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

Seth F. Kremer*

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.

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 systemic flaw that exposed the United States to terrorist attacks. The Attorney General regularly inveighs against the "impediments to communication and information sharing among the men and women charged with keeping America safe." The non-partisan Markle Foundation Task Force has advocated improved sharing of information as the precondition to more effective homeland security, a rec-

---

*Kenneth W. Gerson, 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 perspective analysis of M.E. Roseman, Luke Fleet, Jonathan Freeland, Mitch Marcus, Kim Scheppele, and Paul Waggoner, and the superb research assistance of Miko Kohlinger. They gave my deep thanks, while I retain all responsibility for errors or omissions that remain.


ommodation joined by the Defense Department’s Technology and Privacy Advisory Committee. The General Accounting Office similarly reports that “homeland security” requires increased interpretation of intelligence.

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


The National Criminal Intelligence Sharing Plan contains recommendations to incorporate privacy guidelines developed by the National Criminal Justice Association. SHARING PLAN at 21. See NAT’L CRIMINAL JUSTICE ASSOC., JUSTICE INFORMATION PRIVACY GUIDELINES (2002), http://www.nca.org/pdf/privaftyguide.pdf (last visited Sept. 30, 2006). The Sharing Plan also recommends compliance with the privacy protection mandates of 28 C.F.R. §§ 23 (2003). One difficulty here is § 24.1 makes reference to a “reasonable suspicion” requirement, § 23.25(a), a direct relationship requirement for First Amendment-related records. § 23.30(b), and “need to know” limitations, § 23.30(c). (c) “The ‘protections’ of civil liberties in which the Attorney General lists as part of the Sharing Plan that appear to include among the ‘roadblocks’ he purported to seek to remove. On the other hand, the Sharing Plan suggests that section 25 “in currently pending revision” in light of “the speed of which technology changes, the issue 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," 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. 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")."

On the military side, even after the demise of the Defense Advanced Research Projects Agency's ("DARPA") controversial "Total Information Awareness" ("TIA") program, the Commander of...
Northcom, General Ralph Eberhard, has asserted that "we need to change from the 'need to know' Cold War mentality to the 'need to share,'... in this global war on terrorism." 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." Indeed, "Knowledge is power" as an oxymoron, attracted a tremor of concern from advocates of the system, e.g., Letter from Thirty-One Citizens to Senator Sessions and Sen. Lieberman (May 18, 2001), and technical experts who questioned the feasibility of the system, e.g., Letter from U.S. Association for Computing Machinery to Senators Warren and Levin (Jan. 23, 2000) (arguing criteria regarding Total Information Awareness System), http://www.auz.org/uncle/Lettets/06_final.html. Congress reacted by first demanding a report from the office about the projected impact on civil liberties, or DARPA, REPORT TO CONGRESS REGARDING TOTAL INFORMATION AWARENESS PROGRAM IN RESPONSE TO COMMISSIONED APPROPRIATIONS RECOMMENDATION RESOLUTION OF 2000, PUB. L. NO. 106-7, 117 STAT. 11, § 1140 (2000); and then it apparently is halting funding for the project. See Conf. Rep. on H.R. 3508, Department Of Defense Appropriations Act of 2004, H.R. Rep. No. 108-285, 108th Cong., at § 1141(a) (2003) ("Notwithstanding any other provision of law, none of the funds appropriated otherwise made available in this or any other Act may be obligated for the 'Total 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 TIPAC Report: TIPAC: REPORT TO THE ADVISORY COMMITTEE OF THE INTELLIGENCE COMMUNITY, at 5, (2003) (2003), is not likely to alter new research in data mining software, and the issue will not disappear. Even if not as dramatically as with TSA, since the Pentagon is certainly more sensitive to public perception of its activities, Id. at 5.

D. Doing Simple, Deploying the Harmonized Intelligence Road Map, and TOYeC INTO SERVICE, Feb. 26, 2004, at http://www.defenselink.mil/factfiles/c2qt20040226/20040226COM.htm. This echoes the Northern Command's Chief Information Officer, who earlier announced that "there are steps we can take to change from a 'need to know' to a 'need to share' foundation." Molly Peterson, Housed Intelligence Command Serves 'Need to Share' Information, Dec. 3, 2002, at http://www.govexec.com/dailyfed/2002/12/30021203.html. See also William H. Arkin, U.S. Military, Monitor Unit Monitors: New, L.A. Times, Nov. 23, 2001, at MG (quoting General Eberhard as stating that "we are not going to be out there spying on people ... We get information from people who do," and describing the "CovertInformation-Related Activity," which has been given the acronym of data mining: public records, credit card accounts and intercepted communications); Robert Gans, NSA's Wolf Turns Tawny and 'Need to Share,' EFFECTIVE GOV'T IN ACTION, Oct. 1, 2003, at http://www.galsitecollection.com/elecletters/electricnews/oct/00/0010E1010MA.htm. William New, Government High Military May in "Finance" Data, Jan. 5, 2004 ("[H]earty attacks on the Sep. 11, 2001, terrorist attacks, the 'need to know' approach to information has become a 'need to share' philosophy."); at http://www.govexec.com/dailyfed/2003/10/10031005.htm.


"Knowledge is power" as an oxymoron, attracted a tremor of concern from advocates of the system, e.g., Letter from Thirty-One Citizens to Senator Sessions and Sen. Lieberman (May 18, 2001), and technical experts who questioned the feasibility of the system, e.g., Letter from U.S. Association for Computing Machinery to Senators Warren and Levin (Jan. 23, 2000) (arguing criteria regarding Total Information Awareness System), http://www.auz.org/uncle/Lettets/06_final.html. Congress reacted by first demanding a report from the office about the projected impact on civil liberties, or DARPA, REPORT TO CONGRESS REGARDING TOTAL INFORMATION AWARENESS PROGRAM IN RESPONSE TO COMMISSIONED APPROPRIATIONS RECOMMENDATION RESOLUTION OF 2000, PUB. L. NO. 106-7, 117 STAT. 11, § 1140 (2000); and then it apparently is halting funding for the project. See Conf. Rep. on H.R. 3508, Department Of Defense Appropriations Act of 2004, H.R. Rep. No. 108-285, 108th Cong., at § 1141(a) (2003) ("Notwithstanding any other provision of law, none of the funds appropriated otherwise made available in this or any other Act may be obligated for the 'Total 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 TIPAC Report: TIPAC: REPORT TO THE ADVISORY COMMITTEE OF THE INTELLIGENCE COMMUNITY, at 5, (2003) (2003), is not likely to alter new research in data mining software, and the issue will not disappear. Even if not as dramatically as with TSA, since the Pentagon is certainly more sensitive to public perception of its activities, Id. at 5.

D. Doing Simple, Deploying the Harmonized Intelligence Road Map, and TOYeC INTO SERVICE, Feb. 26, 2004, at http://www.defenselink.mil/factfiles/c2qt20040226/20040226COM.htm. This echoes the Northern Command's Chief Information Officer, who earlier announced that "there are steps we can take to change from a 'need to know' to a 'need to share' foundation." Molly Peterson, Housed Intelligence Command Serves 'Need to Share' Information, Dec. 3, 2002, at http://www.govexec.com/dailyfed/2002/12/30021203.html. See also William H. Arkin, U.S. Military, Monitor Unit Monitors: New, L.A. Times, Nov. 23, 2001, at MG (quoting General Eberhard as stating that "we are not going to be out there spying on people ... We get information from people who do," and describing the "CovertInformation-Related Activity," which has been given the acronym of data mining: public records, credit card accounts and intercepted communications); Robert Gans, NSA's Wolf Turns Tawny and 'Need to Share,' EFFECTIVE GOV'T IN ACTION, Oct. 1, 2003, at http://www.galsitecollection.com/elecletters/electricnews/oct/00/0010E1010MA.htm. William New, Government High Military May in "Finance" Data, Jan. 5, 2004 ("[H]earty attacks on the Sep. 11, 2001, terrorist attacks, the 'need to know' approach to information has become a 'need to share' philosophy."); at http://www.govexec.com/dailyfed/2003/10/10031005.htm.

parts of the former Total/Terrorism Information Awareness package appear to be funded to go forward under other "off the books" appropriations.\(^8\)

The Intelligence Community is pursuing an initiative on "Novel Intelligence from Massive Data" through its "Advanced Research and Development Activity," and the Director of the CIA has been mandated to "assess the feasibility and advisability of permitting intelligence analysis of various elements of the intelligence community to access and analyze intelligence from the databases of other elements." 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,\(^9\) while instigation and air safety initiatives already are seeking to link a variety of publicly and privately held databases to screen air passengers and immigrants.\(^10\) As the Technology and Privacy Advisory Committee re-

---


\(^8\) In U.S. Govt. Accounting Office, Rep. No. GAO-04-365, AVIATION SECURITY: COMPUTER ASSISTED PASSENGER SCREENING SYSTEM (CAPPS) FACES SIGNIFICANT IMPLEMENTATION CHALLENGES (2004) (delineating efforts to exempt CAPPS II from Privacy Act protections of relev-

ance and accessibility and failure to establish either accuracy or privacy of screening tech-


\(^{11}\) Associated Press, CIA Still Mining Terror Data, Wired News, Feb. 21, 2004 ("Congressional officials declined to say which "profiler" programs were killed and which were transferred, but people with direct knowledge acknowledge that the surviving programs included some of 18 dismantled projects known as Evidence Extraction and Link Discovery in Profiler's re-


\(^{13}\) For example, see the report of the Privacy and Civil Liberties Oversight Board, Privacy and Civil Liberties Oversight Board, Final Report and Recommendations: Role of the National Intelligence Director in the National Security Executive Branch (July 2006), available at http://www.oip.dhs.gov/doc立场/displaycontent.jsp?content=6183.
cently observed, "TIA was not the tip of the iceberg, but rather one small specimen in a sea of icebergs."

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.66 While the Fugitive Commissary Act of 1878 barred the Army from domestic law enforcement and the Anti-Pinkerton Act of 1885 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.67 The Justice Department established its own Bureau of Investigation to undertake domestic surveillance.68 Though the domestic military intelligence apparatus was pruned in


67 See, e.g., Totten v. United States, 92 U.S. 105, 106 (1875) (noting that the President was "irrevocably authorized during the war, as commander-in-chief of the armed forces of the United States, to employ secret agents to enter the rebel lines and secure information respecting the strength, resources, and movements of the enemy."); see also Valverde v. United States, 68 U.S. 249 (1866) (removing arrest and conviction of critic of Civil War prosecution by military tribunal); JOHN M. JENSEN, ARMED SURVEILLANCE IN AMERICA, 1775-1988, at 39-40 (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).


70 See FRANK J. DONNER, THE AGE OF SURVEILLANCE 33 (1989) ("The [Justice Department’s] Bureau of Investigation worked closely during the World War II years with private paramilitary groups, principally the America’s Protective League (APL), officially designated ... for fingerprinting, destroying, and subduing."); JENSEN, supra note 21, at 181-82, 147-49 ("The APL, developed a quasi-military organization to operate secrets within industries.").

71 JENSEN, supra note 21, at 125, 160-65; Major Paul M. Peterson, Civilian Demonstrations Now on Military Farmland: Devils on Military Farmland and Other Intelligence Activity, 140 MIL. L. REV. 113, 116 (1998) ("World War I, however, brought on the first extensive domestic intelligence operations.").
the aftermath of scandals in the 1990s, both military and civilian authorities maintained at least "passive" surveillance of radicals thereafter. 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. 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. 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.

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. Between 1967 and 1968, the National Guard was mobilized eighty-three times and the Army was called out four times to suppress domestic riot. The Army was mobilized in 1969 and 1970 to control protesters...
converging on Washington to protest the Vietnam War.28 Fractions 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 1970.29 The rate doubled again early in 1971.30

In response, the military sought to establish a domestic surveillance mechanism to provide warning and operational intelligence in the event of internal disturbances.31 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.32 As the Defense Department recounts the story,

[...] what 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 monstrously intrusive effort. This resulted in the monitoring of activities of innocent persons included 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."33

National Guard and Army troops had to be used 25 times to quell the civil disturbances.

28 See P C L L, supra note 21, at 54-55 (estimating a total of 500,000 soldiers deployed to preserve domestic order between January 4th and December 1969).

29 See P C L L, supra note 11, at 252-53 (describing deployment of twenty thousand federal troops in November 1969); J o m E i l l e, T h e W a r W i t h i n, A m e r i c a n B a t t l e o v e r V i e t n a m 512 (1994) ("May Day" had given an immense mobilization of armed night and twelve thousand armed letters to keep Washington "open").


31 407 U.S. at 312 n.12 ("The Government asserts that there were 1,561 bombing incidents in the United States from January 1, 1971, to July 1, 1971, most of which involved Government related facilities.")


ATIAM C. TIDICKEN, ON AMERICAN POLITICAL SURVEILLANCE FROM FOWLER TO THE BUSH PLAN 121-22 (1978) (describing illegal monitoring of radio signals).

WATCHING THE WATCHERS

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, wiretaps, and covert efforts to discredit groups viewed as potential sources of disruption. 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," claiming as well the right to engage in extracurricular investigations and seizures.

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

"Question: Why do we have intelligence oversight?
Answer: Because Mil needs a static back."
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. 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." 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." 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. The majority opinion acknowledged that the plaintiffs faced "some difficulty in establishing visible injury, at least on this incomplete record." 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," in the light of the "long-established tradition against military involvement in civilian politics," 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 scrutiny limitation.


Tatum v. Laird, 444 F.2d 947, 963 (D.C. Cir. 1971) (citing the trial court decision).

Id. at 962-63 (citing the trial court decision).

Id. at 963.

Id. at 953.

Id. at 954.

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." 18

Rather than risking discovery directed at its domestic surveillance apparatus, the administration, in turn, sought Supreme Court review, which was granted in November 1971. 19 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, 20 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. 21

The ACLU and its allies, on the other hand, argued that legislative investigations 22 and parallel litigation 23 that followed the summary dismissal of Land 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. 24 They advanced a series

18 Id. at 998.
20 Brief for Petitioners at 12, Land v. Tatum, 404 U.S. 1 (1971) (No. 71-088) (defining "type of information that is available to all news media in this country"); id. at 15 (stating that it is "essentially no different from what a good newspaper reporter would be able to gather by attendance at public meetings") (citing majority opinion).
21 Id. at 20-21, 24, 26-27 n.24 ("[P]rior course of events presenting concrete evidence of unlawful inhibitory action.").
23 The ACLU had filed a related case in Illinois, which preceded through presentation of evidence to a preliminary injunction hearing before being dismissed, ACLU v. Westmoreland, No. 73-101 (N.D. Ill. filed Dec. 21, 1973). Westmoreland was dismissed on January 5, 1971, a dismissal that was affirmed by ACLU v. Land, 463 F.2d 699 (7th Cir. 1972), cert. denied, 409 U.S. 1138 (1973).
24 Brief for Respondents at 11-21, Land (No. 71-088) (referring to the record of Westmoreland and the Joint Committee hearings to highlight the continuing expansion of political surveillance powers, the breadth of the political group surveilled (including Americans for Democratic Action and the NAACP), the harmful dissemination of such information, and the court's sensitivity and internment that generated the information); Amicus Brief of a Group of Former Army Intelligence Officers at 16-19, 24, Land (No. 71-286) (highlighting scope of surveillance as described in hearing testimony, including undercover surveillance, "make-ups" of the spirit of Martin Luther King, impersonations of news media, illegal monitoring of radio communications, and looking for information to other government agencies, prisons, private employers, and subversive groups); id. at 26-28 (disputing the Justice Department's "errors and confusions of fact" concerning the limitations on military surveillance); Amicus Brief of Union/Universities Association at 11, Land (No. 71-286) (attaching copies of hearings of Senate Judiciary Committee's Constitutional Rights Subcommittee, commencing 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.

Chief Justice Burger, writing for a five-member majority, held for the defendants. His opinion acknowledged the "prejudicial 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. The majority opinion determined, however, that the plaintiffs' allegations made out no such injury. Somewhat distinguisheably, the opinion repeated the statement of the Court of Appeals that "[i]n so far as it 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." 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. In the absence of an exercise of "regulatory, prescriptive or compulsory" power by the government, a "subjective chill" was insufficient.

The Government urged the Court to take judicial notice of the existence of the legislative investigation. Brief for Petitioners at 55-56, Landi (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. Brief for Petitioners at 7-10, Landi (No. 71-288) urging the Court not to rely on materials presented at the legislative hearings.

* Landi, 468 U.S. at 15-16.

** Id. at 9 (citing 444 F.2d at 955). The crucial qualifier "as far as it is yet shown" made the statement technically accurate. The appendix's account of what had been "shown" in Landi ignored both the allegation of the commission of illegal invasions of privacy and the showings of record in both the parallel House Hearings and the congressional hearings that occurred after the record was closed as trial in Landi.

Likewise, the opinion maintained that the "principal source" of the information were news media and that some information was coming from public meetings and court law enforcement agencies. Id. at 6-7. This statement may or may not have been true, depending on the definition of "principal"; it was accepted formally, and at odds with the plaintiffs' allegations. Plaintiffs' maintained that only five percent of the reports came from news media, and that the sources of 99 percent of the surveillance were confidential private source records, and court informants. See Petition for Rehearing at 7-8, Landi (No. 71-288).

* 468 U.S. at 14.

** 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大纲 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. In response, the Justice Department acknowledged wiretaping one of the defendants without a warrant, but invoked what it regarded as inherent presidential authority over domestic security to maintain that the defendant had no right to examine the logs. 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 "ex post facto legal." 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, but the trial judge, Damon Keith, rejected it. The Justice Department in-

---

* See, e.g., United States v. Ellsberg, 466 F.2d 910, 924-25 (D.C. Cir. 1972) (rejecting defendant's claim that presidential authority to bug his office of Daniel Ellsberg's泄密 to protect national security interests); In re Bellinger, 564 F.2d 369, 399 (7th Cir. 1977) (invalidating government's action in the Chicago case); Bellinger v. Mitchell, 442 F.2d 782, 784 (D.C. Cir. 1971) (noting "the Government 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. Conner, 459 F.2d 163 (5th Cir. 1972) (allowing the government to collect and examine information by wiretapping conversations); United States v. Hugueley, 314 F. Supp. 705 (E.D. Va. 1966) (determining that the government did not have to disclose evidence of intercepted telephone conversations). United States v. O'Bryant, 304 F. Supp. 767, 768 (D.D.C. 1968) ("Since neither defendant's Fourth Amendment right nor Section 605 of the Federal Communications Act of 1934 were violated, the wiretaps used by the government to obtain foreign intelligence information was legal."); United States v. Smith, 311 F. Supp. 454, 458 (C.D. Cal. 1970) (concluding that in "real domestic situations there is no national security exemption from the warrant requirement"); United States v. O'Neal, No. KG-CR-1004 (D. Kan. Sept. 1, 1970); United States v. Brown, 517 F. Supp. 551 (E.D. La. 1970) (holding that the monitored telephone conversations by private officials did not taint defendant's conviction).
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 19, 1971 the Sixth Circuit affirmed. 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.

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.

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." 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. 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." [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

444 F.2d 651.

id. at 329 (Douglas, J., concurring). Citing these cases, the Emire hearings and journalistic revelations, he discerned a pattern of surveillance, bugging, interrogation, assignment, grand jury subpoenas, and efforts to discredit opponents. 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.

The trial court, the Government had argued that the President's inherent authority was immune from all review. 391 F. Supp. at 1077 (prompting Judge Keith to make the observation that "[w]e are a country of laws and not of men.").


id.; see also Reply Brief for the United States at 25-28, Keith (No. 70-155). The government argued, as well, that the Attorney General's judgment is reliable because it is "directly accountable to the President and through him to the electorate." Petition for Cert. at 8, Keith (No. 70-155).
United States—rather than to proliferate among all of the Federal sitting judges in the United States.\textsuperscript{15}

Unlike Land, the Court in \textit{Koeh} rejected the government's position without dissent.\textsuperscript{16} 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 "coercive and complexity of potential unlawful conduct" in domestic security cases.\textsuperscript{17} But it noted as well that "national security cases often reflect a convergence of First and Fourth Amendment values."\textsuperscript{18}

History abundantly documents the tendency of Governments—however benevolent and benign its motives—to view with suspicion those whom it fearslessly dispute its policies. Fourth Amendment protections become the more necessary when the targets of official surveillance may be those suspected of anorthodoxy in their political beliefs. The danger to political dissent is acute where the Government attempts to act under a vague concept as the power to protect "domestic security."\textsuperscript{19}

In light of the "potential danger[s] posed by unreasonable surveillance to individual privacy and free expression,"\textsuperscript{20} 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."\textsuperscript{21} (\textsuperscript{21} "\textsuperscript{21} Previewed executive discretion," the court held, "may yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech."\textsuperscript{22})

---

\textsuperscript{15} Transcript of Oral Argument at *1946, Koeh (No. 70-153).

\textsuperscript{16} Justice Rehnquist, before his elevation to the bench, had been a key player in establishing both the policies of post and domestic surveillance for the Nixon Administration. See Jeffrey W. Sung, Rehnquist, Evel and Revive, 53 BROOK. L. REV. 599, 602-03 (1987) (criticizing Justice Rehnquist's failure to recuse himself in \textit{Land}); Note, Justice Rehnquist's Denial to Participate in \textit{Land} v. Tennessee, 75 COLUM. L. REV. 198 (1975). He had not recused himself in \textit{Land} but elected to \textit{sit in} \textit{Koeh}. 407 U.S. at 524. Justice Burger concurred in the result without opinion, id., at 519; Justice White concurred in statutory grounds, id. at 535.

\textsuperscript{17} Id. at 976-77.

\textsuperscript{18} Id. at 976-77.

\textsuperscript{19} Id. at 976-77.

\textsuperscript{20} Id. at 910-14.

\textsuperscript{21} Id. at 910-14.

\textsuperscript{22} Id. at 916-21.

\textsuperscript{23} Id. at 317-22. The Koeh case left undecided the issue of whether the President could invoke powers unconstitutionally by the Fourth Amendment in the case of Savage-Story. See id. at 306 ("[T]he instant case requires no judgment on the scope of the President's surveillance powers with respect to the activities of foreign powers."). Lower courts divided on the issue. Compare United States v. Russo, 494 F.2d 905, 904-05 (3d Cir.) (en banc) (finding that none of the Fourth Amendment protections, but not a priori judicial warrant, might be applicable even where the President was acting pursuant to his foreign policy duties), cert. denied, 419 U.S. 881 (1974), and United States v. Brown, 484 F.2d 418, 420 (9th Cir. 1973) (holding that the President may constitutionally authorize warrantless searches for the purpose of gathering foreign intelligence), with Zweibon v. Mitchell, 516 F.2d 604, 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 Lariń, where no "regulatory, prescriptive, or compulsory" sanctions were deployed, gathering information was largely immune from constitutional challenge. 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 sought, even if the surveil-
ance 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 Con-
gress to alter the standards for issuance of the warrant. 407 U.S. at 702.

Lariń v. Tatum, 468 U.S. 1, 11 (1984). The distinction between "regulatory" activities, which were not considered to infringe the acquisition or dissemination of infor-
mation, which were not considered to infringe the acquisition or dissemination of infor-
mation, which were not considered to infringe the acquisition or dissemination of infor-
mation, which were not considered to infringe the acquisition or dissemination of infor-
mation, which were not considered to infringe the acquisition or dissemination of infor-
mation, which were not considered to infringe the acquisition or dissemination of infor-
mation, which were not considered to infringe the acquisition or dissemination of infor-
mation, which were not considered to infringe the acquisition or dissemination of infor-
mation, which were not considered to infringe the acquisition or dissemination of infor-
mation, which were not considered to infringe the acquisition or dissemination of infor-
mation, which were not considered to infringe the acquisition or dissemination of infor-
mation, which were not considered to infringe the acquisition or dissemination of infor-
mation, which were not considered to infringe the acquisition or dissemination of infor-
mation, which were not considered to infringe the acquisition or dissemination of infor-
mation, which were not considered to infringe the acquisition or dissemination of infor-
mation, which were not considered to infringe the acquisition or dissemination of infor-
mation, which were not considered to infringe the acquisition or dissemination of infor-
mation, which were not considered to infringe the acquisition or dissemination of infor-
mation, which were not considered to infringe the acquisition or dissemination of infor-
mation, which were not considered to infringe the acquisition or dissemination of infor-
mation, which were not considered to infringe the acquisition or dissemination of infor-
mation, which were not considered to infringe the acquisition or dissemination of infor-
mation, which were not considered to infringe the acquisition or dissemination of infor-
mation, which were not considered to infringe the acquisition or dissemination of infor-
mation, which were not considered to infringe the acquisition or dissemination of infor-
mation, which were not considered to infringe the acquisition or dissemination of infor-
mation, which were not considered to infringe the acquisition or dissemination of infor-
mation, which were not considered to infringe the acquisition or dissemination of infor-
mation, which were not considered to infringe the acquisition or dissemination of infor-

The Lariń majority's dramatic refusal to acknowledge the nature and scope of the Army's surveillance program, ironically, formed the basis for subsequent dissections of Lariń by some lower courts. E.g., Hollow v. Dolea, 125 F.3d 146 (M.D. Ga. 1997) (expanding target-
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." 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 mission a separation of sensitive information and military power be maintained, as a separation of match and powder. . . . (T)o permit the military to execute 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.

The files challenged in Laird were probably poorly adapted to actually implementing a coup. While "counterintelligence" rhetoric was occasionally utilized by military planners, the ultimate goal was simply to provide advance warning of potential plots in which the Army would be called upon to provide backup for civilian authorities. 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.58


60 Plea, supra note 21, at 519-24, at 523-35 (noting that the official doctrine did not contemplate the imposition of criminal law).

61 The FBI conducted "tests of thousands of domestic intelligence investigations" to identify candidates for incarceration under the "Emergency Detention of Suspected Security Risk Persons" of the Internal Security Act of 1950, Pub. L. No. 93-243, 64 Stat. 987, 1061, which was rescinded in September 1971, Pub. L. No. 92-128, 85 Stat. 547 (1971). W. Raymond Warr, Undermining Counterintelligence (Capability), in INTL. J. INTELLIGENCE & COUNTERINTELLIGENCE 321-22 (Fall 2002) (reviewing the repeal of this provision); see also Donner, supra note 74, at 162-69 (discussing "crossover 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 list. 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 exercise of administrative discretion.

2. Blacklist, 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. 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 usually subject to public stigma, scorn and obloquy.

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
psychiatry's office was an effort to find information that could discredit the release of the Pentagon Papers."

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 \textit{Lemon 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 sets 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."

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.

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

---

8. \textit{See}, e.g., \textit{United States v. Enslow}, 566 F.2d 910, 913 (D.C. Cir. 1977) (noting the even the Government's brief conceded that the reasons for interest in Ellsberg's psychiatric records were, at least mixed and included creating a "negative press image" of Ellsberg); \textit{David, supra note 39 (1999) (detailing CONTELPRO reports); Donnelly, supra note 91, at 179-82 (detailing dissemination of files); id. at 277-278 (detailing CONTELPRO results).}


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 threat of submission 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.

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." 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. In 1975, the Senate formed the

---


8 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, and in the next session they established permanent intelligence oversight committees in both the House and Senate. In 1978, agencies were required to establish inspectors general, and in the Foreign Intelligence Surveillance Act ("FISA"), Congress directly addressed the issue of foreign intelligence searches that the Court had pretermitted in <i>Keith</i>. In the executive branch, executive orders issued by Presidents Ford, Carter, and Reagan set constraints on the activities of the intelligence community. The Defense Department established an Office


On January 30, 1975, 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, 1975, as 1, and later in book form in Senate under the title CIA: The Pike Report (Scribner Books 1977). On April 26, 1975, the Church Committee issued its final report, S. Rep. No. 94-750 (1976) (recommending a law 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.


Executive Order No. 11,905, 36 Fed. Reg. 7077 (1975) [hereinafter Ford Order]; Executive Order No. 12,035, 43 Fed. Reg. 5674 (1978) [hereinafter Reagan Order]. These Orderlimited the collection of intelligence regarding "United States persons," mandated the use of "lawful techniques for the collection of intelligence," and required that the CIA provide a "fuller description of the activities and transactions in which a former director, Israelis, or any person participating in the same or related matters." Executive Order No. 12,035, 43 Fed. Reg. 5674 at 5679 (1978) (amended at 50 U.S.C. §§ 5505-52). See also Carter Order at §§ 2.205 to 2.206; Order No. 5. The Carter and Reagan Orders also promulgated regulations other than the FISA: striking to covert influence operations in the United States, while constraining covert participation in arms sales. Reagan Order at 50,552; Carter Order at § 2.207; see also U.S. Postal Service, Inspection Service Authority.
of Inspector General for Intelligence in 1976, which became the Assistant to the Secretary of Defense (Intelligence Oversight) in 1982. 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, 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.”

Beyond the limits embodied in passive law, aggressive Congressional investigation and exposure proved as important as statutory constraints. The trauma of the hearings and the fiefdom of outrage those hearings produced has etched in organizational culture of a number of agencies the propriety of abusing secure 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. In Barron v.
Vopper, an otherwise divided court recently coalesced around the preposition, 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 serious inhibiting effect upon the willingness to voice critical and constructive ideas. 10

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 Kehl 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. 100 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. 101 Given the dependence of Internet

protection accorded to anonymous observers; Buckley v. Am. Constitutional Law Found., 390 U.S. 182, 194-204 (1968) (writing dissenting opinion); see Thornburgh v. Am. Ctr. of Obscuri & Greecen. 762 F. Supp. 67, 70 (1990); 100 "(The) reappraisal of the role of the public interest in deciding, in light of a particularized concern, what constitutes a reasonable expectation of privacy with respect to a public record is by no means compelling, see, e.g., New York v. Ferber, 458 U.S. 19, 34 (1982) (affirming conviction under the Interstate Commerce Reform Act of 1982 (ICRA), 108 Stat. 1, 2 (1988)), citing In re grand jury, 871 F.2d 267, 270 (2d Cir. 1989) (upholding warrantless surveillance in a public place, such as a newsstand, but declining to hold that a warrant is required to search a private home)."

100 11 C. W. Smith v. Maryland 442 U.S. 735, 745-46 (1979) (holding that "pen register" does not require warrant, since telephone numbers are disclosed to telephone company); United States v. Miller, 435 U.S. 425, 440-45 (1976) (finding defendant has no "reasonable expectation of pri-
communication on intermediaries, this opens a vast array of communications to government surveillance.\textsuperscript{44}

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 rate 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 bureaucrats—who dispense benefits and licenses, who hire and fire, who plans health care programs or fiscal policy—has replaced the police officer, judge, or soldier as the locus 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-

\textsuperscript{44} "in bank records; Cal. Bankers Ass'n v. Shulte, 416 U.S. 31, 54 (1974) (finding that required maintenance of bank records does not violate Fourth Amendment). Given the emerging availability of cell phone eavesdropping technology, see A. Hershon, Leak? Hiding? Your Cellphone Is Kingpin, N.Y. TIMES, Dec. 21, 2003, at Al, access to telephone records will become even more revealing.

Again, there may be limits on the retention of particular trusted intermediaries, e.g., Ferguson v. City of Chauncey, 552 U.S. 67, 79-90 (2007) (holding that police have "legitimate expectation of privacy" in medical records), but these limits are far from starkly etched.

\textsuperscript{45} E.g., Erin S. Berr, Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't, 97 MINN. L. REV. 607, 677-79 (2003) (arguing that "so-called" doctrine leaves Internet communications without constitutional protection). The capacity to examine the contents of e-mail through such technologies as Grammar and SCHOLL is constrained in some circumstances by the Electronic Communications Privacy Act, and subject to VISA under the USA PATRIOT Act, 16. at 615. Once access is gained, moreover, there is likely to be an intra race between cryptography-using entities of surveillance and government monitors. Ted伯de, FBI Is Building a "Magic Lantern." Would Alliance Agency in Million Computer The WASH. POST, Nov. 23, 2003, 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 employees, moreover, monitor the Internet connections of their employees. See Birk Zurovec, Who Knows What About Whom? Towards a Generalized Surveillance, Presentation at the Third UNESCO Philosophy Forum (Sept. 14, 2002) (reporting more than one-third of employees monitor employees' Internet activities), at http://www.q selfish.co.uk/sociology/surveillance/publications-zur/ (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 315 of the USA PATRIOT Act. The Unitig 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, § 315, 115 Stat. 272, 287-88, of officials to demand copies of logs of such monitoring.

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 graver 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.

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. 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.

In the aftermath of September 11, many businesses volunteered or grudgingly surrendered access to their records to law enforcement or intelligence officials. 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...
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 and state and federal agencies, including motor vehicle records, liens, deeds transfers, criminal records, voter rolls, and military personnel records. 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. Conversely, the MATRIX system, based in Florida, proposes to link state, federal, and private databases in a searchable configuration.

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 the risks that had heretofore been hypothetical; the costs of...


103 Office of Gen. Counsel, Natl Sec. Law Unit, Guidance Regarding the Use of ChoicePoint for Foreign Intelligence Collection or Foreign Counterterrorism Investigations (Sept. 17, 2001) (pointing legal opinion that ChoicePoint files are "publicly available data," and therefore "minimally intrusive"); http://www.epic.org/privacy/choicepoint/epfpla.pdf. Simpson supra note 102 (giving account of desktop access). In many FBI offices personally targeted computers are in a "closed" network; to access ChoicePoint, or any other "outside" network requires that a person go to a standalone terminal. Personal Communication from N.C. Bowen, Senior Counsel to the FBI (June 21, 2004) (mimeo). See note with author.

104 E.g., Brian Bergenstal, Database Supercharged Terror Quillen, May 30, 2004 (describing 120,000 person list of individuals with a "high terror association" provided by private database owner Scinti to federal authorities, based on "such factors as age, gender, ethnicity, credit history, occupational data, information about phone and driver licenses, and connections to 'suspicious addresses known to have been used by other suspects'"); http://www.npr.org/templates/story/story.php?storyId=59004000. According to one report, the 120,000 list was refused to 1,200, which formed the basis for investigations and some arrests. Robert O'Harrow Jr., Anti-Terror Database Guts Hole, at World Summit, Wash. Post, Mar. 21, 2004, at A12, and also Ryan Singel, COPPS II Sandbag Alert, Fast Sep. Wired News, Jan. 15, 2004 (discussing proposal to allow secret personal as well as criminal identity by checking commercial databases such as those owned by ChoicePoint, Ascend and LexisNexis), at http://www.wired.com/news/privacy/0,1288,184641,00.html (last visited Sept. 30, 2004); Ryan Singel & Noah Shachtman, Anti-Terror Using Jotshal Data, Wired News, Sept. 25, 2005 (receiving release to Anti-terrorism, Torch Concepts, of millions of records of jitterbug passengers and comparison of the data at http://www.wired.com/news/privacy/0,18465095-01-00.html (last visited Sept. 30, 2004).

105 See MATRIS, supra note 11.
ignorance became horrifically 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. Likewise, international cooperation holds the possibility of allowing U.S. intelligence agencies to avoid domestic limits on electronic surveillance. 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. 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 investigatory techniques.

---

68 Section 308 of the USA PATRIOT Act, Pub. L. No. 107-56, § 308, 115 Stat. 272, 278-80, amended Fed. R. Crim. P. 6(a)(5)(D) to permit disclosure of grand jury information when the matters involve "foreign intelligence and counterintelligence." Section 566, 115 Stat. at 304-05, amended the FISA to permit coordination between intelligence officials conducting FISA-approved surveillance efforts and law enforcement officials.

69 At least one source claims that British and U.S. intelligence agencies exchange surveillance information on each other's citizens, Phillip Knightley, How Britain and the US Keep Watch on the World, 16905 (London), Feb. 27, 1994, although the scope of such cooperation has not been proved.

70 See Attorney General John Ashcroft, Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations, pt. VIA.3, 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/olgs/generalcrimeent.pdf, id. at VIA.2, at 22 (authorizing suspicionless monitoring of online sites and forums); see also id. pt. VIA.1, at 21 (authorizing maintenance of databases from any source).

Part VI.C.1 of the Ashcroft Guidelines caution 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 emphasis with which the current Justice Department places its authority, presumably, files maintained partially for the purpose of monitoring First Amendment activities, but also for the purpose of preventing terrorism (or of gauging the custody of the atomic generals) would not fall under the prohibitions.

71 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 appears, from the circumstances or the content in which the statements are made, that there is no prospect of harm.


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 deprivation 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 that prior-out requirement.
Post-September 11 statutory innovations have provided new authority to demand information without judicial supervision or probable cause. \(\text{[11]}\) have obliged courts to issue secret subpoenas and "wrap and trace orders" on an ex parte FBI showing of "reasonable" rather

The prior guidelines decreed that "before employing an investigative technique in an in-

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 uncontrolled and unilateral ability to invoke governmental powers that previously rested in grand juries seeking to prosecute crimes. 38 U.S.C. § 2709(b)(1) (2009), 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.\(\text{[12]}\) This au-

Similar authority and concerns apply to the newly available national security letters to fin-

Title 51, section 5312(a)(2) of the United States Code reads National Security Letter au-

The "financial records" to which the FBI may demand access include any "information

Likewise, the Health Insurance Portability and Accountability Act (HIPAA) regulations pro-

\(\text{[11]}\) E.g., Order No. 15-333 (2011).
than probable cause,\(^{19}\)

\(^{19}\) Under Section 215 of the USA PATRIOT Act, 115 Stat. at 267-46, 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) (2000). However, the investigation may not be "concerned of a United States person solely upon the basis of activities protected by the First Amendment to the Constitution." 50 U.S.C. § 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. § 1681(c)(1) (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 email 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 United States person) "is not conducted solely upon the basis of activities protected by the First Amendment to the Constitution." 50 U.S.C. § 1842(c)(2).

\(^{20}\) 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 as long as foreign (espionage) gathering or intelligence 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 power." See generally P. S. Sealed Case, 59 F.3d 717, 719-20 (Foreign Int. Surv. C. Rev. 1992). 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.")

\(^{20}\) See, e.g., Providence, supra note 106 (describing energetic effect of increase in computer storage and non-papering along with increased data collection technologies). The GAO reports that "newspaper data mining projects are currently being undertaken by federal agencies, fifteen of which use private sector data." GAO, DATA MINING, supra note 50.

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

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. 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." 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 circumvented 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.

---


58 Similarly, one of the major objections to domestic military intelligence is that it makes military less dependent on civilian branches (and locations) in domestic operations. E.g., PNA, supra note 21, at 466 (discussing how the Attorney General opposed military intelligence because it posed dangers to civilian control and federalism).


60 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." 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. 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 re- jected the claims that the efforts to detain "unlawful combatants" can proceed entirely free from the constraints of judicial review or due process. 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 40.
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. 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. The trial court threw out his perjury prosecution on the ground that the "material witness" statute was misused. On appeal, the Second Circuit reinstated the prosecution and upheld the invocation of the material witness statute.

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." 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 nonconformity 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 fingerprints to a fingerprint connected to a terrorist bombing appeared in juxtaposition with the facts that he had prayed

---

17 Id. at 59.
18 Id. at 61.
19 United States v. Awadallah, 549 F.3d 42, 75 (2d Cir. 2008).
20 Id. at 56, 54; Reno v. United States, 489 F.2d 955 (9th Cir. 1973), see DENNIS, supra note 74, at 605-08; Michael E. Deitch, The Improper Use of the Federal Grand Jury: An Instrument for the Incrimination of Political Activists, 75 J. GEN. L. & CRIMINOLOGY 1159, 1181 (1984).
at a mosque and had represented a suspected terrorist in a child custody proceeding.”

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.” 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

According to one report,
Federal officials told Newsweek that they drove Mayfield to a mosque and converted to Islam 16 years ago. The couple was active in a local Qenberi mosque whose members had openly pursued government antiterror policies ... [and] in 2002 Mayfield had volunteered to provide legal help [in a child custody matter] for Jeffrey Battle, one of the defendants of the Portland Seven—a group of local jihadis who had flown to Asia after 9/11 in an unsuccessful effort to fight with the Taliban.”


15 In U.S.C. § 2339B(d)(1) (2002), In Humamization Law Project v. U.S. Department of Justice, 303 F.3d 561, 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, Humamization Law Project, 303 F.3d 1154 (9th Cir. 2006), 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. § 2015 (2004).
support," but backed off in the face of protests.19 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,20 and the Justice Department's "material support" prosecutions include a recent action against a computer science student, Sannu Omar al Hussayen for maintaining websites which contained Islamist writing—a prosecution which only ran aground on the common sense of an Idaho jury.19 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.21

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.22 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-

22 Humanitarian Law Project v. Dept. of Justice, 552 F.3d 592 (9th Cir. 2009) (requiring specific intent to further terroristic aims and holding prohibition of providing "training" and "personnel" to be impermissibly vague); Humanitarian Law Project v. Ashcroft, 309 F. Supp. 2d 1185 (E.D. Cal. 2004) (holding prohibition of provision of "expert advice or assistance" to be impermissibly vague).
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." 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.12

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.13 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.14 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.15 In the

---

13 See Reno v. Am. Arab Anti-Discrimination Comm., 525 U.S. 641, 689 (1999) ("[An alien unlawfully in this country has no constitutional right to assert selective enforcement as a defense against his deportation."); the list of the "L.A. 8," a group of Arab community organizers originally accused of advocating world communism under a false pretense, which was an 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 illegal at the time it occurred. See Editorial, Deep Thugs, WASH. POST, Nov. 1, 2000, at C28 (detailing proposed deportation for having held fundraising events and rallies and having distributed magazines between 1964 and 1966).
15 Ryan Sorgel, Data Scan for Watchlist Usage, WASH. NEWS, May 17, 2004 (describing 180,000 persons "watch list" produced by the "Terrorist Screening Center," available to highway patrol officers, airline screeners, and border control officials), at http://www.wtrd.com/news/privacy/1.844885878.05.html; Guy Taylor, FBI Up for Private Search, WASH. TIMES, Mar. 26, 2004 (recouning 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 their identity against government-provided watch lists. USA PATRIOT Act § 317(a), 115 Stat. at 309-05 (codified as 11 U.S.C. § 1532(b)).
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; 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, and has specifically refused the advice of the Justice Department's Inspector General to disengage its terrorist surveillance from surveillance of political protest. 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 enanglement as material witnesses from participating in dissenting activity. Conversely, here has been at least one high profile effort by Republican legislators to use anti-terrorism surveillance data for partisan

---

66 U.S. Attorney General John Ashcroft, Prepared Remarks for the U.S. Mayor's Conference (Oct. 23, 2001) ("Robert Kennedy's Justice Department, it is said, would arrest multipliers for 'spitting on the sidewalk' if it would help in the battle against organized crime. I have 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.").

67 See, e.g., Karen Abbott, Warnings Proved Party Commissions, ROUGH RIDS NEWS, July 24, 2004 (describing FBI questioning twenty-one year old American Friend Service Committee intern at her home as part of investigation of "promoters and anarchists" by Joint Terrorism Task Force,

68 The Office of the Inspector General of the Department of Justice recommended "transferring responsibility for investigating crimes committed by environmental, animal (fights, and other domestic radical groups or individuals from the Counterterrorism Division to the Criminal Investigative Division." CIC, FBI'S REPORTS, supra note 9, at 50. The FBI refused, id. at 95–98 pp. It. The Inspector General reiterated its belief that the FBI's priority mission is 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 protesters 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 Animal Proteus," but that appendix was redacted.
purposes. Although the FAA has issued a rule limiting release of the precise data involved in this case, 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.

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 bureaucracy is far more likely to be disciplined for not knowing information its superior desires than for collecting too much information. 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 incommensurate. 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
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. Rather, having administrated some of the costs in political freedom that inheres 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 commended.

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.16

16 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 (2001) (critiquing CAPPS II); id. at 188-90 (critiquing data mining to find terrorists); id. at 255-56 (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 (2006). (“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.”).

17 BLACK v. MOORE, 798 F.2d 1205, 1214 (D.C. Cir. 1986) (Scalia, J.). See also, e.g., PAVLICENKO v. SCOFIELD, 328 U.S. 212 (1946) (describing the effectiveness of the GDR and its based on the combination of surveillance with the power of arbitrary arrest, backmail, “systematic discriminating,” and the “haunting fear that you could be arrested anytime . . . the Stat . . . 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. 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.

A world of increased informational interpenetration, transparency should run in both directions. If government officials are better...
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, legally, and accurately.”

B. Designing for Disent: 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

477 Detroit Free Press v. Ashcroft, 539 F.3d 681, 685 (6th Cir. 2008) (holding that the Attorney General can order blanket closure of immigration hearings in the media and the public). In this regard, the Supreme Court’s decision to deny review in M.R.R. v. Warden, 114 S. Ct. 1490 (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 run-up following September 11, is particularly disturbing. Mohamed Kameel Bellahoud 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 eating alone at a Middle Eastern restaurant in Delray Beach, Fla., and reportedly “was seen entering a movie theater with a third Sept. 11 hijacker, Ahmed Alhujjani.” James McLaughlin, Right of Justice: 28 NSW MEDIA & LAW 1 (October 2004), http://www.nclf.org/news/mag/381/co-w-blackout.html. All proceedings in Bellahoud’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. 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.

Existing approaches to multilevel relations in the context of multilevel secure databases allow only users with appropriate security clearances access to classified data. Technologies 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. 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.

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 control how the information or conclusions in a document are used.


See, e.g., Chris Stromh, Homeland Security Privacy Office Pushes Training Efforts, GONZESC.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.gonzesc.com/dailyfed/1103/ 1172003.htm.


E.g., Mario Cardia, Monte et al., TOWARDS ACCOUNTABLE MANAGEMENT OF IDENTITY AND PRIVACY: STUDY POLICIES AND ENFORCABLE TRADING SERVICES 6-6 (2003) (proposing a model that employs sticky privacy policies to increase data records 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, 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 isolation of data from determining the nature and purpose of the search. A variety of commentators have suggested that national security data mining make use of these technologies to limit examination information about innocent individuals. Indeed, the ill-fated TIA program itself contemplated developing a "privacy appliance" to assure that searches did not extend beyond proper limits.

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 techn-
ology. The theoretical availability of a "privacy appliance," "strict" 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.

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 or even 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 name, a friend, or a tendency to visit certain websites or bulletin boards, where coded messages might have been left.

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 "adversion." 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 anti-terrorist intelligence, and policies which stand directly in the way of sharing are unlikely to prove durable. To take

---

47 For example, the practice of collecting vast amounts of information on American citizens was terminated in 1971, when the Department of Defense concluded that data collection for the destruction of all files on "unessential" persons and organizations. Rather than destroying the files, however, several Army intelligence units simply turned their intelligence files and disdained individuals and groups over to local police authorities and one (a Force commander) agreed to create new files for the new year.

C. Thomas G. Greer, Al Qaeda Said to Be Using Sapped Faxes, REGISTER, May 12, 2001, reporting and purporting to be true that al-Qaeda members left secure messages embossed in photographic photographs on Internet bulletin boards, at http://www.thereregex.co.uk/2001/05/12/djihadistsaid_tobeusing. More reputable analysts seem to believe that al-Qaeda uses coded messages in standard e-mail and Internet 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. 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. 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.

---

*See COMM’T for REVIEW of FBI SEC. PROGRAMS, DEPT. OF JUSTICE, A REVIEW of FBI SECURITY PROGRAMS 66–68 (2003) (specifying the abandonment of “need to know” access which facilitates the repeat of the Hansen debacle); available at http://www.aoig.gov/ dpag/publications/watermark.pdf. The FBI will presumably respond to this concern in future efforts.

E.g., id. at 69–71 (describing discovery of misuse of FBI Automated Case Support system by Robert Hansen through review of audit logs); 28 C.F.R. § 25.200(g) (imputing that a “project maintaining criminal intelligence information shall ensure that administrative, technical, and physical safeguards (including audit trails) are adapted to ensure that unauthorized access and against intentional or unintentional damage. A record indicating who has been given in formation, the system for release of the information, and the date of each dissemination outside the project shall be kept”); § 25.200(g)(3) (“The project must store information in the manner so that it cannot be modified, deleted, altered, exchanged, or purged without authorization.”); cf. MATRIX, PRIVACY POLICY § 8 (2004) (requiring log of access and dissemination of information), available at http://www.matrix.org/privacy_policy.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 free-lance surveillance of dissidents or innocents of privacy. They allow organizations to track whether their own rules are being flouted, a capability as important for maintaining security as for maintaining privacy. 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. 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. Such a system could monitor the accuracy of the results of queries and could also be key to alert supervisors to politically based or otherwise improper data analysis.

To be sure, like access control technologies, audit trails are technologically dependent. They will be less useful in less technologically sophisticated environments and can be evaded to some extent by mov-
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 as such. 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, G&O 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").
by discovery in other litigation. 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 refused FOIA requests and has sought to block any public inquiry into its initiatives. 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 discrepancy 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 eroded. 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/SafesandFree/SafesandFree.cfm?ID=15374&cID=252 (last visited Sept. 30, 2004); ACLU, ACLU Seeks Government Accountability For No-Fly List ("The 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/SafesandFree/SafesandFree.cfm?ID=74722&cID=496 (last visited Sept. 30, 2004); Press Release, ACLU, What Is The Magic? (ACLU Seeks Answers on New State-Run Surveillance Program (Oct. 30, 2005) ("The goal of the request 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=14578&cID=130; Press Release, ACLU, Declassified FBI Documents Suggest Shoddy Management of No Fly List, Fail to Show How Innocent Americans Can Get Names Dated; (Dec. 4, 2005) (describing the FBI's erroneous release of classified documents about the controversial ‘no fly’ terrorist watchlist); http://www.aclu.org/SafesandFree/SafesandFree.cfm?ID=140284&cID=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).


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 discarded 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 ef-
fect on security officials. The salutary quality of this effect is likely to
be strengthened if—as should be the case—extraordinary surveil-
ance 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 fric-
tionless environment destabilizes the checks and balances. If a secur-
ity bureaucrat faced no cost to exploring a citizen's life, while the
failure to explore that life carries a risk of catastrophe, however mar-
ginal, 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 bu-
reaucrat with a shadow "budget" which would be charged each time
she accessed the details of a citizen's life.10 Notwithstanding the avail-
ability of technology that could accomplish the task of taxing inquir-
ies, this approach is unlikely to find favor in today's environment,
both because the challenge of setting the appropriate level of pay-
ment would be controversial and because the actual technology de-
ployed by security bureaucrats is likely to be primitive. There is, how-
ever, another approach which can capture some of the virtues of
micropayments. If authority to gather or analyze data must be reau-
thorized at regular intervals, a sunsetted authority combined with the
prospect of disclosure to an authorizing agency that is sensitive to the

10 In a still more utopian vision, one could imagine allowing citizens to set the level of
payment which they were willing to accept for a "park." Compare Venkatesh Balak & Eric Syv-
johtio, Aggregation and Deggregation of Information Goods: Implications for Bundling, The Law-
ening and Micropayment Systems in INTERNET PUBLISHING AND BEYOND: THE ECONOMICS OF DIGITAL
INFORMATION AND INTELLECTUAL PROPERTY 177-20 (Brian Kalin & Hal R. Varian eds., 2004),
news/story/0,15722,11433,00.html, with Ronald J. Mann & James K. Wink, ELECTRONIC
COMMERCIA 409-61 (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." 18

CONCLUSION

In today's environment, ex ante judicial control of surveillance is unlikely. One response lies in strengthening legal doctrines that 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 Attorney 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 mechanisms not been in place, we very well could have seen the same abuses all over again. 19

19 History, Intelligence Oversight, supra note 58.