

<http://www.eff.org/Privacy/Surveillance/Terrorism/PATRIOT/>

The USA PATRIOT Act

The USA PATRIOT Act broadly expands law enforcement's surveillance and investigative powers and represents one of the most significant threats to civil liberties, privacy and democratic traditions in U.S. history.
What is PATRIOT?

The USA PATRIOT Act (officially the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act) was quickly developed as anti-terrorism legislation in response to the September 11, 2001 attacks. The large and complex law received little Congressional oversight and debate, and was signed into law by President Bush Oct. 26, 2001.

PATRIOT gives sweeping anti-privacy powers to domestic law enforcement and international intelligence agencies and eliminates checks and balances that previously gave courts the opportunity to ensure that those powers were not abused. PATRIOT and follow-up legislation now in development threaten the basic rights of millions of Americans.

Why is EFF concerned about PATRIOT?

Under PATRIOT, civil liberties, especially privacy rights, have taken a severe blow:

*

The law dramatically expands the ability of states and the Federal Government to conduct surveillance of American citizens. The Government can monitor an individual's web surfing records, use roving wiretaps to monitor phone calls made by individuals "proximate" to the primary person being tapped, access Internet Service Provider records, and monitor the private records of people involved in legitimate protests.

*

PATRIOT is not limited to terrorism. The Government can add samples to DNA databases for individuals convicted of "any crime of violence." Government spying on suspected computer trespassers (not just terrorist suspects) requires no court order. Wiretaps are now allowed for any suspected violation of the Computer Fraud and Abuse Act, offering possibilities for Government spying on any computer user.

*

Foreign and domestic intelligence agencies can more easily spy on Americans. Powers under the existing Foreign Intelligence Surveillance Act (FISA) have been broadened to allow for increased surveillance opportunities. FISA standards are lower than the constitutional standard applied by the courts in regular investigations. PATRIOT partially repeals legislation enacted in the 1970s that prohibited pervasive surveillance of Americans.

*

PATRIOT eliminates Government accountability. While PATRIOT freely eliminates privacy rights for individual Americans, it creates more secrecy for Government activities, making it extremely difficult to know about actions the Government is taking.

*

PATRIOT authorizes the use of "sneak and peek" search warrants in connection with any federal crime, including misdemeanors. A "sneak and peek" warrant authorizes law enforcement officers to enter private premises without

the occupant's permission or knowledge and without informing the occupant that such a search was conducted.

*

The Department of Justice, with little input from Congress and the American people, is developing follow-on legislation - the Domestic Security Enhancement Act (nicknamed Patriot II) -- which would greatly expand PATRIOT's already sweeping powers.

Since PATRIOT became law:

*

Branch libraries in Santa Cruz (CA) County have posted signs warning patrons that "although the Santa Cruz Library makes every effort to protect your privacy, under the federal USA PATRIOT ACT (Public Law 107-56), records of the books and other materials you borrow from this library may be obtained by federal agents."

*

PATRIOT gives corporations, businesses and merchants justification to track the activities of employees and customers and requires banks and other financial institutions to monitor and report "suspicious" activity.

*

The Defense Advanced Research Projects Agency (DARPA) has started developing a system known as "Total Information Awareness" (TIA), which would mine and collect vast amounts of information about individuals Americans and create a massive domestic surveillance system.

DARPA recently issued its report to Congress regarding the renamed "Terrorism Information Awareness" program. The report, mandated by Congress and written to "assess the likely impact of the implementation" of TIA on civil liberties and privacy, was an opportunity for DARPA to review and require accountabilities for each TIA components. While DARPA has talked about the need for operational or technical (as opposed to legal) TIA privacy safeguards for some time (and deserves credit for having done so), EFF is disappointed by the superficiality of the Report's discussion and concerned about how TIA will affect the privacy of ordinary Americans.

*

The Transportation Security Administration has proposed the Computer Assisted Passenger Prescreening System II, or CAPPS II. The system would use public and private databases to rate passengers by color codes, which could be used by airlines to determine whether a passenger is allowed to board a flight or be subjected to additional questioning.

*

The U.S. State Department has cooperated with the Immigration and Naturalization Service to round up thousands of aliens suspected of terrorism, although most have been either released, given minor charges, or deported on visa or other technical violations.

What EFF has done:

*

EFF assisted Reef Seekers Dive Co. in resisting a federal grand jury subpoena demanding that the dive shop identify everyone who had taken, but not finished, its recreational dive classes over the last three years. The subpoena appears to have been based on fears that a terrorist attack using underwater

explosives could be carried out by partially-trained, recreational divers. After a call from the EFF, U.S. Attorneys withdrew the subpoena, and it has not been reissued.

*

A coalition of civil liberties organizations -- including EFF -- arguing against the Department of Justice in favor of citizens' rights, submitted a brief of amicus curiae in Sept. 2002 related to Foreign Intelligence Surveillance Court-authorized surveillance. The FISA appeals court accepted the brief, giving the public an unprecedented opportunity to participate in a FISA appeal.

*

EFF submitted comments to the Government criticizing the collection of air passenger and other information related to the development of CAPPS II and is working with other civil-liberties groups to protect the privacy of travel information.

*

EFF is working with various groups to create "best practices" for anonymizing or encrypting IP logs so that ISPs and other service providers (like Google) have less information of interest to the Government.

*

EFF has published a critical review of DARPA's report on TIA explaining how the report fails to address many privacy and civil liberties concerns.

*

EFF is encouraging businesses to use privacy-enhancing database techniques that expose less of people's personally identifiable information.

*

EFF supports the Freedom to Read Protection Act, the Domestic Surveillance Oversight Act, and the Data-Mining Moratorium Act.

Driving EFF action is a belief that:

*

Rapidly advancing technology has made surveillance cheaper and easier to conceal.

*

Fourth Amendment law has not kept up with technology.

*

Law enforcement and intelligence agencies must use these new powers carefully and limit their use to bona fide investigations into acts of terrorism. If laws are misused to spy on innocent people, courts must appropriately punish those who misuse them; Congress must reexamine its decision to grant such broad, unchecked powers.

*

Many vague, undefined terms in PATRIOT must be defined in favor of protecting civil liberties and privacy of Americans.

*

ISPs and others served with "roving" wiretaps and other unspecific orders must require the Attorney General provide certification that an order properly applies to them.

*

Congress must require law enforcement and intelligence agencies to report on their use of these new powers.

Why should you be concerned?

*

The U.S. Government - at state and Federal levels - now have more opportunities to watch what you're doing without legal justification.

*

Businesses and merchants are implementing methods to track your purchasing and job-related activities.

*

Law-abiding Americans with no ties to terrorist organizations are being detained and held without due process under PATRIOT's exceedingly vague definitions.

What should you do about it?

*

Join EFF - We're actively engaged in trying to challenge the U.S. Department of Justice's implementation of the PATRIOT. We're involved with major legal actions based on PATRIOT brought by the U.S. Government against individuals. We're working hard to influence the directions of PATRIOT II, the follow-up legislation now being drafted.

*

Tell your elected officials that you won't trade your civil liberties for vague assurances of greater security. Tell them not to repeat the PATRIOT mistake -- rhetoric and promises are no substitute for facts and logic.

For more information:

EFF resources

- * Analysis of the Protecting the Rights of Individuals Act
- * Analysis of the SAFE Act
- * Security and Freedom Ensured Act of 2003 (SAFE Act) [Download PDF (37k)]
- * PATRIOT Act Bills
- * EFF review of May 20 TIA report
- * EFF letter to Congress opposing TIA
- * EFF Analysis of the Provisions of the USA PATRIOT Act that Relate to

Online Activities

- * "Son of Patriot Act" brief summary
- * EFF calls for ongoing oversight of PATRIOT
- * Full EFF archive - "Censorship & Privacy - Terrorism"

Other resources

- * List of Communities Against the PATRIOT Act
- * Electronic Privacy Information Center PATRIOT page
- * American Civil Liberties Union PATRIOT page
- * FindLaw's Writ - Patriot II: The Sequel Why It's Even Scarier than the First Patriot Act