IMBALANCE OF POWERS

How Changes to U.S. Law & Policy Since 9/11 Erode Human Rights and Civil Liberties

September 2002 — March 2003

Imbalance of Powers **is an update to Lawyers Committee's** ***A Year of Loss: Re-examining Civil Liberties Since September 11*****, which was published in September 2002.**

LAWYERS COMMITTEE
FOR HUMAN RIGHTS

Chapter 2

RIGHT TO PRIVACY

INTRODUCTION

The right to privacy is protected by the Fourth Amendment to the Constitution. The Fourth Amendment limits the government's search and seizure powers to "prevent arbitrary and oppressive interference by enforcement officials with the privacy and personal security of individuals."[74] It protects our "right to be left alone," a right which U.S. Supreme Court Justice Louis Brandeis termed "the most comprehensive of rights, and the right most valued by civilized men."[75]

In the wake of September 11, many longstanding prohibitions on government surveillance powers were revoked — with little public discussion or debate. In the last six months, Congress and the courts have made some efforts to check new proposals to further expand the administration's surveillance powers and its access to the personal data of U.S. citizens and others. In other instances, they have allowed further overreaching and secrecy by the executive branch.

In the wake of September 11, many longstanding prohibitions on government surveillance powers were revoked — with little public discussion or debate.

One important aspect of the recent debate involves Operation TIPS, a neighbor-to-neighbor spy program proposed by the Justice Department and designed to encourage citizens to report on the "suspicious activities" of people in their communities. There was a note of irony in Attorney General Ashcroft's advocacy of TIPS — as a senator he had criticized the previous administration's "paranoid and prurient interest in [monitoring] international e-mail" as "a wholly unhealthy precedent" — warning that the American people should not "hand Big Brother the keys to unlock our e-mail diaries, open our ATM records or

translate our international communications."[76] As attorney general, Ashcroft pressed hard for the establishment of Operation TIPS, but Congress turned him down. The final bill establishing the Department of Homeland Security includes a provision banning Operation TIPS.

Despite the strong public reaction against Operation TIPS, the Bush Administration is pursuing an even more invasive initiative: the Total Information Awareness (TIA) program. Total Information Awareness, as its name suggests, is a comprehensive data-mining project, powered by a computerized system that would tap into, integrate, and extrapolate data from thousands of public and private databases. The Pentagon-based project would link data from a wide variety of sources (such as private healthcare records, employment records, school records, library records, and information on purchases) with the monitoring of domestic and international e-mail traffic. As proposed, TIA then would develop a comprehensive data profile of citizens and noncitizens utilizing: biometric, financial, education, travel, medical, veterinary, country entry, transportation, housing, government, critical resources, and communications data.[77] Following a public outcry from many quarters, however, Congress passed a temporary ban on funding for TIA until it could assess its impact on civil liberties.

The administration has also drafted new legislative proposals that would further infringe on Fourth Amendment privacy rights by expanding law enforcement surveillance and intelligence gathering powers. The Domestic Security Enhancement Act of 2003 (known informally as PATRIOT II) would dramatically expand the scope of the Foreign Intelligence Surveillance Act, end consent decrees against illegal police spying, and establish a Terrorist Identification Database, a DNA database that would allow the government to collect genetic information on convicted terrorists as well as on those the government suspects of being involved in terrorist activity.

ACCESS TO LIBRARY AND BUSINESS RECORDS

The government has achieved much of its data gathering by demanding that retailers, libraries, schools, internet service providers, and others turn over client information. Section 215 of the USA PATRIOT Act requires libraries, bookstores and other venues to turn over business records, documents, and other items on demand if the FBI has declared that the items are being sought for an ongoing investigation related to international terrorism or clandestine intelligence activities. Many commercial establishments reportedly have turned over client information without objecting to the government's requests.

This invasion of privacy regarding personal information is exacerbated by provisions that keep secret the fact that the government has accessed this information. Section 215 of the USA PATRIOT Act makes it a crime to reveal that the FBI has seized customer records. This means, for example, that a librarian who speaks out about being forced to reveal a patron's book selections can be subject to prosecution.[78] Even information on the general direction and scope of measures to seize consumer records has been suppressed. In July 2002, House Judiciary Committee Chairman James Sensenbrenner (R-WI) requested information about whether Section 215 of the USA PATRIOT Act had been used to access library, bookstore or newspaper records and, if so, how many times. But the Justice Department refused to answer, saying that such information is classified.[79]

Librarians and booksellers have been outspoken about the potential these new measures have to chill freedom of expression and inquiry. In some parts of the United States, these groups have considered changing their record systems to limit the personal information they acquire from their clients.[80]

The American Library Association (ALA) and other major library organizations have introduced new guidelines for dealing with federal warrants while discussing how to document intrusive measures without putting librarians in legal peril. In a December 11, 2002 consultation, these organizations, including the ALA, the American Association of Law Libraries, and the Special Libraries Association, recommended that "[l]ibrarians should document all investigative actions related to the USA PATRIOT Act."[81]

The American Library Association's Freedom to Read Foundation (FTRF) and the American Booksellers Foundation for Free Expression (ABFFE) joined the ACLU and the Electronic Privacy Information Center in an October 24, 2002 lawsuit brought to request information on subpoenas issued to bookstores and libraries under the USA PATRIOT Act.[82] The lawsuit summarized the scope of Section 215:

> [T]he new provision can be used to obtain circulation records from libraries, purchase records from bookstores, academic records from universities, medical records from hospitals, or e-mail records from internet service providers. The government need not show probable cause or any individualized suspicion of criminal activity; rather, it need only assert that its request is "for an authorized investigation . . . to protect against international terrorism or clandestine intelligence activities.

To understand how the new law can result in a widespread invasion of privacy, it is instructive to examine what happened when the government became concerned that underwater diving skills might be used to perpetrate a terrorist attack. Based on this concern, the FBI attempted to acquire the records of everyone who had taken a scuba-diving course with a dive shop or at the local YMCA. Instead of investigating particular individuals about whom the government might have suspicions, the FBI sought to collect personal information on *all* scuba diving students in order to spot potential wrongdoers. The operation, which may have produced personal details on millions of Americans, came to light when a small dive shop in California — Reef Seekers Dive Company — refused to turn over records on clients, "even when officials came back with a subpoena asking for 'any and all documents and other records relating to all noncertified divers and referrals from July 1, 1999, through July 16, 2002.'"[83] The subpoena was withdrawn when it was made clear that it would have to be defended in a court of law.[84]

EXPANSION OF POWERS UNDER THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA)

BACKGROUND TO FISA

Congress enacted the Foreign Intelligence Surveillance Act (FISA) in 1978 to create a separate legal regime for the gathering of foreign intelligence information, as opposed to domestic law enforcement information.[85] FISA grants the FBI exceptional powers to monitor foreign powers and their suspected agents in counterintelligence operations within the United States.[86] In using these powers, the FBI is exempt from the traditional Fourth Amendment requirements applicable to criminal investigations.

Under FISA, for example, the FBI submits warrant applications to the Foreign Intelligence Surveillance Court, a secret court that hears the government's applications *ex parte* (hearing one side only). In order to obtain warrants under FISA, moreover, the government does not have to demonstrate probable cause of a crime.[87] Instead, the FBI must demonstrate only that there is probable cause to believe that the target of the surveillance is an agent of a foreign power.[88] In order to obtain FISA warrants against "U.S. persons" (i.e., U.S. citizens and legal permanent residents of the United States), however, the government also has to establish that the activities "involve" or "may involve" a violation of criminal statutes (a lower standard than applicable under ordinary criminal law).[89] For "non-U.S. persons," on the other hand, the government

does not have to make any showing that the suspected foreign agent is doing, or is planning to do, anything illegal.[90]

After obtaining a FISA warrant, the FBI can conduct surveillance and physical searches against a suspected foreign agent for a period of 90 days and against a foreign power for an entire year. The searches and surveillance are carried out surreptitiously, without any notice to the people being monitored unless and until they are prosecuted. Furthermore, even if the targets are prosecuted they are generally not permitted to challenge the substance of the government's FISA applications and affidavits, as FISA mandates an *in camera* (closed chambers), *ex parte* review of these materials "if the attorney general files an affidavit under oath that disclosure or an adversary hearing would harm the national security."[91]

Because of the extraordinary nature of these powers, Congress limited the circumstances under which they could be used. The FBI could only use its FISA powers for "the purpose of" gathering foreign intelligence information. The Foreign Intelligence Surveillance Court implemented procedures to enforce this line, trying to ensure that the information obtained through FISA searches and surveillance was not used *sub rosa* in criminal prosecutions.[92]

USA PATRIOT ACT AMENDMENT

At the urging of the administration, however, Congress significantly expanded the government's FISA powers shortly after September 11, 2001. Under Section 218 of the USA PATRIOT Act, the FBI can now seek FISA warrants when the gathering of foreign intelligence is merely "a significant purpose" of the warrant — a slight change in wording that has far-reaching implications. The administration immediately argued that the FBI could now seek a FISA warrant when the government's "primary purpose" was the gathering of information for domestic criminal investigations.[93] This interpretation would mean that FISA, which was enacted to facilitate the gathering of foreign intelligence information, could now be used as a way to sidestep Fourth Amendment requirements in regular criminal investigations.

The Foreign Intelligence Surveillance Court did not agree with the administration's position. In May 2002, the secret FISA court issued its first ever public opinion, unanimously finding that the administration's interpretation of the amendment would turn the entire purpose of FISA on its head.[94] The court — composed of seven federal judges[95] — imposed restrictions on the administration's interpretation of its new powers, refusing to permit domestic law enforcement officials to "make

recommendations to intelligence officials concerning the initiation, operation, continuation or expansion of FISA searches or surveillance."[96]

The Department of Justice appealed the decision to the Foreign Intelligence Surveillance Court of Review ("the Court of Review"), a court composed of three semi-retired federal judges.[97] This court was created specifically to hear *ex parte* government appeals of FISA applications that have been denied by the Foreign Intelligence Surveillance Court (there is no mechanism for hearing appeals of successful FISA applications). The government had never before filed an appeal with the Court of Review, however, as the Foreign Intelligence Surveillance Court has never denied a FISA application out of the thousands of applications it has reviewed.[98] On September 9, 2002, the Court of Review convened for the first time in its 24 year history to consider the Department of Justice's appeal in this case.

The Court of Review overruled the FISA court's decision on November 18, 2002.[99] The court determined that Congress had intended to relax the barriers between criminal law enforcement and foreign intelligence gathering when it passed the USA PATRIOT Act.[100] It held that the government could now lawfully use its extraordinary FISA powers in criminal investigations, so long as those investigations had some purpose of gathering foreign intelligence information. This was true even when the government's primary purpose was to prosecute a crime, provided that the crime, itself, was a "foreign intelligence crime" (such as espionage or terrorism).[101] Under such circumstances, according to the court, criminal law enforcement officials could now directly influence the initiation and operation of searches and surveillance under FISA.[102]

In so holding, the Court of Review did not accept all aspects of the administration's expansive interpretation of its new FISA powers. Although the court held that the government's primary purpose could now be the prosecution of a crime related to foreign intelligence,[103] it also held that "the FISA process cannot be used as a device to investigate wholly unrelated ordinary crimes."[104] The court also noted, however, that ordinary crimes would sometimes be inextricably intertwined with foreign intelligence crimes. In these intertwined cases, the government will now be able to use FISA and bypass traditional criminal law standards, provided that its investigation also serves some counterintelligence purpose.[105]

THE ADMINISTRATION'S NEW PROPOSALS FOR EXPANDING FISA

Not satisfied with the expansion of its FISA powers under the USA PATRIOT Act (as endorsed by the Court of Review), the Department of Justice has been drafting new proposals to further expand its FISA powers.[106] These measures, part of the draft PATRIOT II bill, would further weaken the already tenuous line separating counterintelligence operations from domestic criminal investigations.

One PATRIOT II proposal would significantly increase the scope of FISA by altering the definition of a "foreign power." Currently, a foreign power under FISA is either a foreign government or a foreign organization (ranging from a foreign political organization to a group engaged in international terrorism). Section 101 of the draft bill would expand the definition of a foreign power to cover individuals (including U.S. citizens and permanent residents) suspected of engaging in international terrorism, but who have no known links to any foreign government or to any group engaged in international terrorism. By including unaffiliated individuals within the definition of a "foreign power," the administration would weaken the already minimal due process protections applicable in FISA proceedings. Under the proposal, the administration could obtain a FISA warrant without even establishing that there is probable cause to believe that the target is an agent of a foreign power.[107]

Another proposal in the PATRIOT II draft bill would break down the current distinction under FISA between "U.S. persons" and "non-U.S. persons." As discussed above, in order to get a FISA warrant against a U.S. citizen or legal permanent resident, the administration currently has to show that the person is engaged in activities that "involve" or "may involve" some violation of law. For "non-U.S. persons," (i.e., those who are neither U.S. citizens nor legal permanent residents) however, the administration does not have to make any such showing. Section 102 of the draft bill would eliminate this distinction and apply the lower non-U.S. person standard to U.S. citizens and permanent residents.[108]

A third PATRIOT II proposal would expand the circumstances under which the government can sidestep the FISA courts altogether, using its FISA powers without any judicial review. The attorney general may currently authorize the use of FISA powers without a warrant, for example, for up to 15 days following a congressional declaration of war. Section 103 of the draft bill would expand the scope of the wartime exception, allowing it to be invoked after Congress authorizes the use of military force or after an attack on the United States "creating a national emergency." Presumably, the administration would

unilaterally decide when such an attack had occurred and whether it had created a period of national emergency.[109]

PRIVACY AND THE NEW HOMELAND SECURITY DEPARTMENT

As finally adopted, the Homeland Security Act enacted some important privacy protections, including a prohibition on the neighbor-to-neighbor spy initiative Operation TIPS and a ban on the development of a national ID card. The law also recognized the need for internal oversight by creating a Privacy Officer, a Civil Rights and Civil Liberties Officer, and an Inspector General in the Department of Homeland Security. In order to provide meaningful checks on Department action, however, these offices will need sufficient funding, and enhanced enforcement authority, as well as strong appointments. In particular, the Inspector General's office should have an official designated to receive complaints from the public regarding violations of civil rights.[110]

TOTAL INFORMATION AWARENESS (TIA)

The proposed Total Information Awareness Project (TIA), directed by retired Admiral John Poindexter at the Information Awareness Office (IAO) of the Defense Advanced Research Projects Agency (DARPA), is intended to allow the government to utilize data-mining to aggregate and analyze all public and private commercial database information to track potential terrorists and criminals.[111] The program aims to develop a comprehensive data profile of citizens and non-citizens alike, drawing on databases and public and private records of all kinds.[112] Many of the most intimate, personal details of the daily lives of all Americans would be subject to surveillance and cataloging by the federal government. As envisioned, TIA would enable the federal government to collect comprehensive personal data on ordinary people including driving records, high school transcripts, book purchases, medical records, phone conversations, e-mail, and logs of Internet searches.

The development of TIA began without public notice or a single congressional hearing. No oversight or accountability mechanisms were built into TIA or comparable data-mining efforts by the government. As the public began to learn about TIA and its designs, information about the program started to disappear from the official TIA website. Biographical information about the TIA development team appeared and then was removed from DARPA's Information Awareness Office website in November; next the TIA logo, a globe topped by an all-

seeing eye on a pyramid with the slogan, "Knowledge is Power," were removed from the site; and finally diagrams describing how TIA was to operate have been replaced by less detailed versions.[113]

Members of Congress from across the political spectrum expressed grave concerns about the program, including Senators Grassley (R-IA), Collins (R-ME), Feinstein (D-CA), Harkin (D-IA), Inouye (D-HI), Schumer (D-NY) and former Representatives Armey (R-TX), and Barr (R-GA). A broad range of groups including CATO, ACLU, the Free Congress Foundation, and the Eagle Forum have also raised questions about the privacy and constitutional implications of TIA. Former House Majority Leader Dick Armey (R-TX) commented that TIA is the "only thing that is scary to me."[114]

New Senate Governmental Affairs Committee Chairwoman Susan Collins (R-ME) also raised alarm regarding the danger that data-mining by the Department of Homeland Security poses to privacy, saying TIA presents "the specter of the government using massive databases to compile information on individuals [when] there are no allegations of wrongdoing," and "raises extraordinary concerns about individual privacy."[115] Senator Feinstein (D-CA) expressed strong reservations about TIA stating, "This is a panoply, which isn't carefully conscribed and controlled, for a George Orwell America. And I don't think the American people are ready for that by a long shot."[116]

Criticism of TIA was not limited to concerns about privacy. The program's lack of oversight was also a concern of many critics. *New York Times* Columnist William Safire wrote, "This is not some far-out Orwellian scenario. It is what will happen to your personal freedom in the next few weeks if John Poindexter gets the unprecedented power he seeks."[117] Senator Grassley (R-IA) expressed concerns about TIA funding, specifically the spending of Department of Defense resources on research for domestic law enforcement.[118]

In February 2003, Congress included in an omnibus spending bill a Senate-passed provision, sponsored by Senator Wyden (D-OR), that temporarily banned all funding for TIA until the program could be further explained and its impact on civil liberties assessed.[119] Under this provision, TIA will receive no funds until the Attorney General, Director of Central Intelligence and Secretary of Defense provide a detailed report to Congress, within 60 days of passage of the bill, on the use of TIA. The report requires: an assessment of TIA's impact on civil liberties and privacy; a detailed explanation of the use of funds; any technology transfer to other agencies; and a schedule for research and development.[120]

PROPOSALS TO TERMINATE RESTRICTIONS ON SPYING BY LOCAL POLICE

Last year, Attorney General Ashcroft unilaterally lifted restrictions on domestic spying by the FBI that had been put in place after revelations that the government had conducted oppressive surveillance on Martin Luther King, Jr. and other civil rights leaders deemed "subversive." Many egregious violations of civil rights and civil liberties occurred during the 1950s and 1960s at the hands of local police departments, including the New York City Police Department's Red Squad and the Bureau of Strategic Services (BOSS), which targeted individuals and groups for surveillance and harassment based on their political or religious beliefs and associations. Many state and local law enforcement agencies, some with disturbing histories of similar abuses, are party to court-supervised consent decrees arising out of legal challenges to these practices. These consent decrees prohibit illegal spying by police departments, and as such the Justice Department argues that they inhibit "effective cooperation" with the federal spying now permissible under the new Ashcroft guidelines.

The Domestic Security Enhancement Act of 2003 (Patriot II), the draft Justice Department legislative proposal, would address this problem by abolishing virtually all of these consent decrees and effectively preventing future consent decrees to oversee prohibitions on spying by local police forces.

Attorney General Ashcroft has said that the prohibitions against police spying are "a relic." Yet just last year it was revealed that the police department of Denver was spying on many local individuals and organizations, including nuns and advocates for Native Americans. The Denver police had secretly labeled organizations like the Quaker group, the American Friends Service Committee, "criminal extremist" organizations.[121] The *Portland Tribune* recently uncovered evidence of widespread police spying on "a food co-op, a bicycle repair collective, and a group that was setting up a shelter for abused women."[122]

Recently, New York City and Chicago have won legal battles to end consent decrees that prohibited their police from spying. But others question the efficacy of permitting police spying in the war against terrorism. Chicago authorities say the city police have yet to utilize the new spying powers and Los Angeles has not chosen to challenge its consent decree.[123]

CREATING A TERRORIST IDENTIFICATION DATABASE

Another proposal contained in the Justice Department's draft PATRIOT II bill with far-reaching implications for privacy rights is the creation of a "Terrorist Identification Database." This proposal would authorize the administration to collect the DNA of anyone considered a suspect and of any non-citizens deemed to have any form of association with a "terrorist organization."[124] Even those merely suspected of terrorist involvement would be required to submit DNA samples for inclusion in the database. One could be labeled a suspected terrorist for association of any kind with a group designated as a terrorist organization. Non-compliance with requirements to surrender samples to the DNA database would be a crime punishable by up to one year in prison and a $100,000 fine.[125]

Requiring individuals who have not been convicted of any crime to turn over their DNA, without a court order and without strict safeguards on data security is a particularly egregious invasion of privacy. Providing genetic information is far more invasive than a fingerprint, and provides personal information that is particularly subject to abuse by either government agencies or the private sector. DNA may, for example, disclose a pre-disposition to certain physical or mental illnesses.[126] Requiring genetic information is troubling because it invades the privacy of not just individuals but entire families and their descendants.[127] The DNA database provision of PATRIOT II would put information that comprises the very essence of personal identity into unregulated government control.

RECOMMENDATIONS

1. Congress should amend the Homeland Security Act to give the agency's Privacy and Civil Rights Officers full access to information, enforcement authority and resources.

2. Congress should amend the Homeland Security Act to establish a designated official within the Inspector General's office to receive complaints regarding specific violations of civil rights.

3. Congress should amend article 215 of the USA PATRIOT Act to restore safeguards against abuse of the seizure of business records, and in particular the records of libraries, bookstores, and educational institutions where seizure poses a particular risk of endangering freedom of expression.

Endnotes

[1] *A Year of Loss: Reexamining Civil Liberties since September 11* is available at: http://www.lchr.org/us_law/loss/loss_main.htm.

[2] John Adams, *A Dissertation on the Canon and Feudal Law* (1765), reprinted in 1 *Papers of John Adams* 120 (M.J. Kine ed., 1977).

[3] 5 U.S.C. §552 (1966).

[4] 5 U.S.C. Appendix 2.

[5] *See* Attorney General John Ashcroft, "Memorandum for Heads of All Federal Departments and Agencies," October 12, 2001, available at http://www.doi.gov/foia/foia.pdf (accessed March 2, 2003).

[6] *See* Attorney General Janet Reno, "Attorney General Reno's FOIA Memoranda," October 4, 1993, available at http://www.usdoj.gov/oip/foia_updates/Vol_XIV_3/page3.htm (accessed March 2, 2003).

[7] *See* Adam Clymer, "Government Openness at Issue as Bush Holds on to Records," *New York Times*, January 3, 2003.

[8] *See* The Homeland Security Act of 2002, available at http://news.findlaw.com/wp/docs/terrorism/hsa2002.pdf (accessed March 2, 2003).

[9] *See* ibid., at § 212(3).

[10] *See* "The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63," available at http://www.epic.org/reports/epic-cip.html (accessed February 2, 2003).

[11] *See* Dan Caterinicchia, "Sharing Seen as Critical for Security," *Federal Computer Week*, May 9, 2002.

[12] *See, e.g.*, "Protecting the Homeland by Exemption: Why the Critical Infrastructure Information Act of 2002 Will Degrade the Freedom of Information Act," 2002 *Duke Law and Technology Review* 0018, September 20, 2002, available at http://www.law.duke.edu/journals/dltr/articles/2002dltr0018.html (accessed March 2, 2003).

[13] *See* 5 U.S.C. § 552(b)(4).

[14] *See* 5 U.S.C. § 552(b)(1)(A).

[15] *See* 5 U.S.C. § 552(b)(7).

[16] H.R. Rep. No. 107-609, p. 220 (2002).

[17] Ibid.

[18] *See* "Editorial: Secrecy Isn't Security," *Denver Post*, November 3, 2002.

[19] Senator Carl Levin, "Statement of Senator Carl Levin (D-Mich.) on Confirming Governor Ridge as Department of Homeland Security Secretary," January 22, 2003, available at http://levin.senate.gov/floor/012203fs1.htm (accessed March 3, 2003).

[20] Ibid.

[21] Ibid; Homeland Security Act of 2002, § 214(f).

[22] Homeland Security Act of 2002, § 214(a)(1)(C).

[23] *See* Center for Democracy and Technology, "Coalition Letter Opposing Bennett-Kyl Legislation (S. 1456) Creating FOIA Exemption for Information on Critical Infrastructure Security," May 7, 2002, available at http://www.cdt.org/security/critinfra/020507coalition.shtml (accessed March 3, 2003); Matt Bivens, "Holes in the Homeland Security Act," *Nation*, December 19, 2002, available at http://www.thenation.com/failsafe/index.mhtml?bid=2&pid=229 (accessed March 3, 2003).

[24] *See* "Too Many Secrets," *Orlando Sentinel Tribune*, January 10, 2003; David Banisar, "Reject the Corporate Secrecy Grab: Industry's Push for New Exemptions from the Freedom of Information Act is Unnecessary and Dangerous," *Security Focus*, January 28, 2002, available at http://online.securityfocus.com/columnists/56 (accessed February 5, 2003).

[25] *See* Reporters Committee for the Freedom of the Press, "Committee Warns of Severe Restrictions in Homeland Security Bill," November 19, 2002.

[26] *See* "Homeland Insecurity: Excessive Secrecy Protects No-one," *Columbia Journalism Review*, January/ February 2003.

[27] *See* The Homeland Security Act of 2002, § 871.

[28] *See* 5 U.S.C. App. 2 (1972).

[29] *See* H.R. Rep. No. 107-609, p. 221 (2002).

[30] *See* Ibid. (Noting that many agencies with homeland security missions, such as the DOJ and the FBI, operate under FACA without difficulty).

[31] *See* John W. Dean, "GAO v. Cheney Is Big Time Stalling: The Vice President Can Win Only If We Have Another *Bush v. Gore*-like Ruling," Part II, *FindLaw's Legal Commentary*, February 1, 2002, available at http://writ.news.findlaw.com/dean/20020201.html (accessed March 2, 2003).

[32] *See* Dana Milbank and Ellen Nakashima, "Cheney Rebuffs GAO's Records Request," *Washington Post*, August 4, 2001.

[33] *See* Byron York, "GAO vs. Cheney: Coming Soon," *National Review*, February 20, 2002, available at http://www.nationalreview.com/york/york022002.shtml (accessed February 2, 2003).

[34] *See* Paul Courson, "GAO Files Unprecedented Suit Against Cheney," CNN News, February 22, 2002.

[35] *See* Dana Milbank and Ellen Nakashima, "Cheney Rebuffs GAO's Records Request," *Washington Post*, August 4, 2001.

[36] *See* Marcia Coyle, "GAO is Hit with Setback to Power," *National Law Journal*, December 16, 2002.

[37] *See* Stuart Taylor, Jr., "A Victory Gone Too Far, *Legal Times*, December 16, 2002.

[38] General Accounting Office, "GAO Statement Concerning Litigation," February 22, 2002, available at http://www.gao.gov/press/gaostatement0222.pdf (accessed March 2, 2003).

[39] *See* "Biography of Judge John D. Bates," available at http://www.dcd.uscourts.gov/bates-bio.html (accessed March 2, 2003).

[40] *See Walker v. Cheney*, Civil Action No. 02-0340 (JDB), U.S. District Court for the District of Columbia, available at http://www.dcd.uscourts.gov/02-340.pdf (accessed March 2, 2003).

[41] *See* Stuart Taylor, Jr., "A Victory Gone Too Far, *Legal Times*, December 16, 2002.

[42] *See* Dana Milbank, "GAO Backs Off Cheney Lawsuit," *Washington Post*, February 7, 2003.

[43] *See* United States General Accounting Office, "GAO Press Statement on Walker v. Cheney," February 7, 2003, available at http://www.gao.gov/press/w020703.pdf (accessed March 2, 2003).

[44] Ibid.

[45] *See* "President Signs Anti-Terrorism Bill," While House Press Release, October 26, 2002, available at http://www.whitehouse.gov/news/releases/2001/10/20011026-5.html (accessed March 2, 2003).

[46] *See* Lawyers Committee for Human Rights, *A Year of Loss: Re-examining Civil Liberties since September 11*, pp.7-8, available at http://www.lchr.org/us_law/loss/loss_main.htm (accessed March 2, 2003).

[47] Ibid.

[48] *See* Steve Schultze, "Sensenbrenner Wants Answers on Act," *Journal Sentinel*, August 19, 2002; "Justice: From the Ashes of 9/11: Big Bad John," *National Journal*, January 25, 2003.

[49] Letter of Daniel J. Bryant, Assistant Attorney General, to the Honorable F. James Sensenbrenner, Jr., July 26, 2002, enclosing "Questions Submitted by the House Judiciary Committee to the Attorney General on USA PATRIOT Act Implementation," available on http://www.house.gov/judiciary/patriotresponses101702.pdf (accessed February 20, 2003).

[50] Senators Patrick Leahy, Charles Grassley, and Arlen Specter, "Interim Report: FBI Oversight in the 107th Congress by the Senate Judiciary Committee: FISA Implementation Failures," p. 13, February 2003, available at http://specter.senate.gov/files/specterspeaks/ACF6.pdf (accessed March 5, 2003).

[51] Ibid.

[52] *See* "ACLU Seeks Information on Government's Use of Vast New Surveillance Powers," August 21, 2002, available at http://archive.aclu.org/issues/privacy/USAPA_feature.html (accessed March 2, 2003).

[53] *See* ACLU, "ACLU Presses for Full Disclosure on Government's New Snoop Powers," January 17, 2003, available at http://www.aclu.org/NationalSecurity/NationalSecuritylist.cfm?c=107 (accessed March 2, 2003).

[54] *See* "Groups Hit DOJ's Data on Wiretap FOIA Request as 'Meaningless,'" *Washington Internet Daily*, January 21, 2003.

[55] Letter to David M. Walker, Comptroller General of the U.S., U.S. General Accounting Office, from U.S. House Representative John Conyers, Jr. and U.S. Senator Russell D. Feingold, dated January 28, 2002, available at http://www.house.gov/judiciary_democrats/gaoantiterrorltr12802.pdf (accessed December 10, 2002).

[56] *See* Draft Domestic Security Enhancement Act of 2003, January 9, 2003, available at http://www.publicintegrity.org/dtaweb/downloads/Story_01_020703_Doc_1.pdf (accessed March 2, 2003).

[57] *See* Jake Tapper, "More Secret Arrests, More Power to Spy," *Salon*, February 11, 2003.

[58] Ibid.

[59] Ibid.

[60] Ibid.

[61] *See, e.g.*, Ibid.; Jack Balkin, "A Dreadful Act II: Secret Proposals in Ashcroft's Anti-Terror War Strike Yet Another Blow at Fundamental Rights," *Los Angeles Times*, February 13, 2003.

[62] Jesse H. Holland, "Ashcroft, Mueller, Ridge Talk to Senate Committee about Terrorism Battle," Associated Press, March 4, 2003.

[63] Ibid.

[64] U.S. Supreme Court, *Afroyim v. Rusk*, 387 U.S. 253 (1967), BLACK, J., Opinion of the Court.

[65] Senate Judiciary Committee, Hearing on the War against Terrorism, March 4, 2003, testimony of U.S. Attorney General John Ashcroft, Homeland Security Secretary Tom Ridge, and Federal Bureau Of Investigation Director Robert Mueller, Federal News Service, March 4, 2003.

[66] Under current law, it is up to the judge to determine how much of the government's application to consider *in camera* and *ex parte*. *See* Timothy Edgar, "Interested Persons Memo: Section-by-Section Analysis of Justice Department draft 'Domestic Security Enhancement Act of 2003,' February 14, 2003, p. 10, available at http://www.aclu.org/news/NewsPrint.cfm?ID=11835&c=206 (accessed March 10, 2003).

[67] Ibid. Rule 6(e) of the Federal Rules of Criminal Procedure requires attorneys and grand jurors to refrain from publicly commenting on "matters occurring before the grand jury." The current rule does not apply to grand jury witnesses.

[68] *See* Chuck Grassley, "Grassley Seeks Whistleblower Protections for New Federal Employees Senator Says Public Safety and Security at Stake," Press Release, June 26, 2002, available at http://www.senate.gov/~grassley/releases/2002/p02r6-26b.htm (accessed January 19, 2003).

[69] Ibid.

[70] Senators Patrick Leahy, Charles Grassley, and Arlen Specter, "Interim Report: FBI Oversight in the 107th Congress by the Senate Judiciary Committee: FISA Implementation Failures," pp. 5-6, February 2003, available at http://specter.senate.gov/files/specterspeaks/ACF6.pdf (accessed March 5, 2003).

[71] Ibid., p. 32.

[72] Ibid.

[73] Ibid., p. 1.

[74] *United States v. Martinez-Fuerte*, 428 U.S. 543, 554 (1976).

[75] *Olmstead v. United States,* 277 U.S. 438, 478 (1928) (Brandeis, J. dissenting).

[76] John Ashcroft, "Welcoming Big Brother," *Washington Times*, August 12, 1997. Mr. Ashcroft wrote this op-ed as a U.S. senator, in response to a request by the Clinton administration for increased authority to survey high-tech communications.

[77] Electronic Privacy Information Center, EPIC Briefing on Total Information Awareness, available at http://www.epic.org/events/tia_briefing/ (accessed December 9, 2002).

[78] The American Library Association puts this simply on its website: "Libraries or librarians served with a search warrant issued under FISA rules may not disclose, under of penalty of law, the existence of the warrant or the fact that records were produced as a result of the warrant. A patron cannot be told that his or her records were given to the FBI or that he or she is the subject of an FBI investigation." Available at http://www.ala.org/alaorg/oif/usapatriotlibrary.html (accessed February 20, 2003).

[79] "Questions Submitted by the House Judiciary Committee to the Attorney General on USA PATRIOT Act Implementation," submitted with letter of Daniel J. Bryant, Assistant Attorney General, to the Honorable F. James Sensenbrenner, Jr., July 26, 2002, question 12, available at http://www.house.gov/judiciary/patriotresponses101702.pdf (accessed February 20, 2003).

[80] Dana Hull, "Libraries Face Privacy Test," *Mercury News*, October 18, 2002; Eleanor J. Bader, "Thought Police: Big Brother May be Watching What You Read," *In These Times*, October 25, 2002.

[81] Special Libraries Association, Press Release, January 9, 2003, "Report on the USA Patriot Act Videoconference," available at http://www.sla.org/content/memberservice/communication/pr/pressrelease/2303.cfm (accessed February 20, 2003).

[82] American Booksellers Federation for Free Expression, "ABFFE Sues Justice Department for Data on Patriot Act Subpoenas," available on http://www.abffe.com/. The full text of the lawsuit is available at http://www.epic.org/privacy/terrorism/patriot_foia_complaint.pdf (accessed February 24, 2003). The American Civil Liberties Union (ACLU) and the Electronic Privacy Information Center (EPIC) were also parties to the suit.

[83] "We're just a small business trying to make a living, and I do not relish the idea of standing up against the F.B.I.," said Ken Kurtis, one of the owners of Reef Seekers. "But I think somebody's got to do it." Michael Moss and Ford Fessenden, "New Tools for Domestic Spying, and Qualms," *New York Times*, December 10, 2002.

[84] Ibid.

[85] *See* 50 U.S.C. § 1801-1811, 1821-1829, 1841-1846, 1861-62.

[86] *See, e.g.*, Senators Patrick Leahy, Charles Grassley, and Arlen Spector, "Interim Report: FBI Oversight in the 107th Congress by the Senate Judiciary Committee: FISA Implementation Failures," p. 5, February 2003, available at http://specter.senate.gov/files/specterspeaks/ACF6.pdf (accessed March 5, 2003).

[87] In determining whether there is probable cause to issue a traditional criminal warrant, the issuing judge makes "a practical common-sense decision whether, given all the circumstances set forth in the affidavit before him, including the 'veracity' and 'basis of knowledge' of persons supplying hearsay information, there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates*, 462 U.S. 213, 238 (1983).

[88] *See In Re All Matters Submitted to the Foreign Intelligence Surveillance Court*, U.S. Foreign Intelligence Surveillance Court, May 17, 2002, p. 5, available at http://www.fas.org/irp/agency/doj/fisa/fisc051702.html (accessed March 4, 2003).

[89] *See In Re Sealed Case No. 02-001*, U.S. Foreign Intelligence Surveillance Court of Review, November 18, 2002, p. 34, available at http://www.cadc.uscourts.gov/common/newsroom/02-001.pdf. *See also* David Cole, "Secret Court Takes the Fourth," *CounterPunch*, November 22, 2002 (noting that FISA does not require probable cause of a crime), available at http://www.counterpunch.org/cole1122.html (accessed March 5, 2003).

[90] Anita Ramasastry, "The Foreign Intelligence Surveillance Court of Review Creates a Potential End Run Around Traditional Fourth Amendment Protections for Certain Criminal Law Enforcement Wiretaps," *FindLaw Legal Commentary*, November 26, 2002, available at http://writ.news.findlaw.com/ramasastry/20021126.html (accessed March 5, 2003).

[91] For a discussion of the FBI's powers under FISA, see *In Re All Matters Submitted to the Foreign Intelligence Surveillance Court*, U.S. Foreign Intelligence Surveillance Court, May 17, 2002, pp. 5-6.

[92] Ibid., p. 9.

[93] *See, e.g.*, Anita Ramasastry, "Why the Foreign Intelligence Surveillance Act Court Was Correct to Rebuke the Department of Justice," *FindLaw Legal Commentary,* September 4, 2002, available at http://writ.news.findlaw.com/ramasastry/20020904.html (accessed March 3, 2003).

[94] *See In Re All Matters Submitted to the Foreign Intelligence Surveillance Court*, U.S. Foreign Intelligence Surveillance Court, May 17, 2002.

[95] Section 208 of the USA Patriot Act called for the appointment of 11 federal judges to the Foreign Intelligence Surveillance Court. At the time the decision was issued, however, only seven federal judges sat on the court: (1) Honorable Royce C. Lamberth; (2) Honorable William H. Stafford, Jr.; (3) Honorable Stanley S. Brotman; (4) Honorable Harold A. Baker; (5) Honorable Michael J. Davis; (6) Honorable Claude M. Hilton; and (7) Honorable Nathaniel M. Gorton.

[96] *See In Re All Matters Submitted to the Foreign Intelligence Surveillance Court*, U.S. Foreign Intelligence Surveillance Court, May 17, 2002, p. 14.

[97] The judges on the Foreign Intelligence Surveillance Court of Review are: (1) Honorable Ralph Guy; (2) Honorable Edward Leavy; and (3) Honorable Laurence Silberman.

[98] *See* David Cole, "Secret Court Takes the Fourth," November 22, 2002, available at http://www.counterpunch.org/cole1122.html (accessed March 4, 2003).

[99] See *In Re Sealed Case No. 02-001*, U.S. Foreign Intelligence Surveillance Court of Review, November 18, 2002, available at http://www.cadc.uscourts.gov/common/newsroom/02-001.pdf (accessed March 5, 2003).

[100] *See* Ibid., pp. 24-27.

[101] *See* Ibid., pp. 28-30.

[102] *See, e.g.,* Ramasastry, "The Foreign Intelligence Surveillance Court of Review," *FindLaw Legal Commentary*, November 26, 2002, (explaining that criminal law enforcement can now "legally direct, or at least heavily influence, FBI investigations related to foreign intelligence").

[103] *See In Re Sealed Case No. 02-001*, U.S. Foreign Intelligence Surveillance Court of Review., pp. 29-30.

[104] Ibid., p. 30. *See also* Charles Lane, "In Terror War, 2nd Track for Suspects," *Washington Post*, December 1, 2002.

[105] *See In Re Sealed Case No. 02-001*, U.S. Foreign Intelligence Surveillance Court of Review., pp. 28-30.

[106] *See* Draft Domestic Security Enhancement Act of 2003, January 9, 2003, available at http://www.pulicintegrity.org/dtaweb/downloads/Story_01_020703_Doc_1.pdf (accessed March 5, 2003).

[107] *See, e.g.*, Timothy Edgar, "Interested Persons Memo: Section-by-Section Analysis of Justice Department draft 'Domestic Security Enhancement Act of 2003,' February 14, 2003, p. 4, available at http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=11835&c=206 (accessed March 5, 3003).

[108] Ibid.

[109] Ibid.

[110] Human Rights Watch Press Release, "U.S. Homeland Security Bill, Civil Rights Vulnerable and Immigrant Children Not Protected," November 21, 2002, available at http://www.hrw.org/press /2002/11/homeland1211.htm (accessed December 10, 2002).

[111] Electronic Privacy Information Center, Total Information Awareness (TIA), available at http://www.epic.org/privacy/profiling/tia/ (accessed December 3, 2002).

[112] Electronic Privacy Information Center, EPIC Briefing on Total Information Awareness, available at http://www.epic.org/events/tia_briefing/ (accessed December 9, 2002).

[113] Declan McCullagh, Federal Database Spy Site Slipping Away, *Cnet*, December 20, 2002, available at http://news.com.com/2100-1023-978598.html (accessed February 5, 2003).

[114] Michelle Mittelstadt, Excess of Access for Feds?, *Dallas Morning News*, December 15, 2002, available at http://www.dallasnews.com/dmn/news/stories/121502dnnatsnooping.b2ea3.html (accessed January 8, 2003).

[115] William New, "New Senate Chair Voices Concerns on Information Sharing," *National Journal's Technology Daily*, available at http://www.govexec.com/dailyfed/0103/101003td2.htm (accessed January 13, 2003).

[116] Jim Puzzanghera, "Massive Database Dragnet Explored," *San Jose Mercury News*, November 20, 2002, available at http://www.siliconvalley.com/mld/siliconvalley/4569587.htm (accessed January 8, 2002).

[117] William Safire, "You Are A Suspect," *New York Times,* November 14, 2002, available at http://www.nytimes.com/2002/11/14/opinion/14SAFI.html (accessed January 10, 2002).

[118] Associated Press, "Grassley Wants Review of Database," *Washington Times,* November 24, 2002, available at http://www.washtimes.com/national/20021124-77963510.htm. (accessed December 10, 2002).

[119] Susan Cornwell, Senate Blocks Funding for Pentagon Database, *Washington Post,* January 23, 2003, available at http://www.washingtonpost.com/wp-dyn/articles/A34837-2003Jan23.html (accessed January 27, 2003).

[120] Senator Ron Wyden Press Release, "Wyden Wins Passage of Legislation To Curb Plan to Spy on American Citizens," January 23, 2003, available at http://www.senate.gov/~wyden/media/2002/2003123C23.html (accessed February 10, 2003).

[121] ACLU of Colorado Press Release, ACLU Calls for Denver Police to Stop Keeping Files on Peaceful Protesters, March 11, 2002, available at http://www.aclu-co.org/news/pressrelease/release_spyfiles.htm (accessed February 25, 2003).

[122] Dean Schabner, Big Brother Comeback? *ABC News*, January 02, 2003, http://abcnews.go.com/sections/us/DailyNews/police_spying030102.html (accessed February 25, 2003).

[123] Michael Moss and Ford Fessenden, AMERICA UNDER SURVEILLANCE: Privacy and Security; New Tools for Domestic Spying, and Qualms, *New York Times,* December 10, 2002, available at http://query.nytimes.com/search/article-printpage.html?res=9D05E4DF173AF933A25751C1A9649C8B63 (accessed February 25, 2003).

[124] Anita Ramasastry, "Patriot II: The Sequel Why It's Even Scarier than the First Patriot Act," *Findlaw* February 17, 2003, http://writ.news.findlaw.com/ramasastry/20030217.html (accessed February 25, 2003).

[125] Ibid.

[126] Timothy Edgar, "Interested Persons Memo: Section-by-Section Analysis of Justice Department draft 'Domestic Security Enhancement Act of 2003,' also known as 'PATRIOT Act II'", *ACLU*, February 14, 2003, http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=11835&c=206 (accessed February 25, 2003).

[127] Ibid.

[128] Robert McMahon, "U.N.: Humanitarian Group Awards Karzai, Presses U.S. On Refugee Policy," Radio Free Europe/Radio Liberty, Press Release, available at http://www.rferl.org/nca/features/2002/11/14112002172346.asp (accessed March 6, 2003).