AMERICA'S SURVEILLANCE SOCIETY

Mass surveillance has become one of the U.S. government's principal strategies for protecting national security. Over the past seven years, the government has asserted sweeping power to conduct dragnet collection and analysis of innocent Americans' telephone calls and e-mails, web browsing records, financial records, credit reports, and library records. The government has also asserted expansive authority to monitor Americans' peaceful political and religious activities.

The government's surveillance activities are not directed solely at suspected terrorists and criminals. They are directed at all of us. Increasingly, the government is engaged in suspicionless surveillance that vacuums up sensitive information about innocent people. And this surveillance takes place in secret, with little or no oversight by the courts, by Congress, or by the public.

Using their power to collect massive amounts of private communications and data, agencies like the Federal Bureau of Investigation (FBI) and the National Security Agency (NSA) apply computer programs to draw links and make predictions about people's behavior. Tracking people two, three, four steps removed from the original surveillance target, they build "communities of interest" and construct maps of our associations and activities. With this sensitive data, the government can compile vast dossiers about innocent people. The data sits indefinitely in government databases, and the names of many innocent Americans end up on bloated and inaccurate watch lists that affect whether we can fly on commercial airlines, whether we can renew our passports, whether we are called aside for "secondary screening" at airports and borders, and even whether we can open bank accounts.

Dragnet surveillance undermines the right to privacy and the freedoms of speech, association, and religion.

The list of new surveillance programs and authorities is long—too long to provide here. But among the tools that the government has used to collect information about innocent Americans are:

THE USA PATRIOT ACT OF 2001

The USA Patriot Act dramatically expanded the FBI's power to conduct surveillance inside the United States. It expanded the FBI's authority to install wiretaps without criminal probable cause, provided statutory authority for so-called "sneak-and-peak" searches, and extended the FBI's power to issue "national security letters" (NSLs). The FBI uses NSLs to compel Internet service providers, libraries, banks, and credit reporting companies to turn over sensitive information about their customers and patrons. Because NSLs can be issued without prior court approval and without probable cause, the FBI issues tens of thousands of NSLs every year. And it routinely imposes "gag" orders that prohibit NSL recipients from disclosing even the mere fact that the FBI approached them for information.

• Between 2003 and 2006, the FBI issued almost 200,000 national security letters. Only one led to a terrorism conviction.

THE NSA'S WARRANTLESS WIRETAPPING PROGRAM

In 2005, President Bush acknowledged that he had secretly authorized the NSA to conduct warrantless surveillance of Americans' international telephone calls and e-mails. The NSA's program, which operated in clear violation of both the Foreign Intelligence Surveillance Act (FISA) and the Constitution, allowed the government, with the assistance of major telecommunications companies, to gain direct access to the nation's telecommunications infrastructure.

• In 2008 the NSA's spying budget was $47.5 billion.

THE FISA AMENDMENTS ACT OF 2008

Two judges considered the legality of the NSA's warrantless wiretapping program; both found that the program violated FISA. The Bush administration therefore pressured Congress to amend FISA, and in July 2008 Congress obliged by enacting the FISA Amendments Act of 2008. The Act gave the NSA virtually unchecked power to conduct warrantless, dragnet collection of Americans' international communications. The law also granted sweeping immunity to the telecommunication companies that facilitated the NSA's warrantless wiretapping program.

PROGRAMS THAT TRACK LAWFUL POLITICAL ACTIVITY

In connection with its "Threat and Local Observation Notice" (TALON) database, the Pentagon monitored at least 186 anti-military protests in the United States. The Pentagon also generated reports about lawful political activity by groups such as Veterans for Peace and the War Resisters League, which advocate nonviolence. The FBI has similarly focused on peaceful political activity, monitoring the lawful activities of organizations including the American Friends Service Committee, the American-Arab Anti-Discrimination Committee, Students for Peace and Justice, Greenpeace, and PETA. In some cases the FBI even sent federal agents to infiltrate the organizations.

PERVASIVE VIDEO SURVEILLANCE

An increasing number of American cities and towns have spent taxpayer dollars to create elaborate camera and video surveillance systems designed to monitor public places such as parks, plazas, and sidewalks. Governments are also accessing images collected by privately-owned camera and video systems. With an extensive network of surveillance cameras, the government can indiscriminately track everyone's movements and activity, without any suspicion of wrongdoing. There is nothing to stop government officials from using the cameras for inappropriate purposes such as tracking people for their own entertainment, monitoring political protests, or targeting racial or religious minorities.

While the government's surveillance powers have expanded dramatically, regulation and oversight has been watered down rather than strengthened. The government has more information, but the limitations on how the information can be used are fewer and weaker.

DATA MINING

Data mining is the process of sorting through massive amounts of information in order to detect patterns and aberrations. In order to mine data, the government needs to create huge databases of information—databases that include information not only about suspected terrorists but about innocent people as well. The theory that underlies the databases is the theory that nonconformity is suspicious, which is a theory that is dangerous in itself. But the databases are made more problematic because they contain thousands of errors—errors that can ultimately affect whether a person can board a commercial airline, renew her passport, cross the border without secondary screening, and open a bank account. There are no meaningful restrictions on the government's data mining activities.

FUSION CENTERS

Fusion centers were originally created as hubs to improve the sharing of anti-terrorism intelligence between state, local, and federal law enforcement agencies.Today, these centers are shrouded in secrecy and operate without any legal framework or oversight. With a vague and expansive mission to collect information about all crimes and hazards, fusion centers house law enforcement, intelligence, and private sector data that is shared not only with law enforcement but with the military and some private companies.

CASE STUDY: National Security Letters

In 2005, the FBI used a National Security Letter to demand library patron records from Library Connection, a consortium of 26 libraries in Connecticut. The FBI imposed a gag order on the librarians and as a result they were prohibited from speaking to Congress during the debate about the reauthorization of the Patriot Act. Bizarrely, the FBI continued to enforce the gag order even after *The New York Times* revealed Library's Connection's identity. With the assistance of the ACLU, Library Connection filed suit to challenge the constitutionality of the gag order. The librarians prevailed and the FBI ultimately withdrew both the gag order and the underlying demand for library patron records.

CASE STUDY: Monitoring Political Activity

A lawsuit by the ACLU of Maryland recently exposed a Maryland State Police (MSP) spying operation targeted at lawful protect activity. Under the guise of investigating terrorist threats, the MSP assigned covert agents to infiltrate local anti-war and anti-death penalty groups. As a result of the monitoring, the MSP placed 53 peaceful activists in official terrorism-related databases, including two Catholic nuns, members of the Maryland Campaign to End the Death Penalty and the Baltimore Coalition Against the Death Penalty, and a Democratic candidate for local political office. The ACLU of Maryland is assisting the protesters and calling for legislation to prohibit a recurrence of the abuses.

CASE STUDY: Warrantless Wiretapping

In October 2008, two government whistleblowers revealed to ABC News that NSA spying programs supposedly directed at suspected terrorists were in fact used to monitor the private communications of innocent Americans abroad, including journalists, U.S. soldiers, and aid workers from groups such as the International Red Cross and Doctors Without Borders. According to the whistleblowers, NSA personnel regularly passed around salacious calls, such as the private "phone sex" calls of soldiers calling home. The ACLU has filed a Freedom of Information Act request to find out whether the privacy rights of Americans are adequately protected by the NSA's policies.

Dragnet monitoring of innocent people does not make us safer

Many experts believe that dragnet surveillance is ineffective as a means of identifying would-be terrorists. Mass surveillance programs that are not based on suspicion waste time and resources, creating bigger mountains of information that law enforcement and intelligence officials must sift through in order to find true threats.

It's a mistake to think that we can make ourselves safer by sacrificing our right to privacy. The Fourth Amendment's prohibition against suspicionless searches protects privacy, but it also makes government more effective. It channels our limited investigative resources away from innocent people and towards actual threats.

We should certainly never trade liberty for the *mere appearance* of security.

"Predictive data mining is not well suited to the terrorist discovery problem" and it "waste[s] taxpayer dollars, needlessly infringe[s] on privacy and civil liberties, and misdirect[s] the valuable time and energy of the men and women in the national security community."

—Cato Institute Policy Analysis, December 2006[3]

"We'd chase a number, find it's a school teacher with no indication they've ever been involved in international terrorism—case closed."
"After you get a thousand numbers and not one is turning up anything, you get some frustration."

—Former FBI official on useless leads passed to FBI from NSA warrantless spying program[1]

[1] Lowell Bergman, Eric Lictblau, Scott Shane, and Don Van Natta Jr., *Spy Agency Data After Sept. 11 Led F.B.I. to Dead Ends*, Jan. 17, 2006.
[2] Brian Ross, Vic Walter, and Anna Schecter, *Inside Account of U.S. Eavesdropping on Americans*, ABC News, Oct. 9, 2008.
[3] Jeff Jonas and Jim Harper, *Effective Counterterrorism and the Limited Role of Predictive Data Mining*, CATO Institute Policy Analysis, Dec. 11, 2006, http://www.cato.org/pubs/pas/pa584.pdf.

Our Nation's founders knew that privacy was worth fighting for.

Anger over the British Crown's use of "general warrants" to harass and spy on the colonists is said to have sparked the American Revolution. The revolutionaries fought for independence and then created a system of government that protected personal liberty. The Constitution, which enshrines the principle of checks and balances and guarantees Americans the right to privacy and the freedoms of speech and association, was meant to extinguish the unfettered search power that the Crown had claimed.

Unfettered surveillance has implications for us as individuals. We act differently when we think that people are watching. By reading our emails, listening to our phone calls, tracking our financial transactions, and accessing our library and Internet records, the government monitors our most intimate thoughts and activities. In doing so it encourages conformity and stifles creativity.

Unfettered surveillance also has societal implications, because it chills political activity and dissent. It discourages individuals from associating with controversial political groups, from donating to causes that the government disfavors, and from expressing their views on issues that are charged or controversial. Unfettered surveillance acts as a kind of censorship, and it impoverishes the marketplace of ideas.

"By casting the net so wide and continuing to collect on Americans and aid organizations, it's almost like they're making the haystack bigger and it's harder to find that piece of information that might actually be useful to somebody."

"You're actually hurting our ability to effectively protect our national security."

—Adrienne Kinne, former army linguist stationed at NSA on agency's monitoring of Americans abroad[2]

THE AMERICAN CIVIL LIBERTIES UNION protects the rights to privacy and free speech.

- We've fought legal battles concerning the NSA's warrantless wiretapping program, the FISA Amendments Act of 2008, the national security letter statute, and spying on peaceful protestors.
- We're fighting in Congress to pass civil liberties-friendly national security policies.
- We're engaged in public education efforts about the importance of privacy and free speech.
- Most importantly, we're demanding that the new President and Congress respect the Constitution, human rights, and the rule of law, and restore the liberties we've lost over the past eight years.

JOIN US!
You can help support our work by becoming a member of the ACLU, telling your family and friends about the importance of protecting privacy rights, and signing up to receive Action Alerts from the ACLU Action Center.

To learn more, please visit www.ACLU.org/join.

ACLU
AMERICAN CIVIL LIBERTIES UNION