Before al Qaeda, before the CIA or even the National Security Agency (NSA), there was Operation Shamrock. In the late summer of 1945, while radioactive dust was still drifting off the cities of Nagasaki and Hiroshima, the U.S. Army’s Signal Security Service approached the heads of America’s major communications companies with a request it claimed no patriot could refuse. The companies didn’t refuse.

At the time, telegrams were sent by punching holes in long strips of paper tape and scanning that tape. At the end of every day, a government agent would appear at each company and take away a copy of the paper roll with all the day’s communications recorded on it. Thus, for more than thirty years, until 1975, the federal government secretly collected every international telegram sent to and received by every American, in one of the most sweeping surveillance operations in U.S. history.

All this was done without the sanction of a federal statute or the oversight of any official Congressional committee.

Electronic surveillance programs such as Operation Shamrock, implemented in secrecy without debate or legal authority, serve as a cautionary tale on how such surveillance programs impinge on the principles underpinning our democracy.

The New Era of Executive Unilateralism and Electronic Surveillance

In the past year, Americans learned of several new and vast electronic surveillance programs started in the wake of September 11, 2001. Dipping into the ocean of e-mails, telephone calls and financial transactions produced every day by millions of American citizens, these programs collect traces left by anyone who makes a phone call, sends an e-mail, takes money from an ATM or pays a bill.

Like Shamrock, these new surveillance programs lack any sanction in federal statute. Instead, they are wholly the product of unilateral executive branch action. President George W. Bush himself authorized these programs, and the Administration, acting in secret and without the benefit of Congressional debate or legislation, successfully avoided both clear constraints on its spying and the protection of independent oversight.

No one doubts the magnitude of the threat posed by al Qaeda and its allies. No one doubts the need for electronic surveillance of terrorist suspects’ communications and financial transactions. In the new era of surveillance we doubtless confront quite difficult questions.

But should we make difficult policy decisions involving a balance of liberty and security in the absence of congressional or public oversight and outside the framework of the rule of law? Was the President right to authorize law-breaking programs? Have their costs to constitutional liberties been balanced by security gains? What
Frank Church, conducted an unrelenting inquiry into the Cold War activities of the intelligence agencies.

Canvassing the NSA, CIA and FBI, the Church Committee documented pervasive overreach and abuse. It found an intelligence apparatus trained not on the Soviet threat, but on innocent Americans. The result—damaged lives, ruined reputations and warped national decision-making. Thanks to the Church Committee, Congress in 1978 enacted the Foreign Intelligence Surveillance Act (FISA). FISA required that all electronic surveillance be conducted under authority of a statute, clearly rejecting executive unilateralism. It also fashioned a carefully tailored judicial process for search warrants in cases involving foreign intelligence surveillance.

**Recent Surveillance Programs Have Violated Citizens’ Rights**

At least two newly revealed surveillance programs run by the NSA, and revealed by journalists at the *New York Times* and *USA Today*, suggest that the executive branch’s unilateral surveillance activities risk harm to democratic principles without large benefit to national security. (A third program, involving the harvesting of financial data from an overseas banking cooperative called SWIFT, appears to have hewed to law and contains stringent independent auditing to prevent abuse; it raises few, if any, democratic-related concerns.)

The first program began soon after the terrorist attacks of 9/11. In early 2002, the CIA captured an al Qaeda member named Abu Zubaydah in Pakistan. Along with Zubaydah, the CIA brought in a trove of telephone numbers and names embedded in captured computers and cell phones, a catch promptly given to the NSA.

Inexorably, the NSA spiraled its web of surveillance outward from the initial numbers, eventually conducting surveillance of thousands of people overseas and hundreds of people within the U.S. The unavoidsable consequence of this method of “link analysis” was government surveillance of individuals who had no connection at all to terrorism, or, at best, a tenuous connection. For example, journalists or scholars doing research on Afghanistan or Iraq fell easily into this NSA surveillance web as did everyone the journalist or scholar contacted.

Like the NSA’s Cold War watch-lists, post-9/11 surveillance engendered political abuses. In confirmation hearings for Ambassador to the United Nations John Bolton, Senators learned that Bolton, while Under Secretary at the State Department, asked for and received NSA intercepts of communications between Americans and foreigners. Although the NSA expunged Americans’ names, Bolton asked for—and got—the names reinserted. Bolton was not alone in this practice. According to *Newsweek*, the NSA has handed over the names of about 10,000 citizens to government officials in this fashion. As in the Cold War, surveillance conducted without legal guidelines and independent oversight has resulted in the invasion of American citizens’ privacy by their own government.

In addition to its link-analysis effort, the NSA operated a dragnet of Americans’ electronic communications with eerie echoes of Operation Shamrock. As in 1945, the NSA approached telecom companies and sought access to the telecommunications network through which most e-mail and telephone traffic flows. Again, the NSA secured unrestricted access from at least some companies. This enabled the Agency to gather data about all calls going through these networks. *USA Today* reports that the NSA does not access the content of communications, but gathers only “external” information about the origin, destination and timing of communications. However, this information can be cross-referenced with a host of other federal databases and data-mining efforts to yield more personal information.
This dragnet program also apparently violated the Stored Communications Act. This federal Act prevents companies from giving data to the government without a lawful warrant. In asking companies to hand over even external data without the proper warrants, the NSA incited these companies to violate this law.

The Administration fiercely argues that these NSA efforts furthered counter-terrorism goals. But these broad link-analysis and dragnet approaches may have actually impeded counter-terrorism efforts. Immediately after 9/11, the NSA inundated the FBI with a flood of its unfiltered intercepts. The result? Bureau agents wasted countless man-hours on dead ends and frivolous leads.

The Administration has never plausibly explained why it could not go to Congress to get additional surveillance authority, as FISA envisaged. Attorney General Alberto Gonzales argues that the surveillance could not be revealed without undermining its intelligence value. This argument carries little weight in the face of proof that intelligence conducted without accountability results in unfocused counter-terrorism efforts and wasted resources. Perhaps more disturbing is the fact that the Administration has insisted that it will continue the new surveillance despite its public revelation.

The Role of Congress
Despite the Administration’s reticence about the facts, it is clear that the NSA’s spying violates both FISA and, in some instances, the Fourth Amendment of the Constitution, which prohibits unreasonable searches and seizures, and imposes a warrant requirement. Congress wrote FISA to make it clear that all electronic surveillance had to take place under the aegis of a federal statute.

FISA places only a minimal burden on the government when it seeks a warrant. FISA covers only citizens and green card holders; the 9/11 hijackers could have been watched without any warrant. Congress also included an emergency provision allowing surveillance to continue for 72 hours before a warrant is secured. In cases of war, Congress added a two-week carve-out, giving the executive branch time to return to Congress and seek new spying powers. Despite this flexibility, the Administration has repeatedly bypassed statutory mechanisms, flouting FISA’s prohibition on surveillance without a warrant.

In response to reports of illegal NSA activities, civil liberties groups filed lawsuits in New York and Michigan seeking termination of the surveillance programs. In contrast, Congress lagged in holding hearings that ultimately furnished little illumination.

Several members of Congress have proposed legislation for the NSA’s post-9/11 spying. Troublingly, several legislative proposals, including that of Senate Judiciary Chair Arlen Specter, contain what seemed to be unchecked license for spying with no oversight. These legislators have failed to heed the warning of the 9/11 Commission that “there is adequate supervision of the executive’s use of the powers to ensure protection of civil liberties.” They have also ignored reports from Congress’s own General Accounting Office that data-mining projects across the federal government tend to have flawed privacy protections. There is little cause for confidence that the executive branch, left to its own devices, will act responsibly.

More importantly, Congress has paid little attention to a fundamental issue: How could unlawful intelligence activities have escaped scrutiny for more than four years from the

Oversight and institutional balance yield more focused, more effective intelligence.

Aziz Huq directs the Liberty & National Security Project at the Brennan Center for Justice, NYU School of Law. He is a 2006 Carnegie Scholars Fellow and is co-author of “Unchecked and Unbalanced: Presidential Power in a Time of Terror,” to be published in March 2007 by the New Press.

VOTER LINKS
www.brennancenter.org