOC. 1318 (1974) (describing President Gerald Ford's veto). Among other innovations, the amendments extended FOIA to some investigative material, 88 Stat. 1563–64 (amending 5 U.S.C. § 552(a)(7)) (limiting the exemption for investigative material and requiring that reasonably segregable material must still be disclosed); established time limits for disclosure; and strengthened judicial enforcement, 88 Stat. 1562–63 (amending § 552(a)) (providing administrative deadlines for disclosure and allowing judges to order production of records).

[92] On January 29, 1976, the House Select Intelligence Committee (the Pike Committee) issued its final report, which was never officially released but was published in part in VILLAGE VOICE, Feb. 16, 1976, at 1, and later in book form in Britain under the title CIA, THE PIKE REPORT (Spokesman Books 1977). On April 26, 1976, the Church Committee issued its final report, S. REP. NO. 94-755 (1976) (recommending a bar on domestic CIA activities). These followed the report of the Rockefeller Commission, created January 4, 1975 by President Gerald Ford. ROCKEFELLER COMMISSION REPORT, *supra* note 39.

[93] H.R. Res. 658, 95th Cong., 123 CONG. REC. 22,932, 22,932–49 (1977); S. Res. 400, 94th Cong., 122 CONG. REC. 14,657, 14,673–75 (1976).

[94] Inspector General Act of 1978, Pub. L. No. 95-452, 92 Stat. 1101 (codified as amended in scattered sections of 5 U.S.C.).

[95] Foreign Intelligence Surveillance Act ("FISA"), Pub. L. No. 95-511, 92 Stat. 1783 (1978) (codified as amended at 50 U.S.C. §§ 1801–11 (2000)). FISA provided that no "U.S. Person" may become a target of FISA surveillance "solely upon the basis of activities protected by the first amendment." §§ 1805(a)(3)(A), 1824(a)(3)(A).

[96] Exec. Order No. 11,905, 41 Fed. Reg. 7707 (1976) [hereinafter Ford Order]; Exec. Order No. 12,036, 43 Fed. Reg. 3674 (1978) [hereinafter Carter Order], *revoked by* Exec. Order No. 12,333, 46 Fed. Reg. 59,941 (1981) [hereinafter Reagan Order]. These Orders limited the collection of intelligence regarding "United States persons," mandated the use of the "least intrusive collection techniques feasible within the United States or directed against United States persons abroad," precluded the CIA from electronic surveillance within the United States, and largely limited searches and surveillance within the United States to the FBI. Reagan Order at 59,950–52; *see also* Carter Order at §§ 2-202 to 2-206; Ford Order at § 5. The Carter and Reagan Orders also precluded agencies other than the FBI from seeking to covertly influence organizations in the United States, while constraining covert participation of any sort. Reagan Order at 59,952; Carter Order at § 2-207; *see also* U.S. Postal Service, Inspection Service Authority, 39

of Inspector General for Intelligence in 1976, which became the Assistant to the Secretary of Defense (Intelligence Oversight) in 1982.[97] Attorney General Edward Levi, in 1976, promulgated guidelines on Domestic Security Investigation which substantially constrained the FBI's political surveillance, authorizing full investigation only on the basis of actual or incipient conduct, rather than ideology or advocacy[98] and only in a manner "designed and conducted so as not to limit the full exercise of rights protected by the Constitution and laws of the United States."[99]

Beyond the limits embodied in positive law, aggressive Congressional investigation and exposure proved as important as statutory controls. The trauma of the hearings and the firestorm of outrage those hearings produced has etched in organizational culture of a number of agencies the impropriety of abusing security intelligence.

II. THE AFTERMATH OF SEPTEMBER 11

A. The World Turned Upside Down

Since the convulsions of the 1970s, the concerns which fueled the imposition of constraints on the gathering and use of political intelligence have remained strong. In the Supreme Court, a series of cases have cemented status of informational privacy as a constitutional norm linked both to autonomy and free expression.[100] In *Bartnicki v.*

C.F.R. § 233.3 (2003) (constraining the use of "mail covers") (adopted originally as 40 Fed. Reg. 11,579 (1975)).

[97] Organizational Charter, Assistant to the Secretary of Defense (Intelligence Oversight), 32 C.F.R. pt. 378 (1983) (establishing the office of the Assistant to the Secretary of Defense for Intelligence Oversight); *see also* Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons, Dep't of Defense Directive No. 5240.1-R (1982) (establishing substantive and procedural limits on the conduct of intelligence activities), *available at* http://www.dtic.mil/whs/directives/corres/pdf2/p52401r.pdf (last visited Sept. 30, 2004). Each service also has established its own intelligence oversight office.

[98] Attorney General Edward Levi, Attorney General's Guidelines on Domestic Security Investigations (Apr. 5, 1976) [hereinafter Levi Guidelines], *reprinted in FBI Statutory Charter: Hearings on S. 1612 Before the S. Comm. on the Judiciary*, 95th Cong. 18–26 (1978). These guidelines were subsequently loosened somewhat by the Reagan Administration. *See* Attorney General William French Smith, Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Domestic Security/Terrorism Investigations (Mar. 7, 1983), *reprinted in* 32 CRIM. L. REP. (BNA) 3087 (1983). The Levi Guidelines, for example, required "specific and articulable facts," showing actual or incipient criminal violations before commencing a full investigation, while the Smith version required only a "reasonable indication" as the legal standard for opening a "full" investigation. For discussions of the differences between the two sets of guidelines, see Alliance to End Repression v. City of Chi., 742 F.2d 1007, 1015 (7th Cir. 1984); John T. Elliff, *The Attorney General's Guidelines for FBI Investigations*, 69 CORNELL L. REV. 785 (1984).

[99] Levi Guidelines, *supra* note 98, at II(B).

[100] Watchtower Bible & Tract Soc'y v. Vill. of Stratton, 536 U.S. 150, 166–67 (2002) (finding ordinance prohibiting door-to-door advocacy with a permit as violative of the First Amendment

Vopper, an otherwise divided court recently coalesced around the proposition, echoed verbatim by majority and dissent:

> In a democratic society privacy of communication is essential if citizens are to think and act creatively and constructively. Fear or suspicion that one's speech is being monitored by a stranger, even without the reality of such activity, can have a seriously inhibiting effect upon the willingness to voice critical and constructive ideas.[101]

Courts and the public continue to view the prospect of surveillance and disclosure as evils of constitutional magnitude. Yet today, the settlement of the 1970s is coming unglued, for the limits imposed by *Keith* and the administrative constraints of the 1970s have become increasingly permeable.

At a technical level, a variety of surveillance techniques have become available to intelligence and law enforcement agencies that neither invade physical spaces or intercept conversations that can claim protection under the Fourth Amendment.[102] The Fourth Amendment has, moreover, been held inapplicable to acquisition of information from private parties to whom that information has been entrusted. Thus, the Court has held that when government agencies seek bank records from bankers, or telephone logs from telephone companies, they do not engage in "searches" which require either probable cause or warrant.[103] Given the dependence of Internet

protection accorded to anonymous discourse); Buckley v. Am. Constitutional Law Found., 525 U.S. 182, 199–204 (1999) (striking down required public identification of collectors of signatures as a violation of the First Amendment); McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 341–42 (1995) (protecting an author's decision to remain anonymous under the First Amendment); Thornburgh v. Am. Coll. of Obstetricians & Gynecologists, 476 U.S. 747, 767 (1986) ("[R]eporting requirements raise the specter of public exposure and harassment of women who choose to exercise their . . . right . . . to end a pregnancy."); Brown v. Socialist Workers '74 Campaign Comm., 459 U.S. 87, 98 (1982) (discussing "risk of harassment" of contributors to minority party); *see* McConnell v. FEC, 540 U.S. 93 (2003) (upholding the constitutionality of campaign financing and political restrictions under the Bipartisan Campaign Reform Act of 2002 (BCRA), 116 Stat. 81, but acknowledging importance of First Amendment privacy interests); Wilson v. Layne, 526 U.S. 603, 611–12 (1999) (holding that unnecessary presence of news reporters in search of home violated Fourth Amendment); Planned Parenthood v. Casey, 505 U.S. 833, 887–98 (1992) (finding mandatory notice to husband constituted undue burden in exercise of constitutional right to abortion).

[101] 532 U.S. 514, 533 (2000) (quoting President's Commission of Law Enforcement and Administration of Justice, THE CHALLENGE OF A FREE SOCIETY 202 (1967)); *id.* at 543 (Rehnquist, C.J., dissenting).

[102] *E.g.*, California v. Ciraolo, 476 U.S. 207, 213 (1986) (observation from helicopter is not a "search"); Dow Chemical Co. v. United States, 476 U.S. 227, 234–35, 239 (1986) (aerial photograph is not a "search"). These cases could be read to allow unconstrained "overhead surveillance" by satellite, video surveillance, and e-mail interception. *Kyllo v. United States*, 533 U.S. 27, 33–34 (2001), places some limits on the use of technology to invade "private spaces," but the precise boundaries are quite unclear.

[103] Smith v. Maryland 442 U.S. 735, 743–44 (1979) (finding that "pen register" does not require warrant, since telephone numbers are disclosed to telephone company); United States v. Miller, 425 U.S. 435, 442–43 (1976) (finding depositor has no "reasonable expectation of pri-

communication on intermediaries, this opens a vast array of communications to government surveillance.[104]

Encroachment on informational privacy, moreover, need not initially involve explicit efforts to spy on citizens. As I put the point in 1991:

> The night watchman state is dead in America, if indeed it ever lived. Modern American government, like governments elsewhere, has taken progressively greater responsibility for functions that previously had been left to the market or other social structures. In the late twentieth century, the bureaucrat—who dispenses benefits and licenses, who hires and fires, who plans health care programs or fiscal policy—has replaced the police officer, judge, or soldier as the icon of government.
>
> In the course of her job, the bureaucrat learns more intimate details about citizens than would the police officer or the judge. Implementa-

vacy" in bank records); Cal. Bankers Ass'n v. Shultz, 416 U.S. 21, 54 (1974) (finding that required maintenance of bank records does not violate Fourth Amendment). Given the emerging availability of cell phone tracking technology, *see* Amy Harmon, *Lost? Hiding? Your Cellphone Is Keeping Tabs*, N.Y. TIMES, Dec. 21, 2003, at A1, access to telephone records will become even more revealing.

Again, there may be limits on the revelations of particular trusted intermediaries, *e.g.*, Ferguson v. City of Charleston, 532 U.S. 67, 79–80 (2001) (holding that patients have "legitimate expectation of privacy" in medical records), but those limits are far from sharply etched.

[104] *E.g.*, Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 627–29 (2003) (arguing that disclosure doctrine leaves Internet communications without constitutional protection). The capacity to examine the contents of e-mails through such technologies as Carnivore and ECHELON is constrained in some circumstances by the Electronic Communications Privacy Act, and subject to FISA under the USA PATRIOT Act. *Id.* at 656. Once access is gained, moreover, there is likely to be an arms race between cryptography-using subjects of surveillance and government monitors. Ted Bridis, *FBI Is Building a 'Magic Lantern'; Software Would Allow Agency to Monitor Computer Use*, WASH. POST, Nov. 23, 2001, at A15. This legal constellation allows proponents of increased surveillance to claim that statutory amendments decreasing privacy do not interfere with "constitutional rights."

An increasing number of employers, moreover, monitor the Internet connections of their employees. *See* Elia Zureik, Who Knows What About Whom? Towards a Generalized Surveillance, Presentation at the Third UNESCO Philosophy Forum (Sept. 14, 2003) (reporting more than two-thirds of employers monitor employees internet activities), *at* http://www.queensu.ca/sociology/Surveillance/publications-zureik.htm (last visited Sept. 30, 2004). Current doctrine imposes no limitations on the capacity of employers to provide the records of such monitoring to governmental officials or, presumably, pursuant to Section 215 of the USA PATRIOT Act, The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 [hereinafter USA PATRIOT Act], Pub. L. No. 107-56, § 215, 115 Stat. 272, 287–88, of officials to demand copies of logs of such monitoring.

The question of whether the government can access information obtained by "cookies" placed by private internet sites stands at the confluence of a variety of opaque statutory regimes including the Electronic Communications Privacy Act, 18 U.S.C. § 2510, which encompasses the Wiretap Act and the Stored Communications Act; the Computer Fraud and Abuse Act, 18 U.S.C. § 1030; the USA PATRIOT Act, § 215; the extended Bank Secrecy Act, 31 U.S.C. § 5311; and National Security Letter authority, 18 U.S.C. § 2709. *See, e.g.*, Lee Kovarsky, Note, *Tolls on the Information Superhighway: Entitlement Defaults for Clickstream Data*, 89 VA. L. REV. 1037 (2003) (discussing the collection of clickstream data and the legal rules that should govern it).

> tion and planning personnel have voracious appetites for information, and every license, benefit, or exemption makes the government privy to the details of a citizen's life. Information gathered in one arena is available for use in others. Similarly, the increasing rationalization and routinization of the private sector has generated stores of information potentially available to the government. Every employer accumulates information about her employees, every granter of credit files data about her customers, every transfer of funds leaves an increasingly accessible data trail, all of which is susceptible to government subpoena or request.[105]

The phenomenon has burgeoned in the last decade. Government has continued to collect more information, and records have become increasingly digitized and hence increasingly available for analysis and examination.[106] The exploding collection of consumer information by private sector actors, from retailers to credit intermediaries to insurance companies, moreover, has produced enormous pools of information which can be adapted to domestic surveillance.[107]

In the aftermath of September 11, many businesses volunteered or grudgingly surrendered access to their records to law enforcement or intelligence officials.[108] Others made access to their data warehouses available for purchase. For example, one private company, ChoicePoint, has contracted to provide a variety of federal agencies

---

[105] Seth F. Kreimer, *Sunlight, Secrets, and Scarlet Letters: The Tension Between Privacy and Disclosure in Constitutional Law*, 140 U. PA. L. REV. 1, 1 (1991).

[106] One example should suffice: EZ Pass technology, which allows prepayment of tolls, can double as a tracking mechanism. For more extensive examples, see A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1468–1502 (2000).

[107] *See* Andrew J. McClurg, *A Thousand Words Are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling*, 98 NW. U. L. REV. 63, 65–79 (2003) ("Acxiom's InfoBase profiler collects data from more than 15 million sources and contains demographic information on 95 percent of U.S. households. Experian boasts that its databases cover 98 percent of U.S. households and can contain more than 1000 data items per household. Polk's 'Automotive Profiling System' contains demographic and lifestyle information on more than 150 million vehicle owners and 111 million households. . . . By storing small text files called 'cookies' on the computers of persons visiting DoubleClick-affiliated sites, the company has stockpiled profiles of more than 100 million individuals," and continuing a list of other stockpiles of data.); *cf.* Peter Lyman & Hal R. Varian, *How Much Information?*, (2003) (finding that 5.4 billion gigabytes of information were stored in 2002, compared with 3.2 billion gigabytes in 1999), *available at* http://www.sims.berkeley.edu/research/projects/how-much-info-2003 (last visited Sept. 30, 2004).

[108] E-bay, for example, has volunteered to provide law enforcement with its enormous proprietary stock of data. *See* Ernest Miller & Nimrod Kozlovski, *eBay to Law Enforcement—We're Here to Help*, LAWMEME, Feb. 17, 2003, http://research.yale.edu/lawmeme. The FBI has obtained information voluntarily provided by organizations ranging from dive shop operators to supermarkets. Ben Worthen, *What to Do When Uncle Sam Wants Your Data*, CIO MAGAZINE, Apr. 15, 2003 (reporting a study in which forty-one percent of respondents said they are willing to share information without a court order if they believe it is in the interest of national security), *at* http://www.cio.com/archive/041503/data.html (last visited Sept. 30, 2004). Likewise, airlines have provided passenger information voluntarily (and possibly illegally) to government agencies seeking to prevent terrorism. *See infra* note 111.

the capacity to search and correlate a vast array of data the company gathers from private sources, ranging from credit bureaus to insurance underwriters to travel agencies, as well as local state and federal agencies, including motor vehicle records, liens, deed transfers, criminal records, voter rolls, and military personnel records.[109] The FBI, which provides desktop access to ChoicePoint for its agents, has taken the position that obtaining access to this information is "minimally intrusive," and is not substantially limited by the constraints developed in the 1970s.[110] The position is presumably echoed by the array of other federal agencies that make use of ChoicePoint and similar data services.[111] Conversely, the MATRIX system, based in Florida, proposes to link state, federal, and private databases in a searchable configuration.[112]

The response to the threat of terrorism, moreover, has substantially enhanced federal capacities to obtain information without the consent of the subjects or holders of data. The tragedy of September 11 made real risks that had heretofore been hypothetical; the costs of

[109] *See, e.g.*, Shane Harris, *Private Eye*, GOVERNMENT EXECUTIVE, Mar. 16, 2004 (detailing ChoicePoint's records and noting ChoicePoint owns nineteen billion records), *at* http://www.govexec.com/features/0304/0304s1.htm (last visited Sept. 30, 2004); Glenn R. Simpson, *Big Brother in Law: If the FBI Hopes to Get the Goods on You, It May Ask ChoicePoint*, WALL ST. J., Apr. 13, 2001, at A1. For ChoicePoint's own account of its "point and click" services, see ChoicePoint Business & Government Solutions, *at* http://www.cpgov.com (last visited Sept. 30, 2004). ChoicePoint has also begun to make its services broadly available to the private sector. *E.g.*, Adam Geller, *Employee Security Checks Go Retail*, COM. APPEAL, Mar. 7, 2004, at G1.

[110] Office of Gen. Counsel, Nat'l Sec. Law Unit, Guidance Regarding the Use of ChoicePoint for Foreign Intelligence Collection or Foreign Counterterrorism Investigations (Sept. 17, 2001) (providing legal opinion that ChoicePoint files are "publicly available data," and therefore "minimally intrusive"), http://www.epic.org/privacy/choicepoint/cpfbia.pdf; Simpson, *supra* note 109 (giving account of desktop access). In many FBI offices personally assigned computers are in a "closed" network; to access ChoicePoint, or any other "outside" network requires that a person go to a stand-alone terminal. Personal Communication from M.E. Bowman, Senior Counsel to the FBI (June 21, 2004) (on file with author).

[111] *E.g.*, Brian Bergstein, *Database Measured Terrorism Quotient*, May 20, 2004 (describing 120,000 person list of individuals with a "high terrorism quotient" provided by private database owner Sesint to federal authorities, based on "such factors as age, gender, ethnicity, credit history, 'investigational data,' information about pilot and driver licenses, and connections to 'dirty' addresses known to have been used by other suspects"), http://apnews.myway.com/article/20040520/D82M9B400.html. According to one report, the 120,000 list was refined to 1,200, which formed the basis for investigations and some arrests. Robert O'Harrow, Jr., *Anti-Terror Database Got Show at White House*, WASH. POST, May 21, 2004, at A12; *see also* Ryan Singel, *CAPPS II Stands Alone, Feds Say*, WIRED NEWS, Jan. 13, 2004 (discussing proposal to allow security personnel to verify travelers identities by checking commercial databases such as those owned by ChoicePoint, Acxiom and LexisNexis), *at* http://www.wired.com/news/privacy/0,1848,61891,00.html (last visited Sept. 30, 2004); Ryan Singel & Noah Shachtman, *Army Admits Using JetBlue Data*, WIRED NEWS, Sept. 23, 2003 (recounting release to Army contractor, Torch Concepts, of millions of records of JetBlue passengers and comparison of the data with available private sector data to "ferret . . . out . . . secretive people"), *at* http://www.wired.com/news/privacy/0,1848,60540,00.html (last visited Sept. 30, 2004).

[112] *See* MATRIX, *supra* note 11.

ignorance became horrifyingly concrete. In the immediate aftermath of that trauma, legislative and administrative changes have weakened statutory constraints on collection and sharing of data within the federal structure.[113] Likewise, international cooperation holds the possibility of allowing U.S. intelligence agencies to avoid domestic limits on electronic surveillance.[114] Identification of the Islamist bases of al Qaeda as a prime source of danger has fueled relaxation of administrative limits on surveillance of religious institutions, and Internet websites or bulletin boards.[115] At the same time the perceived needs of the fight against terrorism have loosened the administrative constraints imposed during the 1970s on the FBI's use of other investigative techniques.[116]

[113] Section 203 of the USA PATRIOT Act, Pub. L. No. 107-56, § 203, 115 Stat. 272, 278–81, amended FED. R. CRIM. P. 6(e)(3)(d) to permit disclosure of grand jury information when the matters involve "foreign intelligence and counterintelligence"; Section 504, 115 Stat. at 364–65, amended the FISA to permit consultation between intelligence officials conducting FISA-approved surveillance efforts and law enforcement officials.

[114] At least one source claims that British and U.S. intelligence agencies exchange surveillance information on each others' citizens, Phillip Knightley, *How Britain and the US Keep Watch on the World*, INDEP. (London), Feb. 27, 2004, although the scope of such cooperation has not been proved.

[115] *See* Attorney General John Ashcroft, Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations, pt. VI.A.2, at 22 (May 30, 2002) [hereinafter Ashcroft Guidelines] (authorizing suspicionless "visits" to "any place" or attendance at "any event open to the public."), *available at* http://www.usdoj.gov/olp/generalcrimes2.pdf; *id.* pt. VI.B.2, at 22 (authorizing suspicionless monitoring of online sites and forums); *see also id.* pt. VI.A.1, at 21 (authorizing maintenance of databases from any source).

Part VI.C.1 of the Ashcroft Guidelines cautions that authorized activities "do not include maintaining files on individuals *solely* for the purpose of monitoring activities protected by the First Amendment." *Id.* at 23 (emphasis added). Given the enthusiasm with which the current Justice Department parses its authority, presumably, files maintained partially for the purpose of monitoring First Amendment activities, but also for the purpose of preventing terrorism (or of gratifying the curiosity of the attorney general) would not fall under the prohibition.

[116] Like the guidelines they modified, the Ashcroft Guidelines provide:

> It is important that such investigations not be based solely on activities protected by the First Amendment or on the lawful exercise of any other rights secured by the Constitution or laws of the United States. When, however, statements advocate criminal activity or indicate an apparent intent to engage in crime, particularly crimes of violence, an investigation under these Guidelines may be warranted unless it is apparent, from the circumstances or the context in which the statements are made, that there is no prospect of harm.

Id. pt. I, at 7. *Compare* Attorney General Dick Thornburgh, Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Domestic Security/Terrorism Investigations, pt. 1 (Mar. 21, 1989) [hereinafter Thornburgh Guidelines], *at* http://www.usdoj.gov/ag/readingroom/generalcrimea.htm, *with* Ashcroft Guidelines, *supra* note 115, pt. I, at 7.

The Ashcroft guidelines also comment in Part III that "special care must be exercised in sorting out protected activities from those which may lead to violence or serious disruption of society." *Id.* at 13. However, where prior guidelines required FBI Headquarters approval and notice to the Justice Department before undercover operatives infiltrated organizations "in a manner that may influence the exercise of First Amendment rights, *see* Thornburgh Guidelines, *supra*, pt. IV.B.3, the Ashcroft guidelines drop or dilute that requirement.

Post-September 11 statutory innovations have provided new authority to demand information without judicial supervision or probable cause,[117] have obliged courts to issue secret subpoenas and "trap and trace orders" on an *ex parte* FBI showing of "relevance" rather

The prior guidelines directed that "[b]efore employing an investigative technique in an inquiry, the FBI should consider whether the information could be obtained in a timely and effective way by less intrusive means. . . . [T]he techniques used in an inquiry should generally be less intrusive than those used in a full investigation," *id.* pt. II.B.4, and required a showing of compelling circumstances for "highly intrusive" techniques, *id.* pt. II.B.6. The Ashcroft guidelines by contrast admonish: "The FBI shall not hesitate to use any lawful techniques consistent with these Guidelines, even if intrusive, where the intrusiveness is warranted." Ashcroft Guidelines, *supra* note 115, pt. I, at 7; *see also id.* pt. II.B.4, at 9 (discussing the choice of investigative techniques).

[117] The USA PATRIOT Act conferred upon the FBI new authority to issue "national security letters" that require the production of information without any showing of probable cause or judicial process, conferring on the FBI the new unconstrained and unilateral ability to invoke inquisitorial powers that previously resided in grand juries seeking to prosecute crimes. 18 U.S.C. § 2709(b)(1) (2000), amended by the USA PATRIOT Act, permits the FBI to demand secret access to telephone and ISP records without judicial approval so long as the "records sought are relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment." This authority has been challenged by *ACLU v. Ashcroft (Sealed Case 04 Civ. 2614 (VM)).* *See* ACLU, ACLU Challenge to "National Security Letter" Authority, *at* http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=15543&c=262 (last visited Sept. 30, 2004); *see also* 18 U.S.C. § 2703(c)(2).

Similar authority and constraints apply to the newly available national security letters to financial institutions seeking "a customer's or entity's financial records." 12 U.S.C. § 3414(a)(5)(A) (authorizing the release of financial records for "foreign counter intelligence purposes . . . provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States").

Title 31, section 5312(a)(2) of the United States Code extends National Security Letter authority over "financial institutions" to include "an operator of a credit card system;" "a travel agency;" "a casino, gambling casino;" or "any other business designated by the Secretary whose cash transactions have a high degree of usefulness in criminal, tax, or regulatory matters." 31 U.S.C. § 5312(a)(2) (2002).

The "financial records" to which the FBI may demand access include any "information known to have been derived from, any record held by a financial institution pertaining to a customer's relationship with the financial institution." 12 U.S.C. § 3401(2). Unless the definition of what records pertain "to the customer's relationship" is construed narrowly, it appears that the FBI now has secret and unsupervised access to many commercial databases in the private sector, so long as it can claim the records are "relevant to an authorized investigation of international terrorism." *Cf.* Waye v. First Citizen's Nat'l Bank, 846 F. Supp. 310, 316 (M.D. Pa. 1994) (holding that cancelled checks are "financial records"). The requirement that the request be one "for a customer or entity's financial records" may preclude plenary dragnet searches or data mining.

Likewise, the Health Insurance Portability and Accountability Act (HIPAA) regulations provide that, "A covered entity may disclose protected health information to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act (50 U.S.C. § 401) and implementing authority (e.g., Exec. Order No. 12,333)." 45 C.F.R. § 164.512(k)(2).

than probable cause,[118] and have authorized the secret issuance of surveillance and wiretap orders by the FISA court under a standard quite different from normal "probable cause."[119] Even where acquisition of information is constrained, the exponential increase in the capacity to aggregate and analyze information obtained by non-coercive and non-surreptitious measures gives government the opportunity to acquire vastly more extensive and penetrating oversight than the capabilities provided by the techniques at issue in *Laird v. Tatum*.[120] Not only are current data processing techniques able to transcend the "practical obscurity"[121] that previously attended the size and difficulty of accessing large amounts of data (as for example, by searching out the past addresses or buying habits of targeted individuals), but they are able as well to engage in "data mining" to discover information that was previously only implicit in available data (for example by correlating purchasers of particular periodicals with

[118] Under Section 215 of the USA PATRIOT Act, 115 Stat. at 287–88, the FBI now has authority to trigger non-discretionary judicial orders to obtain "any tangible things (including books, records, papers, documents, and other items) for an investigation . . . to protect against international terrorism." 50 U.S.C. § 1861(a)(1) (2004). However, the investigation may not be "conducted of a United States person solely upon the basis of activities protected by the first amendment to the Constitution of the United States." *Id.* § 1861(2)(B). More narrowly, the FBI can now obtain orders for the production of the contents of consumer reports on a similar showing. 15 U.S.C. § 1681u(c) (2000).

The authority granted by the USA PATRIOT Act also provides for automatic issuance judicial orders for pen registers and trap and trace devices without probable cause. 50 U.S.C. § 1842(a)(1). Courts requested to issue an order authorizing the use of pen registers and trap and trace devices for internet activities and e-mail must issue such orders when a Government attorney certifies that the information likely to be obtained is "information relevant to an ongoing investigation to protect against international terrorism" and that the investigation (if it is an investigation of a U.S. person) "is not conducted solely upon the basis of activities protected by the first amendment to the Constitution." *Id.* § 1842(c)(2).

[119] Section 218 of the USA PATRIOT Act, 115 Stat. at 291, amended FISA to permit secret warrants for interception of communications or physical searches to issue without probable cause to believe that a crime has been or is being committed so long as foreign intelligence gathering or antiterrorist investigation is a "significant purpose" of the surveillance (as opposed to the "primary" purpose of the surveillance), and there is probable cause to believe that the target (or owner of the premises) is an "agent of" a foreign organization. *See generally In re* Sealed Case, 310 F.3d 717, 719–20 (Foreign Int. Surv. Ct. Rev. 2002). For "United States persons," a somewhat higher showing of probable cause is required to show that the person is an "agent of a foreign power." 50 U.S.C. § 1801(b)(2) (including persons as to whom there is probable cause to believe that they have "knowingly" assumed "a false or fraudulent identity," gathered intelligence in a fashion that "may involve" violation of a federal statute, or aided or abetted the same).

[120] *See, e.g.*, Froomkin, *supra* note 106 (describing synergistic effect of increase in computer storage and networking along with increased data collection technologies). The GAO reports that 199 separate data mining projects are currently being undertaken by federal agencies, fifty-four of which use private sector data. GAO, DATA MINING, *supra* note 20.

[121] U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 762 (1989) (recognizing the value of practical obscurity of FBI rap sheets and protecting them from disclosure under the Freedom of Information Act).

membership in particular organizations or presence at particular rallies, and estimating the probability that particular subjects will rent particular videos, or vote Republican).[122]

B. The Present Danger

It is a mistake to view the structures of information control that developed in response to the Nixon abuses solely as a matter of individual rights to avoid surveillance, or to maintain "privacy" in the abstract. Limits on surveillance constitute structural hedges that make other abuses more difficult. In particular, retaliation for dissent is less likely if dissenters are not tracked.[123] Yet, even as the structural limits of the 1970s on surveillance decay, responses to terrorism sharpen the dangers to political liberty.

In the world after September 11, while we are still quite a distance from the prospect of a military coup, the potentials for retaliation have multiplied. Attorney General John Ashcroft has regularly stated that in pursuing what he refers to as a "fundamentally different approach to law enforcement," he encourages his employees to "think outside of the box—but never outside of the constitution."[124] Unfortunately, on this subject, like others, the Attorney General's concept of constitutional constraints may diverge from those to which we are accustomed; the current administration seems to view constitutional rights as obstacles to be circumnavigated rather than ideals to be attained. As long as there is a colorable argument that determinative Supreme Court precedent does not directly preclude an action, the Ashcroft Justice Department seems to consider that it is not "outside of the constitution."

The current administration has claimed the right to imprison "unlawful combatants" without process and without judicial review.[125]

---

[122] *See, e.g.*, K.A. Taipale, *Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data*, 5 COLUM. SCI. & TECH. L. REV. 2, pt. I.A (2003/2004) (outlining the importance of data mining and "knowledge discovery" techniques and contrasting them with simple data inquiry techniques), *at* http://www.stlr.org/cite.cgi?volume=5&article=2; Tal Z. Zarsky, *Desperately Seeking Solutions: Using Implementation Based Solutions for the Troubles of Information Privacy in the Age of Data Mining and the Internet Society*, 56 ME. L. REV. 13, 42 (2004).

[123] Similarly, one of the major objections to domestic military intelligence is that it makes military less dependent on civilian branches (and localities) in domestic operations. *E.g.*, PYLE, *supra* note 21, at 406 (discussing how the Attorney General opposed military intelligence because it posed dangers to civilian control and federalism).

[124] U.S. Attorney General John Ashcroft, Remarks at the Eighth Circuit Judges Conference (Aug. 7, 2002), http://www.usdoj.gov/ag/speeches/2002/080702eighthcircuitjudgesagremarks.htm.

[125] *See* Brief for the Petitioner, Rumsfeld v. Padilla, 124 S. Ct. 2711 (2004) (No. 03-1027). This brief maintains that the President has inherent "authority to seize and detain enemy combatants wherever found," *id.* at 38, whether those individuals are citizens or aliens, and inside or

The Bush administration initially claimed authority to prosecute before secret and unreviewable military tribunals any non-citizen the president deemed an "unlawful combatant."[126] It has since provided some basic procedural protections by regulation to defendants in military tribunals, but continues to maintain in court the position that it has unreviewable authority to detain "enemy combatants," whether lawful or unlawful, citizen or alien.[127] The administration has, so far as the public record reveals, sought to exercise these powers fairly narrowly; it has not rounded up critics and incarcerated them in naval brigs. Further, a majority of the Supreme Court has rejected the claims that the efforts to detain "unlawful combatants" can proceed entirely free from the constraints of judicial review or due process.[128] But the Court has not yet clearly delineated the limitations the Constitution imposes, and the powers the Bush Administration

outside the territory of the United States, and claiming that a statute which interferes with this authority would raise "substantial constitutional doubts," *id.* at 49.

[126] President's Military Order of November 13, 2001, Detention, Treatment, and Trial of Certain Non-Citizens in the War Against Terrorism, 66 Fed. Reg. 57,833 (Nov. 13, 2001) (authorizing detention and military trial of an individual if the president finds there is "reason to believe that such individual . . . (i) is or was a member of the organization known as al Qaida; (ii) has engaged in, aided or abetted, or conspired to commit, acts of international terrorism, or acts in preparation therefore . . . ; or (iii) has knowingly harbored one or more" of such individuals); *see, e.g.*, Neal K. Kaytal & Laurence H. Tribe, *Waging War, Deciding Guilt: Trying the Military Tribunals*, 111 YALE L.J. 1259 (2002) (criticizing the military tribunal order); Comm. on Military Affairs & Justice, Ass'n of the Bar of the City of New York, Inter Arma Silent Leges: *In Times of Armed Conflict, Should the Laws be Silent?* (Dec. 2001) (reporting on the president's military order of Nov. 13, 2001), *available at* http://www.abcny.org/pdf/Should%20the%20Laws%20be%20Silent%204.pdf (last visited Sept. 30, 2004).

[127] Petitioner's Brief, *Padilla* (No. 03-1027). Indeed, in recent draft legislation (Patriot II), the Ashcroft Justice Department has begun to seek authority to revoke the citizenship of individuals who engage in the activities of a group designated as a "terrorist organization," potentially relegating even American citizens to the legal netherworld the administration purports to construct for aliens. *See* Dep't of Justice, Domestic Security Enhancement Act of 2003: Section-by-Section Analysis (depicting a confidential draft for Congress that was leaked to the Center for Public Integrity), http://www.publicintegrity.org/dtaweb/downloads/Story_01_020703_Doc_1.pdf (last visited Sept. 30, 2004). The Department of Justice has since distanced itself from the Patriot II legislative proposal, but certain elements of the package are being pushed through other proposals. *See, e.g.*, Audrey Hudson, *'Patriot II' Bid Garners Little Favor on Hill*, WASH. TIMES, Sept. 12, 2003, at A1 (quoting Sen. Leahy, saying that, "After all the criticism of that sequel and the secretive way it was drafted, the administration now has decided to push a sequel, without calling it a sequel.").

[128] Hamdi v. Rumsfeld, 124 S. Ct. 2633 (2004) (rejecting claim that separation of powers precluded relief for citizen captured on battlefield and detained without any due process); *see id.* at 2652 (Souter, J., & Ginsburg, J., concurring in the judgment and dissenting in part) (stating that executive detention is statutorily improper); *id.* at 2660 (Scalia, J., & Stevens, J., dissenting) (stating that detention is unconstitutional in the absence of congressional suspension of habeas corpus); Rasul v. Bush, 124 S. Ct. 2686 (2004) (holding that non-citizens detained in Guantánamo Bay may seek writs of habeas corpus); Rumsfeld v. Padilla, 124 S. Ct. 2711, 2735 n.8 (2004) (Stevens, J., Souter, J., Ginsberg, J., & Breyer, J., dissenting) (stating that protracted detention of non-citizens is illegal under statute).

seeks would allow it to target inconvenient critics free of either judicial review or public disclosure.

Of more current sobering concern is the use of the "material witness" authority. Let me begin by mentioning the plight of Osama Awadallah who was arrested as a "material witness" in the aftermath of September 11. He was not arrested because there was probable cause to believe that he had committed any crime, but because the Justice Department asserted that in the words of 18 U.S.C. § 3144 his "testimony was material" in a grand jury proceeding. Mr. Awadallah had known one of the September 11 hijackers a year before. He was arrested, shackled for three days, and incarcerated incommunicado for twenty-one days before it became clear that he in fact had no connection to al Qaeda, after he answered several hundred questions without immunity before a grand jury.[129] At that point, he was charged with perjury because at one point in his interrogation, he allegedly falsely stated that he "didn't know a Khalid," and denied writing a sentence containing the name "Khalid" in an examination booklet.[130] The trial court threw out his perjury prosecution on the ground that the "material witness" statute was misused.[131] On appeal, the Second Circuit reinstated the prosecution and upheld the invocation of the material witness statute.[132]

The main precedent invoked by the government was a case from 1971 in which a nineteen year old anti-war activist was grabbed off the street by the Nixon-Mitchell Justice Department, on the eve of a major demonstration in Washington, and dragged off to a grand jury in Seattle as part of an eighty-four city, eleven hundred witness "investigation" of the anti-war movement by the Justice Department's "Internal Security Division."[133] The Ashcroft Justice Department has not, as far as has yet been disclosed, engaged in such wholesale harassment of critics. But it claims the legal capacity to do so, as long as it is investigating any criminal offense.

In this context, the availability of databases correlating information on the exercise of rights of dissent or nonconformism with other data becomes particularly threatening. It appears that the recent erroneous incarceration of attorney Brandon Mayfield for two weeks under the material witness statute stemmed from the fact that the similarity of his fingerprint to a fingerprint connected to a terrorist bombing appeared in juxtaposition with the facts that he had prayed

[129] United States v. Awadallah, 202 F. Supp. 2d 55, 58 (S.D.N.Y. 2002).

[130] *Id.* at 59.

[131] *Id.* at 61.

[132] United States v. Awadallah, 349 F.3d 42, 75 (2d Cir. 2003).

[133] *Id.* at 50, 54; Bacon v. United States, 449 F.2d 933 (9th Cir. 1971); *see* DONNER, *supra* note 24, at 365–68; Michael E. Deutsch, *The Improper Use of the Federal Grand Jury: An Instrument for the Internment of Political Activists*, 75 J. CRIM. L. & CRIMINOLOGY 1159, 1181 (1984).

at a mosque and had represented a suspected terrorist in a child custody proceeding.[134]

Under current statutes, the conduct that constitutes a criminal offense which can form the predicate for invocation of the "material witness" provisions appears to cut an extraordinarily broad swath across rights of free association. Current criminal statutes allow the prosecution of individuals who "knowingly provide material support or resources to a foreign terrorist organization, or attempt[] or conspire to do so."[135] And Executive Order 13224 allows the seizure of assets from persons determined by the secretary of the Treasury to assist designated foreign persons who pose a risk of terrorism, or to be "otherwise associated" with such persons. These are the statutes that the Justice Department has invoked in its prosecution of so-called "sleeper cells," based not on any violent conduct but on conspiracies to give money or other "material support" to individuals or organizations that may engage in such conduct. The statutes extend to organizations that engage in both violent and nonviolent activities (like the Irish Republican Army ("IRA") or the African National Congress ("ANC")), as well as foundations that may be "associated with" such organizations.

Faced with such statutes, there is a strong incentive to steer clear of controversial associations. The administration of the University of California San Diego recently decided to forbid a student website from linking to the website of the Revolutionary Armed Forces of Colombia for fear that this might be construed as "providing material

[134] According to one report,

> Federal officials told *Newsweek* that they doubt Mayfield has been innocently swept up in a case of international intrigue. Mayfield married an Egyptian woman and converted to Islam 16 years ago. The couple was active in a local Oregon mosque whose members had openly protested government antiterror policies . . . [and] in 2002 Mayfield had volunteered to provide legal help [in a child custody matter] for Jeffrey Battle, one of the ringleaders of the Portland Seven—a group of local jihadists who had flown to Asia after 9/11 in an unsuccessful effort to fight with the Taliban."

Michael Isikoff, *An American Connection*, NEWSWEEK, May 17, 2004, http://msnbc.msn.com/id/4933790/; *see also* Sarah Kershaw & Eric Lichtblau, *Bomb Case Against Lawyer Is Rejected*, N.Y. TIMES, May 25, 2004, at A16; Sarah Kershaw & Eric Lichtblau, *Spain Had Doubts Before U.S. Held Lawyer in Blast*, N.Y. TIMES, May 26, 2004, at A1.

[135] 18 U.S.C. § 2339B(a)(1) (2002). In *Humanitarian Law Project v. U.S. Department of Justice*, 352 F.3d 382, 405 (9th Cir. 2003), the Ninth Circuit held that to convict for a violation of section 2339B, the government "must prove beyond a reasonable doubt that the accused knew that the organization was designated as a foreign terrorist organization or that the accused knew of the organization's unlawful activities that caused it to be so designated." The court also concluded that portions of the statutory definition of "material support" were void for vagueness. *Id.* Even though the court subsequently vacated its opinion and granted the government's petition for rehearing en banc, *Humanitarian Law Project*, 382 F.3d 1154 (9th Cir. 2004), Congress is considering legislation that would both implement the Ninth Circuit's knowledge requirement and clarify the definition of "material support." *See* H.R. 10, 108th Cong. § 2043(2004).

support," but backed off in the face of protests.[136] That incident is, perhaps, amusing but especially combined with the "material witness" power claimed by the Justice Department, matters may get deadly serious in short order.

Mosques challenging federal surveillance powers report substantial declines in attendance and religiously mandated contributions,[137] and the Justice Department's "material support" prosecutions include a recent action against a computer science student, Sami Omar al-Hussayen for maintaining websites which contained Islamist writing—a prosecution which only ran aground on the common sense of an Idaho jury.[138] The breadth of the "material support" statute has led some courts to hold parts of it to be unconstitutional, but these determinations are on appeal.[139]

For non-citizen residents of the United States, the threat of retaliation is even more foreboding. In the backwash of September 11, the administration rounded up over one thousand men of near eastern origin, held them for an extended time period, and deported most of them, notwithstanding the absence in many cases of any substantial connection with terrorist threats.[140] The USA PATRIOT Act makes even unknowing association with terrorists a deportable offense, and allows the attorney general to order detention of aliens without any prior showing or court ruling that the person is danger-

[136] Declan McCullagh, *University Backs Down on Link Ban*, CNET NEWS.COM, Oct. 8, 2002, *at* http://news.com.com/2100-1023-961297.html.

[137] Plaintiffs' Response to Defendants' Motion to Dismiss at 8, Muslim Cmty. Ass'n of Ann Arbor v. Ashcroft (E.D. Mich. 2003) (No. 03-72913), *available at* http://www.aclu.org/Files/OpenFile.cfm?id=14305.

[138] *See, e.g.*, Bob Fick, *Trial Merges Terror Charges, Free Speech*, BOSTON GLOBE, May 28, 2004 (quoting a prosecutor alleging that "Al-Hussayen provided the linkage to create the platform and then the content to advocate extreme jihad"), *available at* http://www.boston.com/news/nation/articles/2004/05/28/trial_merges_terror_charges_free_speech/; Richard B. Schmitt, *Free Speech Crux of Terrorism Case: Sami Omar Al-Hussayen's Lawyers Say He Was Trying to Foster Dialogue on His Fatwa-filled Websites*, L.A. TIMES, May 23, 2004, at A25 (recounting prosecution of computer scientist who helped design websites containing Islamist writings under "material support" statute). Apparently Mr. Al-Hussayen is also charged with "failing to list all professional, social and charitable institutions to which [he] belongs." Dahlia Lithwick, *I, Visa*, SLATE MAGAZINE, May 12, 2004. Although acquitted on the terrorism charges, Al-Hussayen agreed to be deported in exchange for the remaining immigration charges against him being dropped. Betsy Z. Russell, *Feds Drop Remaining Charges Against Al-Hussayen*, SPOKESMAN REV. (Spokane, Wash.), June 30, 2004.

[139] Humanitarian Law Project v. Dep't of Justice, 352 F.3d 382 (9th Cir. 2003) (requiring specific intent to further terrorist aims and holding prohibition of providing "training" and "personnel" to be impermissibly vague); Humanitarian Law Project v. Ashcroft, 309 F. Supp. 2d 1185 (C.D. Cal. 2004) (holding prohibition of provision of "expert advice or assistance" to be impermissibly vague).

[140] *E.g.*, OFFICE OF THE INSPECTOR GEN., DEP'T OF JUSTICE, THE SEPTEMBER 11 DETAINEES: A REVIEW OF THE TREATMENT OF ALIENS HELD ON IMMIGRATION CHARGES IN CONNECTION WITH THE INVESTIGATION OF THE SEPTEMBER 11 ATTACKS (2003), *available at* http://www.usdoj.gov/oig/special/0306/full.pdf; David Cole, *Enemy Aliens*, 54 STAN. L. REV. 953, 961 (2002).

ous where he "has reasonable grounds to believe that the alien is engaged in any other activity that endangers the national security of the United States."[141] And the administration claims the right to choose political bases to deport non-citizens for immigration violations, no matter how trivial, at its sole discretion.[142]

Surveillance and data banks carry as well the prospect of other sanctions. Both citizens and aliens face the prospect of potential exclusion from air travel if they appear on governmentally disseminated "no fly lists" or "watch lists" or if their characteristics or associations trigger scrutiny.[143] The dissemination of watch lists to both public and private sectors can, in turn, generate a variety of other constraints, as recipients exercise discretion over the allocation of opportunities and benefits.[144] And, having become the focus of attention by virtue of appearance on a watch list disseminated to law enforcement officers, officers are free to use collateral criminal violations, no matter how minor, as the predicate for searches or prosecution.[145] In the

[141] USA PATRIOT Act, Pub. L. No. 107-56, § 411, 115 Stat. 272, 345–50 (2001) (association); *id.* § 412, 115 Stat. at 350–52 (detention for up to six months).

[142] *See* Reno v. Am. Arab Antidiscrimination Comm., 525 U.S. 471, 488 (1999) ("[A]n alien unlawfully in this country has no constitutional right to assert selective enforcement as a defense against his deportation."). The fate of the "L.A. 8," a group of Arab community organizers originally accused of advocating world communism under a now-repealed statute, which was at issue in *Reno* remains unresolved, and it appears two of the eight might now face deportation under the USA PATRIOT Act for fundraising and distribution of literature that was legal at the time it occurred. *See* Editorial, *Drop This Case*, WASH. POST, Nov. 5, 2003, at A28 (detailing proposed deportation for having held fundraising events and rallies and having distributed magazines between 1984 and 1986).

[143] *E.g.*, Ann Davis, *Post-Sept. 11 Watchlist Acquires Life of its Own*, WALL ST. J., Nov. 19, 2002, at 1 (describing wide circulation and collateral consequences of FBI watch lists of suspected "terrorists"); Sara Kehaulani Goo, *ACLU Files Suit Over 'No-Fly' List*, WASH. POST, Apr. 7, 2004, at A3; Adam Liptak, *A.C.L.U. to Withdraw from Charity Drive*, N.Y. TIMES, Aug. 1, 2004 (describing certification required of federal employee charities that they would not knowingly employ people whose names appeared on several government terrorism watch lists), http://www.nytimes.com/2004/08/01/politics/01aclu.html; *see also* U.S. GEN. ACCOUNTING OFFICE, REP. NO. GAO-03-332, INFORMATION TECHNOLOGY: TERRORIST WATCH LISTS SHOULD BE CONSOLIDATED TO PROMOTE BETTER INTEGRATION AND SHARING (2003) (describing the problem of multiple watchlists with little supervisory control), *available at* http://www.gao.gov/new.items/d03322.pdf.

[144] Ryan Singel, *Data Scant for Watchlist Usage*, WIRED NEWS, May 17, 2004 (describing 120,000 person "watch list" produced by the "Terrorism Screening Center," available to highway patrol officers, airline screeners, and border control officials), *at* http://www.wired.com/news/privacy/0,1848,63478,00.html; Guy Taylor, *FBI Up for Private Screens*, WASH. TIMES, Mar. 26, 2004 (recounting FBI and DHS plan to develop databases that will allow private companies to submit lists of individuals to be screened for connections with terrorism). In addition, the USA PATRIOT Act obliges banks and other financial institutions to verify the identity of their customers and check those identities against government-provided watch lists. USA PATRIOT Act § 312(a), 115 Stat. at 304–05 (codified at 31 U.S.C. § 5318(i)).

[145] Atwater v. City of Lago Vista, 532 U.S. 318 (2001) (holding that custodial arrest for violation of seatbelt statute does not violate Fourth Amendment); Arkansas v. Sullivan, 532 U.S. 769 (2001); Whren v. United States, 517 U.S. 806 (1996) (subjective basis for search is constitutionally irrelevant if probable cause is present).

wake of September 11, the Attorney General announced an intention to use minor charges against those he suspects of being linked to terrorism where proof of more substantive violations is unavailable;[146] there is no reason to believe that local officials will be less aggressive.

The potential impact of dossiers and watch lists on dissent and free expression is shadowed by the risks that the lists may be politicized. In gathering data, the FBI has chosen to monitor political demonstrations through its terrorism notification system,[147] and has specifically refused the advice of the Justice Department's Inspector General to disentangle its terrorist surveillance from surveillance of political protest.[148] The prospect of an FBI dossier alone may well be sufficient to deter non-citizens, applicants for government jobs, or those who seek to avoid entanglement as material witnesses from participating in dissenting activity.

Conversely, there has been at least one high profile effort by Republican legislators to use anti-terrorism surveillance data for partisan

[146] U.S. Attorney General John Ashcroft, Prepared Remarks for the U.S. Mayors Conference (Oct. 25, 2001) ("Robert Kennedy's Justice Department, it is said, would arrest mobsters for 'spitting on the sidewalk' if it would help in the battle against organized crime. It has been and will be the policy of this Department of Justice to use the same aggressive arrest and detention tactics in the war on terror."), http://www.usdoj.gov/ag/speeches/2001/agcrisisremarks10_25.htm; U.S. Attorney General John Ashcroft, Testimony of Attorney General John Ashcroft House Select Committee on Homeland Security (July 11, 2002) ("The Justice Department of Robert F. Kennedy, it was said, would arrest a mobster for spitting on the sidewalk if it would help in the fight against organized crime. In the war on terror, it has been the policy of this Department of Justice to be equally aggressive."), http://www.usdoj.gov/ag/testimony/2002/071102agtestimony.htm.

[147] *See, e.g.*, Karen Abbott, *Warnings Precede Party Conventions*, ROCKY MTN. NEWS, July 24, 2004 (describing FBI questioning twenty-one year old American Friend Service Committee intern at her home as part of investigation of "protestors and anarchists" by "Joint Terrorism Task Force," and threats to "use more intrusive efforts"). *Compare* FBI Response to Media Misinterpretation of its Law Enforcement Sensitive Intelligence Bulletin (Oct. 15, 2003) (claiming that the FBI does not surveil protestors, but including "Law Enforcement Sensitive Intelligence Bulletin" describing, *inter alia* the fact that "[p]rotestors often use the internet to recruit, raise funds, and coordinate their activities prior to demonstrations" and directing that "[l]aw enforcement agencies should be alert to these possible indicators of protest activity and report any potentially illegal acts to the nearest FBI Joint Terrorism Task Force."), *available at* http://www.fbi.gov/response.htm, *with* Eric Lichtblau, *F.B.I. Scrutinizes Antiwar Rallies*, N.Y. TIMES, Nov. 23, 2003, at A1 (detailing FBI monitoring of protest activity).

[148] The Office of the Inspector General of the Department of Justice recommended "transferring responsibility for investigating crimes committed by environmental, animal rights, and other domestic radical groups or individuals from the Counterterrorism Division to the Criminal Investigative Division." OIG, FBI'S EFFORTS, *supra* note 9, at 50. The FBI refused, *id.* at 90–98 app.8. The Inspector General reiterated its belief that "the FBI's priority mission to prevent high-consequence terrorist acts would be enhanced if the Counterterrorism Division did not have to spend time and resources on lower-threat activities by social protestors or on crimes committed by environmental, animal rights, and other domestic radical groups or individuals." *Id.* at 94. More details might well be contained in "Appendix 6" of the audit report, entitled "Potential for Criminal Activity at Antiwar Protests," but that appendix was redacted.

purposes.[149] Although the FAA has issued a rule limiting release of the precise data involved in this case,[150] it is far from clear that all surveillance data is similarly protected, or that the nominal protections would be effective in the face of determined efforts to seek retaliation.[151] If I were an orthodox Jew, which I am not, who frequented rib joints surreptitiously, which I do not, I might well think twice before crossing an FBI agent with desktop access to my credit card receipts.

III. "GOOD FENCES MAKE GOOD NEIGHBORS": HEDGES AGAINST REPRESSION

The limits imposed on domestic intelligence during the 1970s were in part, it must be acknowledged, a sort of willful blindness. They existed in tension both with bureaucratic imperatives and the apparent demands of the effort to protect our country from terrorist attacks. As Pyle points out, a bureaucrat is far more likely to be disciplined for not knowing information his superior desires than for collecting too much information.[152] And in the aftermath of September 11 the danger is not simply one to career advancement but the threat of physical catastrophe.

I have long maintained that negative examples play an important role in constitutional analysis: it is easier to identify and achieve consensus on the evils to be avoided than on the good to be attained, since goods are often plural and inconsistent. Likewise, it is often easier to reverse engineer legal doctrine if one has a clear idea about the threats it seeks to counter. The abuses of the 1970s played the role of legal landmark in much thinking about intelligence oversight before September 11. Today, we are often tempted to replace that

---

[149] *See* David Jackson, *Homeland Security Agency Says It Spent 40 Minutes on Search for Dems*, DALLAS MORNING NEWS, June 17, 2003, at 3A; R. Jeffrey Smith, *In Texas Feud, A Plane Tale of Intrigue; U.S. Role in GOP Hunt for Democratic Lawmakers Is Still Murky*, WASH. POST, June 7, 2003, at A1 (detailing efforts by staff of House Rep. Tom Delay to use resources of the Justice Department, the Department of Transportation, and the Department of Homeland Security to track down Democratic state legislators whose absence was blocking a Republican redistricting plan in Texas).

[150] R. Jeffrey Smith, *FAA Sets New Rules After Flap Over Search*, WASH. POST, July 16, 2003, at A21.

[151] Criminal prohibitions on disclosure of the identity of CIA operatives famously failed to deter the leaking of the identity Valerie Plame as retaliation for the report by her husband Joseph Wilson that cast doubt on administrative claims about the Iraqi nuclear program. *E.g.*, Richard B. Schmitt, *Ex-Diplomat Whose Wife Was Outed at CIA Is Next to Throw Book at Bush*, L.A. TIMES, Apr. 30, 2004, at A11; *see also* Joseph Wilson, Meet the Press Interview, May 2, 2004 ("I mention in the book that there are also reports from journalists back to me that they're fearful of writing these stories. One journalist said because he was afraid he would end up in Guantánamo . . . . Another one said that, of course, they had two children in private schools and a mortgage."), http://www.msnbc.msn.com/id/4880116.

[152] PYLE, *supra* note 21, at 391.

landmark with the crater of ground zero: whatever else we must achieve, we are told, we must avoid another September 11.

This presentation of the issue, however, rests on a false dichotomy. One way to "avoid September 11" is to ground all airplanes. One way to avoid forty-three thousand deaths a year would be to abandon auto travel. Yet, of course, our country chooses to do neither. The real issue is whether the reduction in threat is worth the potential cost to constitutional liberty.

As a civil liberties lawyer, evaluating the security benefits of uncontrolled domestic surveillance and data mining exceeds my core competence, though I would note in passing that the emerging programs are not without their tough-minded and knowledgeable critics.[153] Rather, having adumbrated some of the costs in political freedom that inhere in uncontrolled surveillance and data mining, I turn now to a few proposals on how those costs might be mitigated, in a fashion reasonably consistent with the need to build a domestic system to deal with the threat of terrorist assaults.

A. "The Former Can Hold No Terror": Substantive Legal Protection

Responding to concerns about the effect that government deployment of information might have on constitutional rights a generation ago, then-Judge Scalia commented:

> The line of permissibility, we think, falls not between criticism of ideas in general and criticism of the ideas contained in specific books or expressed by specific persons; but rather between the disparagement of ideas (general or specific) and the suppression of ideas through the exercise or threat of state power. If the latter is rigorously proscribed . . . the former can hold no terror.[154]

[153] For example, security expert Bruce Schneier argues that when one takes into account the cost of false alarms, the diversion of attention, and the prospect of terrorists attempting to game the system, data mining and data warehousing are likely to decrease rather than increase security on balance. BRUCE SCHNEIER, BEYOND FEAR 164–65 (2003) (critiquing CAPPS II); *id.* at 188–90 (critiquing data mining to find terrorists); *id.* at 253–54 (critiquing TIA). Moreover, if we seek cooperation of local immigrant communities, there must be some assurance that the information they submit will not be misused. Current broad and confrontational policies probably make this unlikely; in the medium run, avoiding broad public backlash will depend on assuring the public that abuses are not occurring. *See* RICHARD A. CLARKE, AGAINST ALL ENEMIES: INSIDE AMERICA'S WAR ON TERROR 256–57 (2004) ("To protect our civil liberties and defeat the terrorists, we need to be careful not to do things that create a popular backlash against security measures. As the widespread opposition to the unfortunately named Patriot Act proves, Attorney General Ashcroft has not managed that balancing act.").

[154] Block v. Meese, 793 F.2d 1303, 1314 (D.C. Cir. 1986) (Scalia, J); *cf.* Steven Pfaff, *The Limits of Coercive Surveillance: Social and Penal Control in the German Democratic Republic*, 3 PUNISHMENT & SOC'Y 381, 394–95 (2001) (describing the effectiveness of the GDR Stasi as based on the combination of surveillance with the power of arbitrary arrest, blackmail, "systematic discrediting," and the "haunting fear that you could be arrested anytime . . . . the Stasi . . . knew everything");

But the converse is also true. If prophylactic constraints on the acquisition and dissemination of information within the government are loosened, direct protections against the abuse of that information need to be strengthened. To the extent that government officials can single out dissenters more easily for adverse treatment, protection of dissent requires stronger substantive and procedural constraints on the capacity of the officials to administer that treatment. This insight suggests several implications.

First, as transparency increases, the increased danger of retaliation against constitutionally protected activities should bring with it heightened scrutiny of the exercise of government discretion. At the level of substance, the Court's commitment to the prohibition of unconstitutional conditions becomes increasingly important.[155] At the level of procedure, the heightened danger of covert unconstitutional retaliation should bring with it more rigorous regard for the demands of notice and hearing before the government imposes disadvantages on the basis of shared information—whether those disadvantages consist of placement on "no fly lists" or deportation. The vast increase in the availability of information regarding individuals will make it ever easier to develop purportedly neutral profiles that in fact and in intent focus disadvantages on disfavored political, religious, or ethnic groups. This potential manipulation should generate more willingness to investigate the reasons for exercises of discretion when they are challenged.[156]

In a world of increased informational interpenetration, transparency should run in both directions. If government officials are better

William J. Stuntz, *Privacy's Problem and the Law of Criminal Procedure*, 93 MICH. L. REV. 1016, 1077 (1995) (arguing that "the problem is not information gathering but violence").

[155] As the Court explained in *United States v. American Library Ass'n*: "Under this doctrine 'the government "may not deny a benefit to a person on a basis that infringes his constitutionally protected . . . freedom of speech" even if he has no entitlement to that benefit.'" 539 U.S. 194, 210 (2003) (quoting Bd. of County Comm'rs v. Umbehr, 518 U.S. 668, 674 (1996)); *see, e.g.*, Legal Servs. Corp. v. Velazquez, 531 U.S. 533, 543 (2001); O'Hare Truck Serv., Inc. v. City of Northlake, 518 U.S. 712, 716–18 (1996).

[156] A doctrine that took this phenomenon into account would rethink: (1) the proof requirements for selective prosecution claims, *see* Reno v. Arab Am. Antidiscrimination Comm., 525 U.S. 471 (1999) (holding that an alien cannot bring a claim for selective enforcement in deportation proceedings); United States v. Armstrong, 517 U.S. 456, 463 (1996) (allowing defendants to access government documents to prepare for the defense to the case in chief, but not for the defense of selective prosecution); Wayte v. United States, 470 U.S. 598, 607–8 (1985) (holding that for selective prosecution claim the petitioner bears the burden to show that the government intended to unlawfully discriminate in violation of the Equal Protection Clause); (2) the permission of pretextual searches, *see* Arkansas v. Sullivan, 532 U.S. 769, 772 (2001); Whren v. United States, 517 U.S. 806, 813 (1996) ("[S]ubjective intentions 'of the law enforcement officer' play no role in ordinary, probable-cause Fourth Amendment analysis."); and (3) the doctrine of *Hernandez v. New York*, 500 U.S. 352, 359–60 (1991) (upholding practice of striking Spanish speaking jurors on the theory that hostility towards those who speak Spanish is not animus toward Hispanics).

able to obtain information to target constitutionally protected activities in the exercise of their discretion, it becomes more imperative that discretion should itself be exercised in a setting where the political limits on abuse can be brought to bear. As Judge Keith observed—a generation after rejecting the Nixon Administration's claim to extraconstitutional power—"Democracies die behind closed doors. The First Amendment, through a free press, protects the people's right to know that their government acts fairly, lawfully, and accurately."[157]

B. Designing for Dissent: Structuring Information Systems to Minimize Abuse

Laws do not enforce themselves; still less do they enforce themselves with perfect efficacy. Whatever the level of substantive protection against abuse provided by law "on the books," the removal of prophylactic constraints on information sharing will, *ceteris paribus*, make abuse more likely. The challenge of a well-designed system of information sharing is to adopt procedures that counteract this increase in risk without degrading the nation's capacity to deal with terrorism. What follows is far from an exhaustive analysis. Rather, I explore briefly several mechanisms that make use of informational techniques to counterbalance informational dangers.

1. *Access Controls: Selective Revelation, Rule Processing Technology, DRM, Anonymization*

Traditional security practices in the intelligence community have emphasized a "need to know" principle. Information is disseminated on a selective basis, and often the originator of the information retains control over its use, in order to assure that classified sources of

[157] Detroit Free Press v. Ashcroft, 303 F.3d 681, 683 (6th Cir. 2002). *Contra* N. Jersey Media Group, Inc. v. Ashcroft, 308 F.3d 198, 221 (3d Cir. 2002) (holding that the Attorney General can order blanket closure of immigration hearings to the media and the public). In this regard, the Supreme Court's decision to deny review in *M.K.B. v. Warden*, 124 S. Ct. 1405 (2004), a case which upheld the sealing of a habeas corpus application by an immigrant who was secretly imprisoned as a "material witness" for five months in the roundups following September 11, is particularly disturbing. Mohamed Kamel Bellahouel was imprisoned on the basis of FBI affidavits that he "'likely' served meals to two of the Sept. 11 hijackers, Mohamed Atta and Marwan al Shehhi, while waiting tables at a Middle Eastern restaurant in Delray Beach, Fla." and reportedly "was seen entering a movie theater with a third Sept. 11 hijacker, Ahmed Alnami." James McLaughlin, *Blackout of Justice*, 28 NEWS MEDIA & LAW 7 (Winter 2004), http://www.rcfp.org/news/mag/28-1/cov-blackout.html. All proceedings in Bellahouel's application for a writ of habeas corpus were sealed, notwithstanding the fact that he was later released. *Id.* The Court allowed all briefs to be filed under seal, so it is difficult to determine the basis, if any, for the determination.

information are not disclosed.[158] The risk of abuse is minimized by limiting access to sensitive information. In structure, the problem of privacy and misuse of databases to suppress dissent is cognate: the challenge is to prevent misuse of data, and the more selectively data is disseminated, the less likely it will be to be misused. Conceptually, there is no reason that the mechanisms that have been developed to limit dissemination of classified data cannot equally be deployed to limit misuse of intimate or politically sensitive information.[159]

Existing approaches to multilevel relations in the context of multilevel secure databases allow only users with appropriate security clearances access to classified data. Technologists are currently exploring sophisticated databases which provide fine grained selective access to the materials contained in data networks, based on their privacy and sensitivity; these mechanisms can ensure that particular searchers are entitled to view only particular bits of data.[160] Thus, a domestic security database could be constructed that allows general access, for example, to a subject's address, but access to her gun ownership records only to one group of analysts, and access to her attendance at political rallies only to another select group. Other technologies could prevent analysts from exporting data from their computers to any other computer not similarly authorized, allowing privacy classifications to "stick to" the data as it is shared.[161]

---

[158] For example, the Office of the Inspector General described the current classification system:

> According to one FBI Section Chief, the FBI does not originate 90 percent of the intelligence it uses. The agency that originally collected the intelligence may mark it ORCON, or originator controlled. All agencies that receive this information must receive permission from the originating agency before further dissemination. Agencies usually mark a document ORCON for two reasons. First, it allows the originating agency to protect the sources and methods disclosed in the classified document. Second, it is a vehicle to allow the originating agency to control how the information or conclusions in a document are used.

OIG, FBI'S EFFORTS, *supra* note 9, at 15; *see also* OFFICE OF INSPECTOR GEN., DEP'T OF JUSTICE, A REVIEW OF THE FBI'S PERFORMANCE IN DETERRING, DETECTING, AND INVESTIGATING THE ESPIONAGE ACTIVITIES OF ROBERT PHILIP HANSSEN 23 (2003) [hereinafter OIG, HANSSEN] (criticizing the FBI for failure to enforce "need to know" requirements, thereby facilitating espionage by a member of the FBI), *available at* http://www.usdoj.gov/oig/special/0308/final.pdf.

[159] *See, e.g.*, Chris Strohm, *Homeland Security Privacy Officer Pushes Training Efforts*, GOVEXEC.COM, Nov. 17, 2003 ("[T]he Customs and Border Protection Agency . . . . uses technology that limits the number of employees who can access sensitive information, as well as the time that information can be viewed."), *at* http://www.govexec.com/dailyfed/1103/111703c1.htm.

[160] *E.g.*, RAKESH AGRAWAL ET AL., HIPPOCRATIC DATABASES 2 (2002) (noting that ongoing work of particular interest concerns access control policies), *available at* http://www.almaden.ibm.com/cs/people/srikant/papers/vldb02.pdf.

[161] *E.g.*, MARCO CASASSA MONT ET AL., TOWARDS ACCOUNTABLE MANAGEMENT OF IDENTITY AND PRIVACY: STICKY POLICIES AND ENFORCEABLE TRACING SERVICES 4–6 (2003) (proposing a model that employs sticky privacy policies to increase data receivers accountability in e-

Researchers have begun, as well, to generate methods of searching distributed databases that technologically embed limits on access to particular types of data in the search process itself,[162] and methods that allow data mining for trends across a variety of databases, while masking the particular attributes of individual members of the population searched, and preventing the holders of data from determining the nature and purpose of the search.[163] A variety of commentators have suggested that national security data mining make use of these technologies to limit examination information about innocent individuals.[164] Indeed, the ill-fated TIA program itself contemplated developing a "privacy appliance" to assure that searches did not extend beyond proper limits.[165]

The difficulty with this approach is twofold. First many of the agencies which gather and share information under the post-September 11 security regime are far from the cutting edge of tech-

commerce transactions), *available at* http://www.hpl.hp.com/techreports/2003/HPL-2003-49.html; IBM, Enterprise Privacy Technologies (describing systems utilizing "'sticky policy paradigm' mandates that policy sticks to the data, travels with it, and can be used to decide how the data can be used."), *at* http://www.zurich.ibm.com/security/enterprise-privacy/ (last visited Sept. 30, 2004); *cf.* Julie E. Cohen, *DRM and Privacy*, 18 BERKELEY TECH. L.J. 575, 575 (2003) (giving an account of mechanisms of "digital rights management" that also reveal the activities of users of information).

[162] *E.g.*, MAYANK BAWA ET AL., PRIVACY PRESERVING INDEXING OF DOCUMENTS ON THE NETWORK 11 (2003) (describing research on the problem of "private information retrieval" where "[a] user wishes to privately retrieve the *i*-th bit from a database, without revealing any information about *i*"), *available at* http://www.almaden.ibm.com/software/quest/Publications/papers/vldb03_ppi.pdf.

[163] *E.g.*, Alexandre Evfimievski et al., *Limiting Privacy Breaches in Privacy Preserving Data Mining*, (2003), *available at* http://www.cs.cornell.edu/aevf/research/PODS_2003.pdf; Latanya Sweeney, *Achieving* k-*Anonymity Privacy Protection Using Generalization and Suppression*, 10 INT'L J. ON UNCERTAINTY, FUZZINESS, & KNOWLEDGE-BASED SYSTEMS 571 (2002), *available at* http://privacy.cs.cmu.edu/people/sweeney/kanonymity2.pdf. For a bibliography, see *Privacy-Preserving Data Mining*, *at* http://www.tcs.hut.fi/~helger/crypto/link/data_mining (last visited Sept. 30, 2004).

[164] *E.g.*, JAMES X. DEMPSEY & PAUL ROSENZWEIG, CTR. FOR DEMOCRACY & TECH., TECHNOLOGIES THAT CAN PROTECT PRIVACY AS INFORMATION IS SHARED TO COMBAT TERRORISM 15 (2004) (noting that techniques to anonymize data are still in their infancy), *available at* http://www.cdt.org/security/usapatriot/20040526technologies.pdf; MARKLE REPORT, *supra* note 4, at 34 (calling for the use of anonymizing techniques for searching to minimize the privacy impact); TAPAC REPORT, *supra* note 5, at ix, x, 50–51 (recommending data anonymization); Taipale, *supra* note 122, at 74 (arguing that "*rule-based processing* and a *distributed database architecture* can significantly ameliorate the general data aggregation problem by limiting the scope of inquiry and the subsequent processing and use of data within policy guidelines" and that "*selective revelation* can reduce the non-particularized suspicion problem, by requiring an articulated particularized suspicion and intervention of a judicial procedure before identity is revealed").

[165] *E.g.*, Matthew Fordahl, *Device Will Watch Over the Watchers*, DESERET MORNING NEWS (Salt Lake City, Utah), July 21, 2003, at C2; Leslie Walker, *Balancing Data Needs and Privacy*, WASH. POST, May 8, 2003, at E1 (describing research conducted by Teresa Lunt at the Palo Alto Research Center who received a grant to develop a "privacy appliance" for TIA).

nology. The theoretical availability of a "privacy appliance," "sticky" privacy policies, or privacy preserving data mining is likely to be irrelevant to police forces that operate with card files, or an FBI structure that is struggling to bring its computer system up to minimum levels of effectiveness. Equally important, once a piece of information leaves the digital environment, its technological classification vanishes. An official who seeks to avoid technological access controls need only transcribe and convey the material by more traditional means.[166]

Second, privacy classifications exist at the discretion of the classifiers and a "privacy appliance" can be turned off or turned down as easily as it can be turned on. If the programmers of the "appliance" quarantine data about attendance at political rallies, but not religious services, only political privacy is protected. Even if administrators act in the best of faith, simply identifying the scope of data that may be used to track dissenters is no easy task. Conversely, it is difficult *ex ante* to know what information might prove useful in seeking to uncover potential perpetrators of terrorist outrages. Queries might plausibly seek to identify suspects who shared an apartment with a known terrorist. But they might equally inquire into whether the suspect shared a mosque, a friend, or a tendency to visit certain websites or bulletin boards, where coded messages might have been left.[167] Given the history of domestic surveillance it is more than possible to imagine administrators who make efforts to tweak the "privacy appliance" in a fashion that minimizes interference with their opportunity to suppress "subversion."

Like traditional "need to know" security, the privacy protection mechanisms are at odds with the premise of post-September 11 information sharing. The common wisdom—warranted or not—is that it is precisely the limits on sharing of information which stands in the way of effective antiterrorist intelligence, and policies which stand directly in the way of sharing are unlikely to prove durable. To take

[166] For example:

> The practice of collecting vast amounts of information on American citizens was terminated in 1971, when new Department of Defense restrictions came into effect calling for the destruction of all files on 'unaffiliated' persons, and organizations. Rather than destroying the files, however, several Army intelligence units simply turned their intelligence files and dissident individuals and groups over to local police authorities; and one Air Force counterintelligence unit in San Diego began to create new files the next year.

Hearings Before Subcomm. on Constitutional Rights, S. Comm. on the Judiciary, 92nd Cong. 1297 (1971).

[167] *Cf.* Thomas C. Greene, *Al-Qaeda Said to Be Using Stegged Porn*, REGISTER, May 12, 2003 (reporting and purporting to debunk claim that al Qaeda members left secret messages embedded in pornographic photographs on Internet bulletin boards), *at* http://www.theregister.co.uk/2003/05/12/alqaeda_said_to_be_using. More reputable analysts seem to believe that al Qaeda uses coded messages in mundane e-mail and instant message format.

one example, even as the FBI was recovering from the damage wrought by turncoat Robert Hansen, who had gathered and stolen enormous amounts of data by utilizing queries in the FBI's "Automated Case Support" system, FBI headquarters removed access controls to that system as a means of facilitating "sharing" of data for the war on terrorism.[168] It seems unlikely that decision makers would prove more solicitous in their protection of personal information of dissenters.

2. *Audit Trails*

If implementation of technological limits on access to personally identifiable data is likely to run aground on the "need to share" intelligence, another measure which does not interfere prospectively with sharing may prove more feasible. In any sort of environment where abuse is a possibility, the abuse becomes less likely when it is more subject to discovery. Thus, it was common before September 11 for information systems to mandate non-falsifiable or tamper resistant audit trails that would, on inspection, reveal the use to which information was put.[169] With the emergence of the "need to share," these safeguards become still more salient. A series of analyses addressing the emerging issues of data mining and aggregation in the current intelligence climate have similarly called for the adoption of strong audit trails for analyses and dissemination of personally identifiable data.[170]

---

[168] *See* COMM'N FOR REVIEW OF FBI SEC. PROGRAMS, DEP'T OF JUSTICE, A REVIEW OF FBI SECURITY PROGRAMS 46–48 (2002) (describing the abandonment of "need to know" access which facilitates the repeat of the Hanssen debacle), *available at* http://www.usdoj.gov/05publications/websterreport.pdf. The FBI will presumably respond to this concern in future efforts.

[169] *E.g.*, *id.* at 38–41 (describing discovery of misuse of FBI Automated Case Support system by Robert Hanssen through review of audit logs); 28 C.F.R. § 23.20(g) (mandating that "a project maintaining criminal intelligence information shall ensure that administrative, technical, and physical safeguards (including audit trails) are adopted to insure against unauthorized access and against intentional or unintentional damage. A record indicating who has been given information, the reason for release of the information, and the date of each dissemination outside the project shall be kept"); *id.* § 23.20(g)(3) ("The project must store information in the system in a manner such that it cannot be modified, destroyed, accessed, or purged without authorization."); *cf.* MATRIX, PRIVACY POLICY § 8 (2003) (purporting to require log of access and dissemination of information), *available at* http://www.matrix-at.org/privacy_policy.pdf.

[170] *E.g.*, MARKLE REPORT, *supra* note 4, at 15; TAPAC REPORT, *supra* note 5, at ix–x; Arthur J. Cockfield, *Who Watches the Watchers? A Law and Technology Perspective on Government and Private Sector Surveillance*, 29 QUEEN'S L.J. 364, 378 (2003); Dempsey & Rosenzweig, *supra* note 164, at 13; Taipale, *supra* note 122, at 75 (calling for mitigation of abuse by use of "strong credential and audit features and diversifying authorization and oversight"); A. Michael Froomkin, The Uneasy Case for National ID Cards 46–48 (Mar. 2004) (draft), http://personal.law.miami.edu/~froomkin/articles/ID1.pdf.

Audit trails of both queries and dissemination of data do not interfere with data sharing, but can mitigate its dangers. At a minimum, audit trails allow the organizational hierarchy to know what use is being made of sensitive data and data mining capabilities. Effective and available query logging and audit trails limit the possibility that rogue members of the intelligence community will embark on freelance surveillance of dissidents or invasions of privacy.[171] They allow organizations to track whether their own rules are being flouted, a capability as important for maintaining security as for maintaining privacy.[172] Privacy officers can use audit trails as a basis for increased training where appropriate. Audit trails available to internal inspectors general and potentially to criminal prosecutors or injured citizens provide some deterrence of blatantly illegal inquiries. Should illegal releases of data occur, audit trails provide the capacity to track the release back to the source.

Audit trails (especially combined with "sticky" data tags which lay down trails as the data is disseminated) can allow corrected data to follow inquiries through the system when data or analyses prove to be inaccurate.[173] At a more advanced level, at least one proposed system would, as a part of intelligence analysis, monitor the inquiries of analysts in real time.[174] Such a system could monitor the accuracy of the results of queries and could also be keyed to alert supervisors to politically based or otherwise improper data analysis.[175]

To be sure, like access control technologies, audit trails are technology dependent. They will be less useful in less technologically sophisticated environments and can be evaded to some extent by mov-

[171] In the 1970s, it appeared that parts of the military hierarchy were as surprised as civilians at the breadth and depth of domestic surveillance undertaken at the ground level. *See* PYLE, *supra* note 21. In recent months, it has appeared that our Homeland Security bureaucracy may be equally ill informed. *See* Ryan Singel, *Senators Question TSA Denials*, WIRED NEWS, Apr. 15, 2004 (detailing eight months of denials by TSA officials, Admiral Loy, and Privacy Officer O'Connor Kelly that CAPPS II had been tested on actual passenger data, when in fact three airlines had provided millions of passenger records that had been subject to testing), *at* http://www.wired.com/news/privacy/0,1848,63067,00.html.

[172] OIG, HANSSEN, *supra* note 158, at 23 (advocating tracking of high security documents and real time auditing of inquiries). The FBI does occasionally catch and punish illegal access to its system by reviewing its logs. *See* Bill Braithwaite & Steven S. Lazarus, Markle Found. Connecting for Health Initiative—Advanced HIPPA Privacy & Security Case Studies (June 6, 2003) (setting forth case studies of privacy auditing in HMOs), http://cpanel.cygnusnet.com/~ehcca/presentations/HIPAAWest3/braithwaite_lazarus.pdf; Press Release, Dep't of Justice, FBI Legal Technician Pleads Guilty to Unlawfully Accessing the FBI's Computer System (Feb. 26, 2004) (available at http://www.usdoj.gov/opa/pr/2004/February/04_crm_120.htm).

[173] MARKLE REPORT, *supra* note 4, at 36.

[174] ARDA, *supra* note 16 (describing system that "attempt[s] to induce as much of this information as possible from what the analyst does during the analytic process").

[175] *Cf.* RAKESH AGRAWAL ET AL., AUDITING COMPLIANCE WITH A HIPPOCRATIC DATABASE 7 (2004) (discussing the development of a query intrusion detector), *available at* http://www.almaden.ibm.com/software/quest/Publications/papers/vldb04_audit.pdf.

ing outside of digital dissemination. But the most threatening data mining is itself effective only in the use of advanced computer technology, and even partial trails are useful as clues to track disclosures that end outside of the digital environment.

Unlike privacy enhancing or access limiting technologies, audit trails are likely to be well integrated with the security demands of most large scale data systems. The precise nature of the sensitive data, moreover, need not be identified *ex ante*. Investigators seeking to uncover abuses can themselves mine audit logs for patterns of potential harassment identified after the fact.

3. *Watching the Watchers*

Audit trails, however, can serve deterrent or restorative functions only if they are utilized; an unexamined log is hardly worth having. The institutional environment in which the records of surveillance are reviewed is crucial in any effort to construct a system that is consistent with civil liberty.

One audience for information regarding the use of surveillance is internal. Most intelligence agencies have their own inspectors general, or intelligence oversight officers and the Department of Homeland Security was equipped with both a Privacy Officer and a Civil Rights and Civil Liberties Officer. To the extent that these internal agents have the inclination and capacity, the prospect of their examination will have a salutary impact on the way in which sensitive data is analyzed and disseminated. There is reason to wonder, however, whether such officers are likely to be sufficiently funded or motivated in most cases.

More active analysis of the way in which internal surveillance is undertaken is likely to come from external watchdogs. Congress, through intelligence oversight committees, GAO investigations, and demands of individual members has had some impact on the "war on terror" thus far. Much of the information on internal security exercises since September 11 has come in response to such congressional inquiries, and it is important that audit logs be available for inspection by the legislative branch.

Still more public oversight of domestic surveillance since September 11 has been generated by advocates external to government invoking the Freedom of Information Act ("FOIA"),[176] and potentially

[176] *See, e.g.*, Press Release, Electronic Privacy Information Center, Lawsuit Seeks Information on Law Enforcement Agency Purchases of "Profiling" Data (Jan. 15, 2002) ("EPIC charged that the Departments of Justice and Treasury have violated the law by failing to respond to a series of Freedom of Information Act (FOIA) requests . . . ."), http://www.epic.org/privacy/litigation/profilingpr.html; ACLU, Patriot FOIA ("[T]he ACLU and other public interest organizations have filed two requests under the Freedom of Information Act (FOIA) seeking records relating

by discovery in other litigation.[177] In the normal course of events, the executive branch can be expected to oppose outside efforts to discover information regarding surveillance; indeed the current administration has adamantly resisted FOIA requests and has sought to block any public inquiry into its initiatives.[178] This approach is shortsighted.

If the goal is simply to maximize surveillance in the short run, of course, disclosure may be viewed as counterproductive, for it allows political opponents of surveillance to gain traction. Yet, ultimately in the 1970s it was the surreptitious quality of the surveillance that led to its delegitimation; programs that are openly avowed are likely to garner more long run support. A showing of the discretion with which they are used and the accuracy of their results is likely to allay, rather than exacerbate concerns.

The more persuasive response to the demand for disclosure is likely to rest on the claim that surveillance disclosed is surveillance evaded. Counterterrorism is, after all, a dynamic enterprise. Once terrorists understand that a particular mode of communication or activity evokes surveillance, they are likely to abandon it. But here,

---

to the Justice Department's implementation and use of the USA PATRIOT ACT."), *at* http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=15327&c=262 (last visited Sept. 30, 2004); ACLU, ACLU Seeks Government Accountability For No-Fly List ("[T]he government has refused to confirm the existence of any protocols, procedures or guidelines as to how the 'no fly' lists were created or to detail how they are being maintained or corrected . . . ."), *at* http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=15422&c=206 (last visited Sept. 30, 2004); Press Release, ACLU, What Is The Matrix? ACLU Seeks Answers on New State-Run Surveillance Program (Oct. 30, 2003) ("The goal of the requests is to find out what information sources the system is drawing on—information program officials have refused to disclose—as well as who has access to the database and how it is being used."), http://www.aclu.org/Privacy/Privacy.cfm?ID=14257&c=130; Press Release, ACLU, Declassified FBI Documents Suggest Shoddy Management of "No Fly" List, Fail to Show How Innocent Americans Can Get Names Cleared (Dec. 4, 2003) (describing the "FBI's first-ever release of classified documents about the controversial 'no fly' terrorist watchlist"), http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=14520&c=272; Electronic Privacy Information Center, Litigation Docket: Court Cases: FOIA Litigation (describing the cases the EPIC is currently litigating), *at* http://www.epic.org/privacy/litigation/ (last visited Sept. 30, 2004).

[177] *E.g.*, Doe v. Ashcroft (S.D.N.Y.) (No. 04-2614) (challenging National Security Letter to an ISP), *at* http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=15543&c=262 (last visited Sept. 30, 2004); Green v. Transp. Sec. Admin. (challenging No Fly List), *at* http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=15543&c=272 (last visited Sept. 30, 2004); Muslim Cmty. Ass'n of Ann Arbor v. Ashcroft (E.D. Mich.) (No. 03-72913) (challenging Section 215 of the USA PATRIOT Act), *at* http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=13255&c=207 (last visited Sept. 30, 2004).

[178] *E.g.*, Ctr. for Nat'l Sec. Studies v. Dept. of Justice, 331 F.3d 918 (D.C. Cir. 2003) (rejecting FOIA request seeking information regarding detentions in the aftermath of September 11, the names of detainees, and their attorneys under the FOIA); ACLU v. Dept. of Justice, 2004 U.S. Dist. LEXIS 9381 (D.D.C. 2004) (rejecting FOIA request seeking information regarding the use of Section 215 of the USA PATRIOT Act); ACLU v. Dept. of Justice, 265 F. Supp. 2d 20 (D.D.C. 2003) (rejecting FOIA request seeking information regarding the use of surveillance and investigatory powers).

there must be some effort to evaluate the actual magnitude of the effect. The disclosure of the number of "library" searches, for example, if that number is in fact limited, may assuage the concern of readers without substantially increasing the tactical advantage of terrorists. It is here that the possibility of "anonymized" data analysis may come into its own. To the extent that logs of internal searches can be "anonymized," they may be disclosed to at least limited public analysis to examine patterns without substantial fear.

4. *Into the Sunset*

Of course, the prospect of exposure even to the executive branch watchdogs or to intelligence oversight committees will have some effect on security officials. The salutary quality of this effect is likely to be strengthened if—as should be the case—extraordinary surveillance powers are limited in duration.

More information means more efficient control; yet most of our social institutions are built on assumption of friction. Moving to frictionless environment destabilizes the checks and balances. If a security bureaucrat faces no cost to exploring a citizen's life, while the failure to explore that life carries a risk of catastrophe, however marginal, it would be irrational not to investigate, notwithstanding the fact that each investigation imposes a risk on the person investigated.

One way of addressing this profligacy could be to provide the bureaucrat with a shadow "budget" which would be charged each time she accessed the details of a citizen's life.[179] Notwithstanding the availability of technology that could accomplish the task of taxing inquiries, this approach is unlikely to find favor in today's environment, both because the challenge of setting the appropriate level of payment would be controversial and because the actual technology deployed by security bureaucrats is likely to be primitive. There is, however, another approach which can capture some of the virtues of micropayments. If authority to gather or analyze data must be reauthorized at regular intervals, a sunsetted authority combined with the prospect of disclosure to an authorizing agency that is sensitive to the

[179] In a still more utopian version, one could imagine allowing citizens to set the level of payment which they were willing to accept for a "peek." *Compare* Yannis Bakos & Erik Brynjolfsson, *Aggregation and Disaggregation of Information Goods: Implications for Bundling, Site Licensing and Micropayment Systems*, *in* INTERNET PUBLISHING AND BEYOND: THE ECONOMICS OF DIGITAL INFORMATION AND INTELLECTUAL PROPERTY 117–20 (Brian Kahin & Hal R. Varian eds., 2000), *and A Micropayment for Your Thoughts*, WIRED NEWS, Dec. 1, 2003, *at* http://www.wired.com/news/ebiz/0,1272,61419,00.html, *with* RONALD J. MANN & JANE K. WINN, ELECTRONIC COMMERCE 460–61 (2002) (discussing micropayments and noting that micropayment systems have been developed).

costs of infringements of civil liberty establishes a "shadow price" for overusing the authority in question.

This suggestion is not merely hypothetical. As part of its efforts to make public the scope of potential surveillance, the ACLU obtained a copy of the FBI guidance for use of the "national security letter" authority granted by the USA PATRIOT Act. The guidance admonishes its recipients: "In deciding whether or not to re-authorize the broadened authority, Congress will certainly examine the manner in which the FBI has exercised it. . . . Supervisors should keep this in mind when deciding whether or not a particular use of the NSL authority is appropriate."[180]

CONCLUSION

In today's environment, *ex ante* judicial control of surveillance is unlikely. One response lies in strengthening legal doctrines that exert *ex post* control against abuse of information obtained by surveillance. The effect of such doctrines, even if courts adopt them, however, will be sporadic. The most effective constraints lie at the intersection of technology, politics, and norms. It is precisely those constraints that underpinned the settlement of the 1970s, and the challenge for administrators of good will is to find a set of structures and commitments that will achieve a new settlement that preserves American liberty.

The task is well described by the office the Army charged with intelligence oversight, in its—perhaps prematurely optimistic—response to the claim that the abuses of the Nixon era are mere "ancient history":

> When dealing with . . . constitutional rights, there is no such thing as "ancient history." For example, terrorism is on everyone's minds these days. At one point recently, a senior federal official said publicly that terrorism is so serious that U.S. citizens may well need to give up some of their rights so they could be properly protected. This is very much like the thinking that led to the 1960s and 1970s abuses. Had the intelligence oversight mechanism not been in place, we very well could have seen the same abuses all over again.[181]

[180] Memorandum from Gen. Counsel, Nat'l Sec. Law Unit, FBI, National Security Letter Matters 3 (Nov. 28, 2001), http://www.aclu.org/patriot_foia/FOIA/Nov2001FBImemo.pdf.

[181] History, Intelligence Oversight, *supra* note 38.