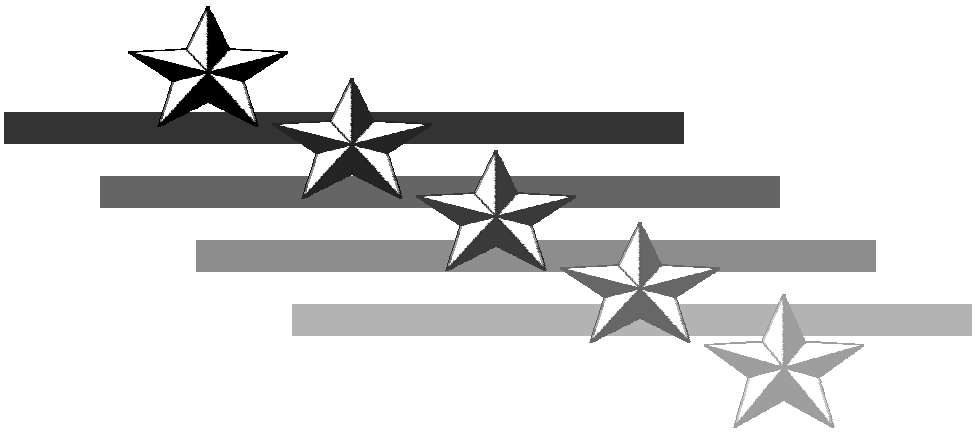
ALL ABOUT THE
USA PATRIOT ACT

A Manual for Activists

(and anyone else who wants to know more about the erosion of our liberties since September 11, 2001)



American Civil Liberties Union of Virginia

ALL ABOUT THE USA PATRIOT ACT

A Manual for Activists
(and anyone else who wants to know more about
the erosion of our liberties since September 11, 2001)

Funding for this report was provided by the
Tony Dunn Foundation
Washington, D.C.

Published by
American Civil Liberties Union Foundation of Virginia
Six North Sixth Street, Suite 400
Richmond, Virginia 23219

Telephone: (804) 644-8022
Email: acluva@acluva.org
Website: www.acluva.org

April 2005
June 2005
July 2005
January 2006
Revised February 2006

Contents

I. Why a Manual?

Perhaps the most controversial and least understood law in recent memory, the USA PATRIOT Act is a rambling 342-page hodgepodge that amends more than a dozen separate federal statutes, many in ways that dramatically erode the privacy and due process rights of American citizens and our immigrant population. It goes without saying that it defies easy distillation.

This manual explains key provisions of the PATRIOT Act for those who want to understand it better and especially for those who want to use that knowledge to change it. The ACLU is profoundly concerned about the loss of civil liberties since 9/11, having identified it as the highest organizational priority since the passage of the PATRIOT Act in late 2001. The information herein, having been scrupulously researched and documented, is accurate, to be sure. But the manual's purpose is to persuade-- to persuade the reader to persuade others to contact their congressional representatives, pass anti-PATRIOT Act resolutions in their locality, or simply pass on their outrage to others so that they too might act to restore our lost liberties.

Don't be daunted by the manual's size. Except for the most curious and compulsive among us, the manual is not meant to be read cover to cover. Find the parts that interest you, assemble them in the most meaningful way for your purposes, and rely on the rest as a resource.

One last thing. The PATRIOT Act and its many administrative and executive relatives are moving targets. Hardly a day goes by without something happening -- another court ruling, policy change, or newly exposed violation of our rights. At the end of the manual is a list of websites and other resources that can be used to find the latest information on most of the subjects addressed here. And while we plan to keep this manual updated, it will always be a little behind.

If you are reading this and are concerned about the loss of liberties in the United States, you have a friend in the ACLU. We can't be everywhere at once, but we'll try to help. Do not hesitate to call.

Kent Willis
Executive Director
ACLU of Virginia

II. Introduction: September 11, the USA PATRIOT Act & More

Three days after the terrorist attacks of September 11, 2001, before any investigation into what had caused the attacks or how they might have been prevented, the administration of President George W. Bush asked Congress to pass a package of far-reaching laws crafted by the Department of Justice under then-Attorney General John Ashcroft. These laws were described by Ashcroft as "carefully drawn to target a narrow class of individuals: terrorists" and crucial to federal law enforcement officials facing new challenges posed by a war on global terrorism. To underline this purpose, the legislation became known as the USA PATRIOT Act, an acronym for "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism."

Responding to the Administration's pleas for prompt action, the Senate Judiciary Committee held only one hearing on the provisions of PATRIOT Act and questioned only one witness: Ashcroft. The House Judiciary Committee drafted and circulated a less threatening alternative bill, but House members never got a chance to vote on it. They voted instead on an Administration-style bill that had been substituted at the last minute.

Five weeks after it was introduced, on October 26, 2001, President George W. Bush signed the PATRIOT Act into law.

But in fact, the government already had broad authority to prosecute anyone it reasonably believed was engaged in terrorism. It was also already empowered to spy on anyone it believed to be the agent of foreign power. But those powers were subject to various checks and balances put into place to prevent the government from running amuck. The effect of USA PATRIOT was to reduce those checks and balances while at the same time expanding the government's powers.

Americans would soon learn that the new powers bestowed by the PATRIOT Act are not, in fact, narrowly drawn. Nor do they apply only to the pursuit of suspected terrorists. Instead, they were deliberately written to be broadly construed, and they profoundly compromise the civil liberties promised by the U.S Constitution.

Meanwhile, through an exhaustive series of executive orders and agency rule changes, the executive branch has enhanced and increased its authority in a manner unprecedented even in wartime. Among other things, the Bush Administration has empowered itself to overrule immigration judges, suspend attorney-client privilege, engage in racial profiling dragnets, suspend the due process rights of non-citizens and engage in acts that, despite the prevarications of White House and Department of Justice lawyers, can only be described as torture. All this while at the same time invoking the pretext of national security to limit the public's right to information about government activities and the scrutiny of Congress.

In the months following September 11, federal agents engaged in mass arrests of Arab South Asian, North African and Muslim men, many of them legal, working, law-abiding immigrants. Under a provision of the PATRIOT Act, the U.S. attorney general may arrest and detain, without charge, any non-citizen he has "reasonable grounds to believe" poses a threat to national security. Federal agents made broad use of this provision, to identify and target an estimated 7,600 persons for questioning. Another 1,200 were imprisoned in federal detention centers, some on material witness warrants designed for use only on those whose testimony is crucial to a specific criminal investigation. Another 762 were jailed for minor civil immigration

violations and held incommunicado, without bond, often shackled and in solitary confinement, for an average period of 80 days each. None has ever been charged with a terrorism-related crime.

Targeted because of their ethnic and religious affiliations and referred to by the government as "persons of interest," the names of these prisoners were kept secret from the public. Immigration hearings, previously open to all, were summarily closed. And in a massive covert deportation program carried out late at night, planes conscripted from commercial airlines flew many of the detainees back to countries from which they had fled persecution.

Sweeps in Afghanistan and other Arab countries in an apparent attempt to round up Al Qaeda operatives led to the arrest of so-called "enemy combatants" -- a term found nowhere in either U.S. or international law, most of whom were taken to the U.S. military base in Guantánamo Bay, Cuba.

The Bush administration chose Guantánamo specifically because it considered the base to be beyond the reach of both U.S. and international law. In June 2004, the U.S. Supreme Court ruled otherwise. Guantánamo prisoners, said the Court, had the right to challenge their detentions in U.S. federal courts. However, this ruling has had little practical effect on the detainees. Most have never been charged and have not yet seen a lawyer.

Torture of U.S. detainees at the hands of American troops in Iraq came to light in April 2004 with the publication of photos depicting naked prisoners being menaced by dogs, beaten by guards and forced to simulate sodomy and maintain so-called "stress positions." Documents, testimony and eyewitness accounts since have revealed a widespread culture of torture and abuse, some of it religiously and culturally based, throughout U.S. detention facilities in Iraq, Afghanistan, and especially, Guantánamo.

The ACLU determined through a Freedom of Information Act request that the FBI has been gathering information not just on those who might possibly pose a threat to U.S. security, but also on the ACLU itself, Greenpeace and other groups. Although the FBI has yet to release the information gathered on the ACLU, the organization has learned that its post 9/11 government dossier now exceeds one thousand pages.

The focus of this manual is on the Patriot Act, but it is impossible to ignore these other threats to our freedoms that have arisen over the last four years.

III. Understanding the USA PATRIOT Act

A. Section-by-Section Explanation of Key PATRIOT Act Provisions

The PATRIOT Act is not easy reading. The law (P.L. 107-56) is a 342-page-long assemblage of amendments to existing laws referenced with a dizzying array of acronyms, code sections and subtitles. This formula, common to many laws, can make the simplest provision seem beyond comprehension. What follows is a distillation of the PATRIOT Act's most controversial provisions with accompanying explanations about the state of the law prior to USA PATRIOT and how it has changed. Many of these changes were so drastic that Congress agreed that they would "sunset" on December 31, 2005. Provisions scheduled to expire are indicated.

1. Section 201: Authority to Intercept Wire, Oral, and Electronic Communications Relating to Terrorism

Previous Law: Domestic wiretapping by federal authorities was governed by Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (§18 U.S.C. 2516). This statute prohibits wiretapping in general, but lists exceptions for law enforcement agents pursuing serious criminal cases involving a long list of predicate offenses, including the sabotage of nuclear facilities, espionage, treason, kidnapping murder, piracy, presidential assassination, hijacking and extortion. In addition, the Foreign Intelligence Surveillance Act of 1978 (FISA) contained provisions under which investigators could apply to a secret FISA court for permission to electronically monitor suspects in cases "linked to espionage" or involving the "agent of a foreign power."

Under USA PATRIOT: Section 201 adds the following new crimes to the list of predicate offenses under which federal investigators may seek wiretaps: "terrorist acts of violence committed against Americans overseas," "use of weapons of mass destruction," use of "chemical weapons," "acts of terrorism transcending national boundaries," "financial transactions with countries that support terrorists," and "providing material support to terrorists." But since federal investigators already had the power to wiretap in all such cases involving espionage or agents of a foreign power, critics allege that this amendment functions primarily to broaden that power to permit wiretapping of a U.S. person suspected of domestic terrorism.

Status: Set to expire Dec. 31, 2005, extended to Feb. 3, extended to Mar. 10, 2006.

2. Section 202: Authority to Intercept Wire, Oral, and Electronic Communications Relating to Computer Fraud and Abuses

Previous Law: Under previous law, investigators could not wiretap or intercept wire communications (communications involving a human voice) in order to investigate violations of the Computer Fraud and Abuse Act (18 U.S.C. §1030).

Under USA PATRIOT: Under Section 202, investigators can seek and get permission to wiretap voice communications while investigating computer fraud and abuse. Section 202 confers this authority by adding computer fraud and abuse (as defined by the various felonies listed in the Computer Fraud and Abuse Act) to the list of predicate felonies for

which investigators can get wiretap permission in Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (§18 U.S.C. §2516(1)).

Status: Set to expire Dec. 31, 2005, extended to Feb. 3, extended to Mar. 10, 2006.

3. Section 203b and 203d: Authority to Share Criminal Investigative Information

Previous Law: Section 2517 of Title 18, United States Code, provides the guidelines for the use and disclosure of intercepted wire, oral, or electronic communications gathered in criminal investigations.

Under USA PATRIOT: Section 203b amends 18 U.S.C. §2517 to allow for the disclosure of information gathered from intercepted wire, oral, or electronic communications in criminal investigations to "any Federal law enforcement, intelligence, protective, immigration, national defense or national security official in order to assist the official receiving the information in the performance of his official duties."

Section 203d, adds section 403-5d to Title 50, United States Code, which provides a general exception for foreign intelligence. This provision, much like section 203b, allows "foreign intelligence" information collected during a criminal investigation to be disclosed to other federal agents. "Foreign intelligence" is defined as "information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons or international terrorist activities." This definition specifically includes information about a U.S. person that concerns a foreign power or foreign territory and "relates to the national defense or the security of the United States" or "the conduct of the foreign affairs of the United States."

Status: Set to expire Dec. 31, 2005, extended to Feb. 3, extended to Mar. 10, 2006.

4. Section 206: Roving Surveillance Authority under FISA

Previous Law: In non-FISA cases, court orders authorizing wiretaps and pen register/trap and trace devices were valid only within the geographic jurisdiction of the issuing court. In FISA cases, law enforcement agents seeking to conduct electronic surveillance were required to specify which particular telephone line, computer or facility they intended to monitor and the particular third party (such as a specific common carrier or communications service provider) that would have to assist them in doing so.

Under USA PATRIOT: Now, law enforcement agents can obtain "roving wiretap" authority under FISA. This means that unnamed and unspecified third parties all over the country may be drafted in order to assist authorities in their efforts to monitor targets. In addition, users of public facilities offering Internet access, such as libraries and university computer labs are exposed to government monitoring whenever the government suspects that its target is using the same facility. Moreover, unlike other roving wiretap laws, this provision does not include a requirement that the eavesdropper make sure that the target is actually using the device being monitored. This problem is aggravated by the fact that the unspecified third parties conscripted into assisting the government (librarians, for example) are prohibited under penalty of law from disclosing to other users that monitoring activities are taking place.

Status: Set to expire Dec. 31, 2005, extended to Feb. 3, extended to Mar. 10, 2006.

5. Section 207: FISA Surveillance of Non-US Persons Who Are Agents of a Foreign Power

Previous Law: Unless directed at a foreign power, the maximum duration for FISA surveillance orders and extensions was 90 days. For physical searches, it was 45 days.

Under USA PATRIOT: Section 207 extends the maximum life of an order for a physical search to 90 days. In cases involving an agent of a foreign power, it extends both surveillance and physical search orders to 120 days with possible extensions up to a year.

Status: Set to expire Dec. 31, 2005, extended to Feb. 3, extended to Mar. 10, 2006.

6. Section 212: Emergency Disclosure of Electronic Communications to Protect Life and Limb

Previous Law: Title 18 U.S.C. §2702 prohibits electronic communication service providers from disclosing customer records and communications, and details certain exceptions. For example, law enforcement may obtain such information as it pertains to the commission of a specific crime.

Under USA PATRIOT: Section 212 adds another exception to Section 2702. It authorizes electronic communication service providers to disclose the records of users and content of communications to a government entity, "if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information." In the event of an emergency, the government can demand this information without consent, notice, or judicial review.

Status: Set to expire Dec. 31, 2005, extended to Feb. 3, extended to Mar. 10, 2006.

7. Section 213: Authority for Delaying Notice of the Execution of a Warrant

Previous Law: Principles laid out in the Fourth Amendment and related case law required government agents to obtain a search warrant based on probable cause in order to search someone's home or business, and to notify that person prior to, or at the same time as, the search. Courts made exceptions to this "prior notice" rule in cases where an announcement was likely to cause evidence to be destroyed or imperil police or in cases where authorities were conducting legal surreptitious surveillance.

In addition, Title 18 U.S.C. §3109 authorizes law enforcement officers to break and enter when executing a warrant only after they have knocked and announced their purpose. Finally, Rule 41(d) of the Federal Rules of Criminal Procedure requires an officer who seizes property under a warrant to give the person whose premises are searched a copy of the warrant and a receipt for any property seized.

Under USA PATRIOT: Section 213 allows "sneak and peek" searches of homes and businesses without notice whenever "immediate notification of the execution of the warrant may have an adverse effect." This provision is not limited to terrorism cases, but applies to all government searches for material that "constitutes evidence of a criminal offense under the laws of the United States." Now, in any such search, notice can be delayed for an undefined "reasonable period" which can be extended for a similarly undefined "good cause."

In addition, Section 213 permits authorities to "seize" any piece of tangible property or communications where the court finds "reasonable necessity" for such a seizure.

Status: This provision is permanent.

8. Section 214: Pen Register and Trap and Trace Authority Under FISA

Previous Law: Under Title III of the Omnibus Crime Control and Safe Streets Act of 1968, police could get permission to install a wiretap on a showing of probable cause that one of an enumerated list of crimes had been committed. Warrants for such wiretaps were valid for 30 days, and the court oversaw their implementation. In 1978, Congress passed the Foreign Intelligence Surveillance Act (FISA), which lowered the standards in cases involving "agents of a foreign power" and persons "linked to espionage." In those cases only, government agents could obtain FISA orders to install trap and trace pen register devices by certifying to the FISA Court that the information they sought would be "relevant to an ongoing criminal investigation."

Under USA PATRIOT: The requirement that FISA orders apply only to cases involving "agents of a foreign power" or persons "linked to espionage" is gone, as is the requirement that, in ordinary criminal cases, law enforcement officials must show probable cause in order to obtain a warrant.

Government agents can now get FISA orders for trap and trace devices in cases involving anyone. Agents have only to assert that the devices will be used as part of an investigation to protect against international terrorism or clandestine intelligence activities and that their request is not solely motivated by an American's exercise of his or her First Amendment rights.

Status: Set to expire Dec. 31, 2005, extended to Feb. 3, extended to Mar. 10, 2006.

9. Section 215: **Access to Records and Other Items under the Foreign Intelligence Surveillance Act**

Previous Law: Federal agents needed to show probable cause that a crime had been committed to obtain a search warrant or subpoena from a neutral judge in order to conduct a search or compel production of books, records, papers, documents or other items. This rule was somewhat compromised in cases involving "agents of a foreign power" where FISA allowed searches and surveillance without such a showing of probable cause as long as their primary purpose was to obtain foreign intelligence information and the target was "linked to foreign espionage."

Under USA PATRIOT: Government agents now have the authority to request "any tangible thing" about anybody from anybody as long as they claim that it is relevant to an ongoing investigation of international terrorism or clandestine intelligence activities. "Any tangible thing" is a category so broad it could reasonably encompass everything from business, medical, educational, library, bank, church, and phone records to an apartment key. Those targeted have no way of finding out that the government is watching them because everyone ordered to produce information is automatically gagged – under penalty of law – from disclosing that fact to anyone.

Status: Set to expire Dec. 31, 2005, extended to Feb. 3, extended to Mar. 10, 2006.

10. Section 216: Modification of Authorities Relating to Use of Pen Registers and Trap and Trace Devices

Previous Law: As written, prior law pertained only to the telephone industry and referred to the collection of "numbers dialed" on a "telephone line" and the "originating number" of a telephone call. Internet surveillance by federal authorities was not well regulated. Some judges applied wiretap law to the Internet; others did not. The collection of this information required law enforcement to obtain a court order under a low standard of proof, that "the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation." The court issuing that order had to be located in the same jurisdiction as that of the information to be collected.

Under USA PATRIOT: Section 216 amends previous legislation to allow the court order that must be obtained to collect the information to come from the jurisdiction of the offense, rather than the source of the information. This warrant would be executable in multiple jurisdictions. Section 216 also amends the definitions of pen registers and trap-and-trace devices to expressly apply to the internet and e-mail. The new definition of a pen register is: a "device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted." A trap and trace device is now a "device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing or addressing and signaling information reasonably likely to identify the source or a wire or electronic communication." Warrants to monitor computer communications may be issued for any suspected crimes, not just those that are terrorism-related. Section 216 maintains the low standard of proof, but because of its expanded application to other media, it exacerbates an existing problem, in the ACLU's view.

Status: This provision is permanent.

11. Section 217: **Interception of Computer Trespasser Communications**

Previous Law: With few statutory exceptions, the intentional interception or disclosure of the contents of any intercepted communication without a judicial order was illegal under the wiretap statute (Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (§18 U.S.C. 2516).

Under USA PATRIOT: Internet Service Providers, universities, network administrators and other computer owners can now give government agents permission to monitor their computers for "trespassers" without a judicial order or notice to persons being monitored. Under Section 217, only those who have a "contractual relationship" with the owner or operator of such computers have a reasonable expectation of privacy. Everyone else – college students who use university computers, library patrons who use library computers, customers at Internet cafes and airport lounges – is subject to monitoring.

Status: Set to expire Dec. 31, 2005, extended to Feb. 3, extended to Mar. 10, 2006.

12. Section 218: **Foreign Intelligence Information**

Previous Law: The Foreign Intelligence Surveillance Act of 1978 (FISA) created an exception to the Fourth Amendment requirement of a warrant issued upon probable cause for police searches, wiretaps and subpoenas in cases that involved the monitoring of foreign powers and their agents. Government officials investigating such cases applied to a secret FISA court that convened infrequently, performed no oversight and almost always issued the requested warrant. Instead of demonstrating to the FISA Court that they had probable cause to believe that a crime had been committed, agents had only to demonstrate probable cause to believe that their target was an "agent of a foreign power."

In FISA cases involving U.S. citizens or legal permanent residents, the standard was higher. Government agents had to show that the activities of the targeted citizens or residents "involve" or "may involve" a violation of U.S. criminal law.
FISA warrants were good for 90 days against a suspected foreign agent and for up to a year against a foreign power. FISA searches and surveillance were carried out secretly, without notice to the targeted parties, unless or until they were prosecuted. Because of the extraordinary nature of these powers, Congress limited their exercise to investigations whose "primary purpose" was the gathering of foreign intelligence."

Under USA PATRIOT: Section 218 subjects everyone and anyone – citizen or non-citizen – to a search or wiretap under FISA. The government no longer has to show that it is targeting the agent of a foreign power or someone linked to espionage. Nor must it assert that its primary purpose is the gathering of foreign intelligence. Now, a federal agent need only claim that an investigation contains a "significant" foreign intelligence component, and the Court must issue the order he requests. Finally, the fruits of the search, which could not be used as evidence under FISA, can be seized and used as evidence under USA PATRIOT.

Status: Set to expire Dec. 31, 2005, extended to Feb. 3, extended to Mar. 10, 2006.

13. Section 219: **Single Jurisdiction Search Warrants for Terrorism**

Previous Law: Federal and state judges could issue search warrants for property or persons within the confines of their judicial districts only.[1] A 1990 federal rule amendment allowed federal judges to also issue warrants for persons or property outside of their districts providing the person or property was within the district at the time the warrant was issued.[2]

Under USA PATRIOT: Section 219 amends the Rules of Federal Criminal Procedure to allow federal magistrates to issue search warrants "in any district in which activities related to the terrorism may have occurred, for a search of property or for a person within or outside the district."[3]

Status: This provision is permanent.

[1] F.R.C.P. 41(a)(1).
[2] F.R.C.P. 41(a)(2).
[3] F.R.C.P. 41(a)(3).

14. Section 220: **Nationwide Service of Search Warrants for Electronic Evidence**

Previous Law: Under 18 U.S.C. §2703, government agents could get a search warrant compelling a communications provider to disclose the contents of e-mails less than six months old. But federal rules restricted search warrants to property within the issuing jurisdiction, meaning agents had to request a warrant in the district where the relevant provider was based, rather than in the district where their investigation was based.

Under USA PATRIOT: Section 220 amends section 2703 to allow federal magistrates to issue warrants for e-mails stored by providers in other jurisdictions, thereby opening the door for prosecutors to find judges who are favorable to their position. This change applies to all criminal investigations; not just terrorism cases.

Status: Set to expire Dec. 31, 2005, extended to Feb. 3, extended to Mar. 10, 2006.

15. Section 411: Definitions Relating to Terrorism

Previous Law: The Immigration and Nationality Act states that foreign nationals may be deported if they were inadmissible at the time they entered the country or if they subsequently engaged in terrorist activity (8 U.S.C. 1227). Foreign nationals may be inadmissible for various terrorism-related reasons (8 U.S.C. 1182), including association with a terrorist organization. Under Section 219 of the Immigration and Nationality Act (8 U.S.C. 1189), the Secretary of State may designate as a terrorist organization, any foreign group which he finds to have engaged in terrorist activities.

Under USA PATRIOT: Section 411 expands the grounds for deportation and inadmissibility for alleged support of terrorist causes. This section redefines the categorizations of "engaging in terrorist activity" and "representing a terrorist organization," and adds espousing terrorist activity, being the spouse or child of an inadmissible alien, and associating with a terrorist organization and intending to engage in activities that could endanger the welfare, safety or security of the United States. Section 411 expands the definition of a terrorist organization to those groups that the Secretary of State has identified in the *Federal Register* as having provided material support for, committed, incited, planned, or gathered information on potential targets of terrorist acts of violence.

Status: This provision is permanent.

16. Section 412: Detention of Suspected Terrorists; Habeas Corpus; Judicial Review

Previous Law: The Immigration and Nationality Act (8 U.S.C. 1226) details the laws regarding the apprehension and detention of foreign nationals.

Under USA PATRIOT: Section 412 adds section 1226a to the Immigration and Nationality Act, titled the "Detention of Terrorist Aliens." This section allows the attorney general to unilaterally detain non-citizen terrorist suspects for seven days without charges. Within seven days, the attorney general must initiate removal or criminal proceedings or release the suspected terrorist alien. If the suspect is held, the detention is subject to judicial review at six month intervals for an indefinite time.

Status: This provision is permanent.

17. Section 505: **Miscellaneous National Security Authorities**

Previous Law: Under the Electronic Privacy Act, the Right to Financial Privacy Act, and the Fair Credit Reporting Act, the FBI had to show that the records being sought pertained to potential acts of espionage or terrorism by a particular individual, before third parties could release confidential information.

Under USA PATRIOT: Section 505 amends these statutes to allow the Director of the Federal Bureau of Investigation to request the abovementioned records through National Security Letters (NSLs), which are administrative subpoenas issued directly by the Justice Department without a court order. NSLs can be used to retrieve business documents whenever the documents are deemed "relevant" to a terrorism or national security investigation. Records demanded can include "any record...pertaining to the customer's relationship with the institution." Under the 2004 Intelligence Authorization Bill, almost any business was subject to this provision.

Status: This provision is permanent.

On Sept. 29, 2004, in *Doe* v. *Ashcroft*, U.S District Judge Victor Marrero of the Southern District of New York struck down the National Security Letter statute (particularly 18 U.S.C. 2709b) on the grounds that it violates free speech rights under the First Amendment as well as the right to be free from unreasonable searches under the Fourth Amendment. When a statute is deemed unconstitutional in its entirety, as was the case with the NSL statute, all amendments to the statute are necessarily struck down as well. Thus, section 505a of the PATRIOT Act was declared unconstitutional. However, Judge Marrero's decision has been put on hold pending the government's appeal of Judge Marrero's decision, which is currently before the 2nd Circuit Court. Consequently, the government may continue to prosecute under the NSL statute and section 505.

18. Sections 507 and 508: Disclosure of Student Records

Previous Law: The General Education Provisions Act (20 U.S.C. 1232g) and the National Education Statistics Act (20 U.S.C. 9007) provide for the privacy of student records held by educational institutions and the National Center for Education.

Under USA PATRIOT: Section 507 allows Justice Department officials to collect educational records relevant to an investigation or prosecution of a crime of terrorism without individual suspicion. Section 508 allows those same officials to collect individually identifiable information from the National Center for Education without individual suspicion. Educational institutions and employees of the National Center for Education who cooperate receive immunity from liability for the disclosure.

Status: These provisions are permanent.

19. Section 802: Definition of Domestic Terrorism

Previous Law: Section 2331 of Title 18 on Crimes and Criminal Procedure defines "international terrorism".

Under USA PATRIOT: Section 802 amends the definition of "international terrorism" to include a violent, criminal act intended to affect the conduct of government by mass

destruction. This section also defines “domestic terrorism” to include any act that is “dangerous to human life,” involves a violation of any state or federal law and is intended to influence government policy or coerce a civilian population. [The ACLU fears protesters will be targeted under this section.]

Status: This provision is permanent.

20. Section 805: Material Support for Terrorism

Previous Law: Following the 1995 bombing of the Murrah Federal Building in Oklahoma City, Congress enacted "The Antiterrorism and Effective Death Penalty Act of 1996” (AEDPA), part of which made it illegal for U.S. citizens (and noncitizens) to provide material support to the activities of any foreign group designated by the Secretary of State as "terrorist.” The law also called for the Secretary of State to create a list of "Foreign Terrorist Organizations" or “FTOs.” The Treasury Department became responsible for blocking funds to those put on the list.

Under USA PATRIOT: Section 805 amended the AEDPA by adding a prohibition against giving "expert advice or assistance" to terrorists and increasing prison sentences for material support crimes from 10 to 15 years.

Status: This provision is permanent.

On Jan. 23, 2004, in a lawsuit brought by the Humanitarian Law Project and other non-profit organizations against the Department of Justice, U.S. District Judge Audrey Collins in Los Angeles declared Section 805 unconstitutional on the grounds that it was “impermissibly vague,” violating the promises of freedom of speech and freedom of association in the First Amendment of the U.S. Constitution, as well as the Fifth Amendment’s guarantee of due process. This ruling applies only to those in the 9th circuit. In other parts of the country, the provision may be enforced.

21. Section 901: Responsibilities of Director of Central Intelligence Regarding Foreign Intelligence Collected under FISA

Previous Law: Section 103(c) of the National Security Act of 1947 (50 U.S.C. 403-3(c)) details the responsibilities of the Director of Central Intelligence.

Under USA PATRIOT: Section 901 expands the responsibilities of the Director of Central Intelligence to allow him to, “establish the requirements and priorities for foreign intelligence information” gathered under FISA. This section allows for domestic spying, which could put the CIA back in the business of monitoring Americans’ lawful activities.

Status: This provision is permanent.

~Much of the information compiled in this section was based on a Congressional Research Service report titled, “Terrorism: Section by Section Analysis of the USA PATRIOT Act,” written by Charles Doyle. ~

For Background Documents and Online Resources for Keeping Current on the PATRIOT Act , see page 32

B. Reauthorizing the USA PATRIOT Act

Sixteen controversial provisions of the USA Patriot Act that were due to expire on December 31, 2005 have been extended twice, giving Congress until March 10, 2006 to make a decision. In the wake of reports of domestic warrantless spying by the Federal Bureau of Investigation and National Security Agency, members of Congress and the public have become increasingly concerned about abuse of power by the Executive Branch.

1. The Conference Report

During the summer of 2005, the House of Representatives and Senate each passed its own version of legislation to reauthorize the Patriot Act. With vast differences between the bills, the conference committee with representatives from both houses met to draft one bill to be voted on by the full Congress. The conference committee submitted its report on December 8, 2005.

The reauthorization bill would make virtually all of the expiring provisions permanent without including necessary changes to restore checks and balances. Of the 16 provisions due to expire, all but two will become permanent. The exceptions, sections 206 ("roving wiretaps," *page 6*) and 215 ("business records," *page 8*) will have four-year sunsets.

The changes to the Patriot Act do not include meaningful safeguards for civil liberties. For example, personal records from libraries, bookstores, doctor's offices, businesses, etc. can still be obtained under a secret order from the FISA court (*section 215, page 8)* or by a FBI-issued "national security letter" (*section 505, page 12)* that requires no court oversight. FISA orders and NSLs continue to contain a potentially permanent gag provision that bars a recipient from telling anyone (other than the recipient's lawyer) that records have been obtained. Also, secret "sneak-and-peek" searches (*page 7*) are still allowed under a broad standard. The new 30-day time limit with the possibility for an unlimited number of 90-day renewals would still allow these searches to remain secret for weeks, months, or even years.

Below is a more detailed analysis of some of the controversial provisions of the conference report:

a. Section 206: Roving Surveillance Authority under FISA ("roving wiretaps")

The FISA roving wiretap provisions do not even meet the same standards as criminal wiretaps. Criminal wiretaps require that either the target or the phone be identified and that the government determine the target is near the phone to listen in. Neither of these conditions is required for FISA roving wiretaps. Moreover, the ten-day after the fact notice requirement is no substitute for privacy safeguards in criminal wiretaps.

b. Section 213: Authority for Delaying Notice of the Execution of a Warrant (sneak-and-peek searches)

The conference report still allows for secret searches of a person's home or business to remain secret indefinitely. There is a 30-day presumptive time limit with an unlimited number of 90-day renewals, which far exceeds the customary 7-day limit that was imposed by federal courts before the Patriot Act. Even these long time limits can be waived in any case if the government shows that "the facts of the case justify" a

longer period. The conference report also preserves the vague "catch-all" standard allowing delays for an "adverse result," including jeopardy to an ongoing investigation.

c. Section 215: Access to Records and Other Items under FISA (secret court orders for library, medical, other personal records)

The conference report adopted the House language rather than the Senate's, which was supported by Chamber of Commerce, conservative, library, and civil liberties organizations. There is no requirement for connecting private, personal records to a foreign terrorist or spy. The new "presumption of relevance" makes it easier to get records if there is such a connection, but it is still just as easy as it is now to get records of innocent people who are not connected to terrorists. The "minimization" standards have been watered down so there is no requirement of a connection to a foreign terrorist or spy to retain information.

Also, the right to judicial review could prove illusory. A recipient, who must go to the expense of hiring a pre-approved lawyer with security clearance, must challenge an order before a pre-selected group of 3 FISA court judges. The standard for a challenge is only whether the order is lawful; the FISA court still lacks discretion to suppress a subpoena on any other grounds. The government may make unlimited use of secret evidence in resisting a challenge.

Lastly, the "grand jury" standard is seriously compromised by language that says the government may use these orders to obtain privileged information, such as attorney-client communications. Moreover, there is no express right to challenge a secrecy order.

d. National Security Letters ("NSLs")

The proposed reauthorization creates a new crime of unauthorized disclosure of an NSL, creating more leak investigations. Any knowing disclosure – even if made with no intent to obstruct the investigation – could be punished by up to one year in prison. Today, there is no explicit penalty. Reporters could be subpoenaed and forced to reveal confidential sources if they learn about an NSL – something that cannot happen now.

There is no requirement to connect private, personal records to a foreign terrorist or spy in order to obtain a NSL. NSLs remain permanent and are not subject to future congressional review through a sunset clause.

The conference report would allow the government to get a court order requiring a business or person to hand over records or face jail time for contempt of court thereby transforming national security <u>letters</u> into national security <u>subpoenas</u>. The right to challenge the secrecy of a gag order is illusory. The government has the unlimited right to keep a records order secret indefinitely and the court must accept the government's statement that disclosure of the order would harm national security as conclusive. This is an unconstitutional interference with the court's right to review whether government's interests are compelling enough to outweigh the recipient's right to speak out.

2. Congressional Voting

Capitulating to the executive branch, the House of Representatives passed the conference bill reauthorizing the Patriot Act by a vote of 251 to 174 on December 14, 2005. The Senate, however, denied a cloture motion on December 16. By denying cloture, senators allowed debate on the Patriot Act to continue and made possible a filibuster. In a compromise, however, the Senate on December 21 passed a bill extending the Patriot Act sunset provisions for six months.

Dissatisfied with the long extension, the House shortened the Patriot Act extension to just five weeks. The Senate, represented by John W. Warner, approved the compromise allowing debate to continue until February 3.

Nowhere near a compromise at the start of February Congress extended the expiring provisions of the Patriot Act until March 10. Senate holdouts have been negotiating with the White House to ensure civil liberties safeguards in the Patriot Act reauthorization legislation.

C. USA PATRIOT Act and the Bill of Rights

Almost everyone knows the Bill of Rights, the first ten amendments to the Constitution put in place to protect individual freedoms. This section examines the PATRIOT Act through the lens of the Bill of Rights, offering examples of how the Act diminishes or threatens to diminish our most widely revered individual rights, such as free speech, privacy, and fairness in criminal proceedings.

1. First Amendment (free speech, assembly, and religion)

The First Amendment guarantees the free practice of religion, freedom of speech, and by extension, freedom of association. It also promises the right to peaceably assemble and the right to petition the government for redress of grievances. Specifically:

> *Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people to peaceably assemble and to petition the government for redress of grievances.*

A combination of factors makes Section 215 of USA PATRIOT a direct threat to our First Amendment rights. Section 215 gives government agents unprecedented access to personal records held by third parties, such as libraries, schools, physicians, and financial institutions. The individual or group whose records are sought need not be a criminal suspect. Instead, the government must show only that the inquiry is relevant to an ongoing investigation of international terrorism or clandestine intelligence activities.

Knowing the government may be gaining easy access to personal records means more than a loss of privacy; it is also likely to affect the choices individuals make that produce the records in the first place, including books they buy or check out of the library or the groups to which they belong.

More directly, Section 215 undermines free speech by gagging the person who has been compelled by the government to hand over the records by making it a crime to tell anyone else about the transaction. Thus, if a librarian is forced under Section 215 to provide to the government a list of the books checked out by patron, that librarian may not tell anyone else, including the patron, about the exchange of information.

In addition, Section 215 allows the government to ignore the First Amendment's promise of freedom of association by expanding the power of its agents to gather materials on the activities of religious and political institutions, and to infiltrate these groups with no suspicion of criminal activity.

2. The Fourth Amendment (search and seizure)

The Fourth Amendment protects us from unreasonable government searches of our homes, businesses, persons and possessions. It specifically requires that such searches be supported by warrants describing the person or thing to be searched:

> *"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."*

Using USA PATRIOT as its primary enabling tool, the Bush administration has used its "war on terror" to compromise the Fourth Amendment rights of all Americans, not just those of suspected spies and terrorists. For example, before USA PATRIOT, the government could only obtain search warrants by demonstrating to a judge that its agents had probable cause to believe that the person they targeted was involved in criminal activity. The one exception to this rule was the Foreign Intelligence Surveillance Act, or FISA. Under FISA, the secret FISA court could authorize a secret search but only in an espionage case and only as long as the target of the search was "the agent of a foreign power" or someone "linked to espionage."

Now, under Section 218 of USA PATRIOT, this is no longer true. FISA searches can be conducted against anyone -- not just suspected spies and terrorists -- as long as the FBI contends that the search is relevant to "foreign intelligence."

Even when searches are not relevant to foreign intelligence, USA PATRIOT changes the rules to make things easier for the government. Prior to 9/11, law enforcement agents conducting a search pursuant to a warrant in a non-FISA case were required to "knock and announce" themselves before entering a premises. Now, under Section 213, agents can ignore the "knock and announce" rule if "immediate notification of the execution of the warrant may have an adverse effect." Also under Section 213, the government does not necessarily have to disclose that the search occurred -- even after it has been completed. Instead, agents can now wait for an undefined "reasonable period" before revealing to a citizen that they have searched his or her property. This reasonable period can be extended, possibly indefinitely, for "good cause shown."

In addition, under Section 215 of USA PATRIOT, FBI agents can, with no demonstration of probable cause or warrant, demand an individual's private records as well as any other "tangible items" from third parties such as bookstores, doctors, libraries and banks. Under prior laws, access to such records could only be gained by court-ordered subpoena. Now, such access is automatic if agents assert that the records are necessary to "protect against international terrorism

or clandestine intelligence activities." And again, once such a demand is made, Section 215 prohibits the person or entity asked to produce the records from disclosing that fact to anyone—including the person whose records were sought.

3. The Fifth and Sixth Amendments (fairness in criminal prosecutions)

> *No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offense to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.*
>
> *-The Fifth Amendment*

> *In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the state and district wherein the crime shall have been committed, which district shall have been previously ascertained by law, and to be informed of the nature and cause of the accusation; to be confronted with the witnesses against him; to have compulsory process for obtaining witnesses in his favor, and to have the assistance of counsel for his defense.*
>
> *- The Sixth Amendment*

The primary and most important promise made by the Fifth Amendment is that no "person" shall be "deprived of life, liberty or property" without due process of law.

Due process of law, as the Sixth Amendment makes clear, requires that the government inform anyone it accuses of a crime of "the nature and cause of the accusation, that it provide to that person "a speedy and public trial." It also specifically requires the government to safeguard the right of the accused to confront hostile witnesses and present favorable ones and to have access to the assistance of a lawyer. The U.S. Supreme Court has ruled that these rights belong not just to U.S. citizens, but specifically to "any person" accused by the government. The Court has also affirmed that legal aliens who remain "physically present" in the United States are "persons" entitled to the due process protections of life, liberty, and property under the Fifth Amendment and that even illegal aliens are entitled to the protections of the Bill of Rights:

> The Fifth Amendment, as well as the Fourteenth Amendment, protects every one of these persons from deprivation of life, liberty, or property without due process of law. Even one whose presence in this country is unlawful, involuntary, or transitory is entitled to that constitutional protection.[1]

Section 412 of USA PATRIOT allows the government to take into custody any alien whom it has "reasonable grounds to believe" is "engaged in any…activity that endangers the national security of the United States." Such aliens can be held for seven days, at which point they must either be charged with a crime or deported. Aliens held pursuant to immigration violations, however, can be held indefinitely under this provision.

---

[1] Mathews v. Diaz, 426 U.S. 67 (1976)

The Fifth Amendment also prohibits the government from confiscating private property without just compensation. But Title I, Section 106 of USA PATRIOT amends the International Emergency Powers Act to give the president unprecedented powers in the time of armed hostilities or attack by foreign actors to "confiscate any property, subject to the jurisdiction of the United States, of any foreign person, foreign organization, or foreign country that he determines has planned, authorized, aided, or engaged in such hostilities or attacks against the United States."

Although the statute itself does not allow for judicial review of such seizures, Section 316 of USA PATRIOT grants the owners of confiscated property the right to challenge the classification of their property as a terrorist asset. However, Section 316 also allows for the suspension of the Rules of Federal Evidence in such cases if the court decides that complying with them could endanger national security.

4. The Constitutional Right to Privacy

Although not specifically enumerated, the U.S. Supreme Court has held that the Bill of Rights conveys a constitutional right to privacy. The USA PATRIOT compromises our right of privacy by expanding the government's search and seizure rights as outlined above. But other provisions also infringe on privacy by giving the government easy access to citizens' financial, educational, and other records.

Title III of the PATRIOT Act, also known as the International Money Laundering Abatement and Financial Anti-Terrorism Act of 2001, compromises the right to privacy by encouraging increased monitoring by banks and financial institutions. Section 355 allows financial institutions to communicate and document their suspicions concerning the involvement of current or former employees in "potentially unlawful activity." Section 356, meanwhile, requires securities brokers and dealers to submit reports documenting suspicious activity or transactions.

Section 358 amends the Right to Financial Privacy Act of 1978 to give law enforcement authorities access to financial data related to intelligence or counterintelligence activities, investigations, or analysis "to protect against international terrorism." Under this Section, "financial analysis" becomes a sufficient reason for federal authorities to review private financial information.

In the Consumer Watch column of the Richmond Times-Dispatch's (June 19, 2005) business section, Iris Taylor explains how Title III of the PATRIOT Act could affect everyday consumers. A reader, who wished to remain anonymous, told Taylor of his discovery that the government had looked into his financial activities, which resulted in his unfairly being given a higher interest rate on a loan. The bank reported to the government the reader's "suspicious activity" of opening several credit accounts in a short period of time, and performed a credit check. However, the reader was actually opening money market accounts, which is unrelated to credit accounts and would not require a credit check. Title III has created an atmosphere among financial institutions that encourages over-reporting to the government and unnecessary credit checks to the detriment of consumers.

Section 507 of USA PATRIOT amends The Family Educational Rights and Privacy Act (FERPA) to allow government access to precisely the information the Act was intended to protect: educational records. Prior to USA PATRIOT, FERPA permitted disclosure of such records pursuant to a subpoena issued on probable cause and a sworn affidavit that the

information was essential to a criminal investigation. As amended by USA PATRIOT, such records must now be automatically disclosed to federal agents once they certify that it may be relevant to a terror investigation. This amendment makes disclosure of educational records the rule, rather than the exception, and has permitted federal "sweeps" of the educational records of certain groups of persons, notably aliens residing in the United States on student visas.

Finally, Sections 405, 414 and 1008 of USA PATRIOT require the Attorney General to explore the feasibility of using "biometric identification systems," or fingerprinting, at U.S. airports, customs offices and harbors. The provisions also allow this identification to be used for issuing passports and visas, as well as other secure information systems, such as bar code identifiers that will "interface" with other law enforcement agencies to identify and detain individuals who may pose a threat to national security.

IV. Not Just the Patriot Act: Other Threats to Liberty since 9/11

A. The Homeland Security Act of 2002

At 484 pages, The Homeland Security Act of 2002, signed by President Bush on November 25 of that year, exceeds even USA PATRIOT in length. At its core is a massive restructuring of government that incorporates 22 disparate federal agencies – including the Coast Guard, the Border Patrol, the Customs Service, the Immigration and Naturalization Service (INS), the Secret Service and the Transportation Security Administration (TSA) – into one Department of Homeland Security (DHS) with roughly 170,000 employees.

Like USA PATRIOT, The Homeland Security Act expands government authority to collect and mine data on individuals and groups while at the same time limiting and removing public access to information about the government.

Title II of the Act establishes a Directorate for Information Analysis and Infrastructure Protection authorized to collect and analyze law enforcement and intelligence information from any federal agency as well as any "other information from…private sector entities" and to distribute that information to federal, state and local governments, and private businesses.

Among these "private sector entities" are Internet Service Providers, or ISPs. Under Section 225(d), such companies "may voluntarily turn over to the government the contents of e-mail communications" if they believe that an emergency…requires disclosure without delay." Although giving such information to the government is "voluntary," under the Act, civil libertarians point out that ISPs are unlikely to refuse a government request made in the context of what the government claims is an emergency.

While Fourth Amendment protections apply to the government, they do not apply to data in the hands of private industry. The provisions of Title II, therefore, free the government to collect information from private industry about anyone's purchases, banking, travel, and reading without any of the traditional safeguards (e.g., a warrant issued by a judge upon a demonstration of probable cause) put into place to prevent government harassment or overreaching.

But when it comes to citizens who seek information about the government, Title II has the opposite effect. It prevents the public from finding out about the risks and vulnerabilities associated with the country's infrastructure by exempting from disclosure under the federal Freedom of Information Act (FOIA) "all critical infrastructure information voluntarily submitted" to the agency."

USA PATRIOT broadly defines "critical infrastructure as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of these matters."

In the context of The Homeland Security Act, this definition allows the President and the Secretary of Homeland Security to designate almost any infrastructure as "critical" and therefore exempt.[4]

The department's effectiveness in improving safety and preventing terrorism attacks is open to question. Clark Kent Ervin, who was DHS Inspector General from December 2003 to December 2004, lost his job after criticizing the agency. He described it as a "dysfunctional, poorly-managed bureaucracy that has failed to plug serious holes in the nation's safety net."[5]

Among Ervin's findings while in office:

• Undercover investigators were able to sneak explosives and weapons past security screeners at 15 airports during tests in 2003.

• Federal air marshals, hired to provide a last line of defense against terrorists on airlines, slept on the job, tested positive for alcohol or drugs while on duty, lost their weapons and falsified information in 2002.

• Department leaders should have taken a more aggressive role in efforts to combine the government's myriad terrorist watch lists since the department was created in 2003.

• TSA gave executive bonuses of $16,477 to 88 of its 116 senior managers in 2003, an amount one-third higher than the bonuses given to executives at any other federal agency.

• TSA spent nearly $500,000 on an awards banquet for employees in November 2003. The cost included $1,500 for three cheese displays and $3.75 for each soft drink.[6]

On February 15, 2005, Michael Chertoff became the Bush Administration's second Director of the Department of Homeland Security. Chertoff, who headed the Justice Department's Criminal Division under John Ashcroft, is thought to have masterminded the government's post-9/11 round-up of hundreds of Middle Eastern, South Asian and African men who were held on the pretext of civil immigration violations. In the ensuing months, Chertoff also advised the Central Intelligence Agency on the legal limits of "interrogation techniques" in accordance with the White House Office of Legal Counsel's definition of torture as the infliction of pain "equivalent to organ failure or imminent death."

[4] Congressional Research Service Report for Congress," Homeland Security Act of 2002: Critical Infrastructure Information Act, February 28, 2003".

[5] "Ex-official Tells of Homeland Security Failures," by Mimi Hall, USA Today, December 28, 2004.

[6] Id.

B. Terror in the Courts: Federal Prosecutions since 9/11

Anyone studying federal terrorism prosecutions since the attacks of September 11 will notice a distinct pattern: federal law enforcement officials announce a "major arrest" in the "war on terror," emphasizing their investigative prowess, the dangerousness of their suspect and the idea that, because of his arrest, an attack has been averted. This announcement is followed by months, if not years, of legal bickering between defense attorneys and federal prosecutors who believe that, because they are conducting a "war on terror," they are free to operate outside constitutional and procedural rules and to ignore judicial orders.

As the bickering continues and the appeals are filed and the years go by, the accused, often classified as an "enemy combatant," languishes in solitary confinement. Often, this happens despite the fact that the accused has not been charged with a crime and the Constitution expressly forbids the government from depriving anyone of "life, liberty or property without due process of law."[7]

On June 28, 2004, the US Supreme Court handed down two decisions related to the detention of "enemy combatants." The first of these, *Hamdi v. Rumsfeld*,[8] held that "due process demands that a citizen held in the United States as an enemy combatant be given a meaningful opportunity to contest the factual basis for that detention before a neutral decisionmaker."

The *Hamdi* decision effectively relieved the Bush administration of its claim that "clear Supreme Court precedent" existed for its actions in classifying detainees as "enemy combatants" undeserving of both the basic rights conferred by the U.S. Constitution and the protections afforded to prisoners of war under the Geneva Conventions.[9]

The second case, *Rasul v. Bush*,[10] demolished the Bush administration's contention that U.S. courts have no jurisdiction over the military prison at Guantánamo Bay, Cuba, and decreed in no uncertain terms that "United States courts have jurisdiction to consider challenges to the legality of the detention of foreign nationals captured abroad in connection with hostilities and incarcerated at Guantánamo Bay."

One day later, on June 29, 2004, the Department of Defense announced that it had referred three "enemy combatants" who were jailed at Guantánamo Bay for trial by military

---

[7] Amendment 5, Bill of Rights

[8] *Hamdi v. Rumsfeld*, June 28, 2002.

[9] The administration's so-called "clear precedent" was a 1942 Supreme Court case, *Ex Parte Quirin*, which dealt with Nazi saboteurs, at least one of whom was a U.S. citizen. But in *Hamdi*, the Court said that "enemy combatants" are either lawful -- for example, the regular army of a belligerent country -- or unlawful -- for example, terrorists. When lawful combatants are captured, they are prisoners of war (POWs). As POWs, they cannot be tried (except for war crimes), they must be repatriated after hostilities are over, and they have only to provide their name, rank, and serial number if interrogated. Unlawful combatants are different, according to the Court's analysis. When unlawful combatants are captured, they are subject to trial by a military tribunal. This is what happened to the Nazi saboteurs in *Quirin*. But the president's executive order of November 2001 expressly excludes U.S. citizens from the purview of military tribunals.

[10] *Rasul v. Bush*, June 28, 2002.

commission pursuant to an executive order signed by President Bush in November of 2001. Two weeks after that, the department announced the referral of a third "enemy combatant" for trial by commissions. In the interim, it had announced the formation, in response to the Court's ruling in *Hamdi*, of the "Combatant Status Review Tribunal" or CSRT. The CSRT was to serve as the "neutral tribunal" before which detainees could challenge their classification as enemy combatants" in keeping with the Court's decision.

However, on November 8, 2004, U.S. District Court Judge James Robertson ruled that the CSRT violated the U.S. Constitution and the Geneva Conventions because its rules did not allow detainees to have the assistance of counsel.[11] Without counsel, Robertson ruled, the CSRT's procedures for determining detainee status could not be considered competent. And without competent procedures for determining detainee status, no detainee could be tried by a commission authorized to try only "enemy combatants."

In addition, Robertson ruled, the Bush administration acted improperly and in contravention to the Geneva Conventions by summarily denying prisoner of war status to an entire class of detainees. Under the Conventions, the judge maintained, no detainee can be tried by military commission as an "enemy combatant" unless and until "a competent tribunal" has determined that he is not entitled to the protections afforded to prisoners of war.

Robertson's opinion was followed by a contradictory decision, on Jan. 19, 2005, by U.S. District Court Judge Richard Leon of the D.C. Circuit.[12] Ruling in a lawsuit brought by seven Guantánamo detainees, Leon wrote that "no viable legal theory exists" by which they [the detainees] can contest their status in U.S. courts."

Two weeks later, on Jan. 31, 2005, U.S. District Court Judge Joyce Hens Green, also of the D.C. Circuit, issued a third opinion agreeing with Robertson.[13] The matter is now before the D.C. Circuit Court of Appeals.

Yaser Hamdi

Yaser Hamdi was an American citizen captured with pro-Taliban forces by the Northern Alliance in November of 2001 following the U.S. invasion of Afghanistan. Hamdi was designated an enemy combatant and taken to the military prison at Guantánamo Bay, Cuba. Once there, his status as an American citizen came to light and he was transferred first to the Navy brig in Norfolk, Va., and then to the Navy jail in Charleston, S.C.

Hamdi's classification as an "enemy combatant" specifically precluded the right to legal representation in U.S. courts. It also allowed the government to confine him "incommunicado" indefinitely without access to visitors or legal advice. But in May of 2002, Frank W. Dunham, Jr., the federal public defender for the Eastern District of Virginia, filed a habeas corpus petition on

---

[11] Salim Ahmad Hamdan v. Donald H. Rumsfeld, Civil Action No. 04-1519, U.S. District Court, Washington, D.C. Nov. 8, 2004.

[12] *Khalid v. Bush*, Civil Case No. 1:04-1142 (RJL), U.S. Disctrict Court for the District of Columbia, Jan. 19, 2005.

[13] *In re Guantánamo Detainee Cases*, Civil Action Nos. 02-CV-0299(CKK),02-CV-0828(CKK),02-CV-1130(CKK), 04-CV-1135 (ESH), 04-cv-1136 (JDB),04-CV-1137 (RMC),04-CV-1144(RWR),04-CV-1164(RBW),04-CV-1194 (HHK),04-CV-1227 (RBW),04-CV-1254(HHK). Jan 31, 2005.

Hamdi's behalf as Hamdi's "next friend." The petition challenged Hamdi's confinement on the basis of his classification as an enemy combatant.

The case landed in the Norfolk, Va. courtroom of U.S. District Court Judge Robert G. Doumar who ordered the government to respond to the petition and to allow Hamdi unmonitored visits with Dunham. The government immediately appealed to the U.S. Court of Appeals for the Fourth Circuit, which issued an order staying Doumar's ruling.

The Fourth Circuit subsequently held that the habeas petition was invalid because Dunham had no previous significant relationship with Hamdi and therefore lacked the legal standing to act as his next friend. In the meantime, however, Hamdi's father had filed a similar petition and Doumar had ruled again, ordering for a second time that Hamdi be allowed unmonitored meetings with his lawyer.

Again the government went to the Fourth Circuit and again the Fourth Circuit ruled in its favor. This time, the court agreed that Hamdi's father had legal standing to file as Hamdi's next friend, but ruled that Doumar's decision to grant Hamdi unmonitored attorney visits was "premature." The case was sent back to Doumar for a ruling on whether Hamdi, as an enemy combatant, retained the right to counsel guaranteed by the Sixth Amendment.

To this end, Doumar ordered the government to provide him with the "screening criteria" it used to decide that Hamdi was an enemy combatant. In addition, he demanded the names and addresses of those who made the designation and other related documents. These disclosures would not threaten national security, he assured the government, because he planned to view the documents, which would be delivered under seal and then returned to the government, alone in his chambers.

But prosecutors defied Doumar's order, asserting that the materials he requested were outside "the scope of proper inquiry." Instead, they asked him to dismiss the case based on the 9-paragraph affidavit of Michael Mobbs, whom they described as a "special advisor" to the Defense Department. According to this "Mobbs Declaration," Hamdi was "affiliated with a Taliban military unit and received weapons training." No accompanying evidence supported these claims.

This was not enough for Doumar. Noting that the Mobbs Declaration fell "far short" as a justification for Hamdi's detention, he ruled that no "meaningful judicial review" of Hamdi's status as an enemy combatant could take place without more evidence.

The government appealed to the Fourth Circuit, which reversed Doumar on Jan. 8, 2003, and ruled that the Mobbs Declaration "if accurate," provided a sufficient basis upon which to conclude that [Hamdi's] imprisonment was constitutional pursuant to the president's war powers. In announcing the decision, Attorney General John Ashcroft called it "an important victory for the president's ability to protect the American people in times of war." But the case wasn't over. The U.S. Supreme Court granted certiorari and, combining the case with that of accused shoebomber Jose Padilla, announced its opinion on June 28, 2004.[14]

[14] *Hamdi et al.* v. *Rumsfeld, Secretary of Defense, et al.*, No. 03-6696; *Rumsfeld, Secretary of Defense* v. *Padilla et al.*, No. 03-1027; *Rasul et al.* v. *Bush, President of the United States, et al.*, Nos. 03-334 and 03-343; all decided June 28, 2004.

The court ruled that, while the president has the authority to detain enemy forces captured in battle, he does not have the power to unilaterally declare American citizens to be "enemy combatants" and then to detain them indefinitely based on that classification with no recourse for challenging their detention. To do so, said the court, violates the Fifth Amendment's promise that no person may be deprived of liberty without "due process of law."

The justices further emphasized that the only legitimate reason for detaining enemy combatants without trial is to prevent them from returning to the battlefield while hostilities are ongoing. Under the traditions of both American and international law of war, they must be released once hostilities have ceased.

However, the court went on to say that the "neutral tribunal" to which detainees must be allowed to appeal did not have to be a federal court, but could instead be an "appropriately authorized and properly constituted" military commission. And in the interest of lessening the burden of such due process requirements on the executive branch of government, procedural rules might be relaxed in its favor. "Hearsay, for example, may need to be accepted as the most reliable available evidence from the Government in such a proceeding. Likewise, the Constitution would not be offended by a presumption in favor of the Government's evidence," wrote the Court.

In fact, the Court suggested, "a burden-shifting scheme" under which accused combatants would have to prove their innocence instead of the more traditional arrangement of making the government prove their guilt might also be helpful in terms of lightening the burden of due process on the executive branch. Although American troops remain in Afghanistan, hostilities there have officially ceased at least since the election of Afghani President Hamid Karzai in October 2004. In the meantime, both the Geneva Conventions and the U.S. Supreme Court's decision in *Hamdi v. Rumsfeld* expressly state that prisoners of war must be released upon the cessation of hostilities. Yet Hamdi and hundreds of others taken into custody by U.S. forces in Afghanistan remain behind the walls of American prisons at Guantánamo Bay and elsewhere.

The U.S has taken the position that all Afghan soldiers are enemy combatants and "terrorists" by virtue of having fought for a government that conspired to commit a terrorist act (i.e., knowingly harboring Osama bin Laden). Under this theory, these prisoners will remain "enemy combatants" and "terrorists" in the ongoing "war on terrorism" which has no foreseeable end. As if to underline this fact, the Bush administration began holding "combatant status review tribunals" for all 558 prisoners at Guantánamo following the Supreme Court's decision in *Hamdi*.

As of March 29, 2005, 520 of the 558 retained their classification as enemy combatants."[15] Because the tribunals were conducted in secret and the names of the detainees are withheld from the public, the determination of Hamdi's status by the tribunals is unknown.

Jose Padilla

On June 10, 2002, John Ashcroft announced from Moscow that the U.S. had a "made a significant step forward in the war on terrorism."[16] That step, said Ashcroft, was the capture and

[15] Combat Status Review Tribunal Summary. Available online at: http://www.defenselink.mil/news/Combatant_Tribunals.html

[16] Transcript of the Attorney General John Ashcroft Regarding the transfer of Abdullah Al Muhajir (Born Jose Padilla) To the Department of Defense as an Enemy Combatant June 10, 2002. Available online at: http://www.usembassy.it/file2002_06/alia/a2061010.htm

arrest of “a known terrorist who had been planning to build and explode a radiological dispersion device, or 'dirty bomb,' in the United States."[17] That “terrorist” was Jose Padilla.

In the weeks that followed, Secretary of Defense Donald Rumsfeld asserted that Padilla was “unquestionably involved in terrorist activities.”[18] Even President Bush weighed in, calling Padilla a “would-be killer” and observing to reporters that, “This guy Padilla is a bad guy.”

In fact, Padilla was an American citizen of Puerto Rican descent who had grown up in Chicago. He was arrested on May 8, 2002 at O’Hare International Airport after getting off a flight from Pakistan and taken to New York. Initially held as a material witness, he was declared an “enemy combatant” within days of his arrest. He was then transferred to the Navy’s prison near Charleston, South Carolina, where he was held without charges, in solitary confinement and with no access to his lawyer. Padilla remained in military custody for over three years.

U.S. District Court Judge Michael Mukasey was the first judge to weigh in on the Padilla case. Mukasey ruled that the government could detain Padilla as a material witness, but at the same time he appointed a lawyer to represent Padilla and ordered the government to give him access to her. It was after this decision that Padilla was declared an “enemy combatant” and taken to South Carolina. Both Padilla’s lawyer and the government appealed to the U.S. Court of Appeals for the Second Circuit.

In December of 2003, the Second Circuit ruled that Bush’s classification of Padilla as an “enemy combatant” was unlawful and ordered the government to either charge Padilla with a crime, take him into custody as a material witness or release him within 30 days. However, the Court then stayed its own ruling pending the government’s appeal to the U.S. Supreme Court. The Supreme Court agreed to hear the case on Feb. 20, 2004.

The following June, the Department of Justice held a press conference during which officials released a seven-page document entitled “Summary of Jose Padilla’s Activities with al Qaeda.”[19] According to the document, Padilla had confessed to investigators that he met repeatedly with senior leaders of al Qaeda, including Lieutenant Khalid Shaikh Mohammed, the mastermind of the Sept. 11, 2001 attacks. Mohammed had assigned Padilla and an unidentified accomplice to blow up apartment buildings in various U.S. cities and discussed with him the possibility of detonating a nuclear bomb, the document said. Padilla, it alleged, claimed he could build such a bomb in his basement using instructions from the Internet.

Had Padilla been prosecuted in a court of law, Deputy Attorney General James B. Comey Jr. told reporters at the press conference, he "would likely have ended up a free man" because his attorney would have advised him to tell authorities nothing. It was only because he had instead been classified as an “enemy combatant” that the government was able to interrogate and incarcerate him as it saw fit.

“We have decided to release this information to help people understand why we are doing what we are doing in the war on terror and to help people understand the nature of the threat we

---

[17] Id.

[18] “Lawyer: Dirty Bomb Suspect’s Rights Violated,” CNN.com, June 11, 2002. Available online at: http://archives.cnn.com/2002/US/06/11/dirty.bomb.suspect/

[19] “U.S. Details Case Against Terror Suspect,” by Dan Eggen, *The Washington Post*, June 2, 2004.

face," Comey said. Three weeks later, the Supreme Court dismissed Padilla's petition on a technicality.

On Feb 28, 2005, a U.S. District judge in Spartanburg, S.C. again ordered the government to either charge Padilla or release him. In his 23-page opinion containing this ultimatum, U.S. District Court Judge Henry Floyd, a Bush appointee, made short work of the administration's position that the president's executive powers during wartime authorize him to deprive citizens of their constitutional rights at will by classifying them as "enemy combatants."

"Certainly Respondent does not intend to argue here that, just because the President states that Petitioner's detention is "consistent with the laws of the United States, including the Authorization for Use of Military Force, that makes it so," wrote the judge. "Not only is such a statement in direct contravention to the well settled separation of powers doctrine, it is simply not the law. Moreover, such a statement is deeply troubling. If such a position were ever adopted by the courts, it would totally eviscerate the limits placed on Presidential authority to protect the citizenry's individual liberties."[20]

The government promptly appealed Judge Floyd's decision. In June 2005, the ACLU submitted an amicus brief on Padilla's behalf arguing that the indefinite military detention of Padilla violates the core constitutional principles of due process of law and the supremacy of civilian authority over military. On September 9, 2005, the Fourth Circuit Court of Appeals reversed the trial court's decision and held that the president was authorized to detain "enemy combatants" under the Authorization of Use of Military Force passed by Congress in the wake of September 11. Padilla then filed a petition for cert in the United States Supreme Court. The Supreme Court will consider Padilla's petition on January 13, 2006.

In what some might call a tactical move to avoid having the Supreme Court hear Padilla's case, the government decided to file criminal charges against Padilla in civilian court. Because of the pending habeas corpus appeal, the government was required to seek permission from the Fourth Circuit to transfer Padilla's custody from military to civilian authority. In late December 2005, the Fourth Circuit denied the government's motion to transfer Padilla as well as the motion to withdraw the appellate court's previous opinion issued on September 9. The government appealed the case to the Supreme Court, which ruled on January 4, 2006 that Padilla could be transferred to Justice Department custody.

On January 5, Padilla made his first court appearance in Miami, Florida before U.S. Magistrate Judge Barry L. Garber. Judge Garber set hearings for the criminal trial to begin on January 12.

[20] *Padilla v. Hanft*, U.S. District Court for the District of South Carolina, Charleston Division, CIVIL ACTION NO. 2:04-2221-26AJ, Feb 28, 2005. Available online at http://scd.uscourts.gov/Padilla/images/000000/48.pdf

C. PATRIOT ACT II and Related legislation

In February of 2002, less than two years after Congress passed USA PATRIOT and right before the U.S. invasion of Iraq, the Center for Public Integrity published a leaked draft of a bill called "The Domestic Security Enhancement Act of 2003." Written and conceived by then-Attorney General John Ashcroft and his staff, this bill detailed a comprehensive expansion of USA PATRIOT, which, it is suspected, the administration was keeping under wraps until U.S. troops were on the ground in Iraq. At that point, according to this theory, the administration planned to exploit the crisis engendered by the war to ram the legislation through Congress without debate – just as it did with USA PATRIOT in the aftermath of the 9/11 terror attacks.

But the leaked draft, soon to be dubbed "PATRIOT II," provoked such a furor among constitutional scholars, civil rights groups and the public that the administration was forced, as a matter of public relations, to abandon its plan. "PATRIOT II, described by one legal expert as "a wholesale assault on privacy, free speech and freedom of information,"[21] gave the government broad new powers of surveillance, eliminating the nominal and largely symbolic judicial oversight provided for under USA PATRIOT.

The bill expanded the Justice Department's control over immigration matters by criminalizing minor immigration violations and expanding its deportation and extradition powers. It called for the creation of a DNA database of people suspected of association with terrorism or terrorist groups. It codified the administration's refusal to release information to the public about "war on terror" detainees. And it authorized the Justice Department to strip Americans of their citizenship for belonging to any groups designated by the department as "terrorist."

The administration abandoned "PATRIOT II," but only in name. Beginning in the spring of 2003, Ashcroft and Bush began publicly complaining about "weaknesses" and "loopholes" in USA PATRIOT "which terrorists could exploit, undermining our defenses."[22] Soon afterwards, various "PATRIOT II" provisions started resurfacing in Congress, some as riders attached to, or inserted into, other bills; some as new bills introduced under new, Patriotic-sounding titles.

"It appears we are witnesses to a stealth enactment of the enormously unpopular 'PATRIOT II' legislation that was first leaked months ago," observed Congressman Ron Paul of Texas. "Perhaps the national outcry when a draft of the PATRIOT II act was leaked has led its supporters to enact it, one piece at a time, in secret."

At the time, Paul was speaking of the innocuously-named "Intelligence Authorization Act for Fiscal Year 2004." Typically, a bill so named, although massive, does little more than allocate funds to cover the intelligence activities of the federal government. But this bill, which had sailed through Congress in November 2003, dramatically expanded the already-considerable powers bestowed on the government by PATRIOT Act. It did this by redefining the term, "financial institution" to include casinos, stockbrokers, car dealerships, credit card companies, insurance agencies, the U.S. Post Office, jewelers, airline companies and any other business "whose cash transactions have a high degree of usefulness in criminal, tax, or regulatory matters."

The effect of this change was to infinitely expand the kinds of businesses from which federal agents can demand information without seeking court approval. Under USA PATRIOT,

[21] "PATRIOT II, The Sequel: Why It's Even Scarier than the First PATRIOT Act," by Anita Ramasastry, *Findlaw News*, Feb. 17, 2003.

[22] Statement by Attorney General John Ashcroft, June 5, 2003.

the definition limited agents to traditional financial institutions like banks and credit unions. Now, since the passage of the "Intelligence Authorization Act for Fiscal Year 2004," any business dealing in cash transactions is legally obliged to provide any information sought in a National Security Letter from federal agents and to keep secret the fact that such a letter was sent.

This bill gave the executive branch sweeping new powers, yet the change was barely noticed. There were no public hearings in Congress and no floor debates.

More bills would follow. Some passed and became law:

"The Pretrial Detention and Lifetime Supervision of Terrorists Act of 2003," allowing the government to abduct and detain indefinitely, without charges or trial, people all over the world. This bill (H.R. 10) was passed by the House, then added to S. 2845, and passed into law on Dec. 17, 2004 as the National Intelligence Reform Act of 2004 (P.L. 108-458, see below).

P.L. 108-458: "The Intelligence Reform and Terrorism Prevention Act of 2004," amending the definition of "agent of a foreign power" in the Foreign Intelligence Surveillance Act (FISA) to include a "lone wolf provision" under which a non-United States person who engages in international terrorism or activities in preparation for international terrorism is deemed to be an "agent of a foreign power" under FISA. The act amends the definition of "financial institution" to include stockbrokers, car dealerships, casinos, credit card companies, insurance agencies, jewelers, airlines, the U.S. Post Office, and any other businesses "whose cash transactions have a high degree of usefulness in criminal, tax, or regulatory matters. Gets rid of the requirement in Section 215 of USA PATRIOT that the FBI must report to Congress regarding how often its agents send National Security Letters.

"The Real ID Act of 2005," making it easier for the government to send asylum-seekers back to the countries they fled if they cannot provide written "corroboration" of their claims. This act allows the government to deport anyone who provides support – even non-violent, humanitarian support – to an organization the government labels as "terrorist," and forces states to deny drivers' licenses to undocumented immigrants. On May 11, 2005, Congress passed the "Real ID" Act as part of a supplemental appropriations bill (P.L. 109-13).

Other bills died in Congress or had provisions interspersed into other legislation:

H.R. 2934, S. 1604: The "Terrorist Penalties Enhancement Act of 2003," expanding the federal death penalty to acts defined by the PATRIOT Act as "terrorism" that are federal crimes punishable by more than one year in prison. In addition to creating twenty-three separate new death penalties in one stroke, the bill also creates an unprecedented "catch-all" death penalty for any federal crime, or any attempt or conspiracy to commit such a crime that meets the PATRIOT Act's overbroad definition of terrorism and is punishable by more than one year in prison.

S. 410: The Foreign Intelligence Collection Improvement Act of 2003," including The Home-land Intelligence Agency Act of 2003 and The Foreign Intelligence Surveillance Public Reporting Act," amending FISA reporting requirements with respect to electronic surveillance and physical searches. Also requires reporting of "significant interpretations" and authorizes government agents to infiltrate "religious and political groups for foreign intelligence and international terrorism purposes."

The "Clear Law Enforcement for Criminal Alien Removal Act of 2003," mandating the enforcement of immigration law by state and local police and the inclusion of the names of civil immigration violators in the "National Crime Information Center" database given to police.

HR 100: "The Citizens and Legal Immigration Act," providing for the secret surveillance of non-citizens not connected to terrorist groups (sec. 2001) and expanding "national security" surveillance - surveillance approved by a secret court without probable cause of crime - to include any non-citizen (other than a lawful permanent resident) who is suspected of involvement in terrorism even if not connected to any foreign government or terrorist group.

S2679, HR3179: "The Antiterrorism Tools Enhancement Act of 2003," allowing the government to seize records and compel testimony in terror cases by bypassing grand juries and the already nominal judicial oversight provided for in USA PATRIOT. Other provisions include:

- The expansion of secret eavesdropping and search powers not involving a "foreign power" in intelligence cases that are not subject to the stricter safeguards of eavesdropping and searches in criminal cases (sec. 102);
- A requirement that federal judges hear, in secret, government requests for permission to delete classified information from documents to be provided to the defense (sec. 108);
- Authorization for the secret use of secret evidence derived from intelligence intercepts and searches in immigration cases (sec. 109);
- A broadening of the federal death penalty to include any crime that meets the USA PATRIOT Act's overly vague definition of terrorism a death-eligible offense, if death results (sec. 110);
- Redefines the crime of "material support of terrorism" so that association with an organization labeled a terrorist organization by the government is a criminal offense.

The "Vital Interdiction of Criminal Terrorist Organizations (VICTORY) Act of 2003," creating new administrative authority to seize documents without even the pro forma judicial oversight contained in USA PATRIOT, and to compel the testimony of witnesses in cases unrelated to a foreign power, with no probable cause of a crime. The VICTORY Act further contains a provision allowing the government to present illegally-obtained wiretap evidence in a court of law when the government acted "in good faith" while obtaining it and creates the new crime of "narco-terrorism" defined as the sale of any controlled substance "if the seller knew or should have known" that proceeds from the sale would benefit a terrorist group. Due to negative publicity, this particular act seemed to disappear. Instead, various provisions from this act were dispersed to other bills for consideration.

V. Background Documents & Online Resources for Keeping Current

A. USA Patriot Act

Most current information on the Patriot Act: http://blog.reformthepatriotact.org/

"United and Strengthening America By Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Public Law 107-56-Oct. 26, 2001. Available online at: http://www.epic.org/privacy/terrorism/hr3162.html

Report for Congress, "Terrorism: Section by Section Analysis of the USA PATRIOT Act," by Charles Doyle, Congressional Research Services, December 10, 2001. Available online at: http://www.epic.org/privacy/terrorism/usapatriot

Report for Congress, "The USA PATRIOT Act: A Legal Analysis for Congress," by Charles Doyle, Congressional Research Services, April 15, 2002. Available online at: http://www.epic.org/privacy/terrorism/usapatriot

"A Year of Loss: Reexamining Civil Liberties Since 9/11," A Report by the Lawyers' Committee for Human Rights. http://www.humanrightsfirst.org/us_law/loss/imbalance/imbalance.htm

"Imbalance of Powers: How Changes to U.S. Law & Policy Since 9/11 Erode Human Rights and Civil Liberties," A Report by the Lawyers' Committee for Human Rights. Available online at: http://www.humanrightsfirst.org/us_law/loss/imbalance/imbalance.htm

"Assessing the New Normal: Liberty and Security for the Post-September 11 United States," A Report by the Lawyers' Committee for Human Rights. Available online at: http://www.humanrightsfirst.org/us_law/loss/assessing/assessingnewnormal.htm

"A Guide to the USA PATRIOT Act and Federal Executive Orders," Bill of Rights Defense Committee. Available online at**:** http://www.bordc.org/resources/repeal.pdf

"UnPATRIOTic Acts: The Justice Department's Power to Rifle through Your Records and Personal Belongings without Telling You, American Civil Liberties Union. Available online at: http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=13246&c=206

"Seeking Truth From Justice: PATRIOT Propaganda - The Justice Department's Campaign to Mislead The Public About the USA PATRIOT Act," American Civil Liberties Union. Available online at: http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=13099&c=207

"Insatiable Appetite: The Government's Demand for New and Unnecessary Powers After September 11," American Civil Liberties Union. Available online at: http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=10623&c=207

"EFF Analysis of The Provisions of the USA PATRIOT Act That Relate to Online Activities," Electronic Frontier Foundation, Updated Oct. 27, 2003. Available online at: www.eff.org/Privacy/Surveillance/Terrorism/20011031_eff_usa_patriot_analysis.php

"Forfeiting Enduring Freedom for Homeland Security: A Constitutional Analysis of the USA PATRIOT Act of 2001 and the Justice Department's Anti-Terrorism Initiatives," The Rutherford Institute, January 2002.
http://64.227.78.173/documents/pdf/tri%5Fanalysis%5Fof%5Fusa%5Fpat%5Fact.pdf

Website: Watching Justice: "An Eye on the Department of Justice."
http://www.watchingjustice.org/issues/issue.php?docId=53

Website: The Federation of American Scientists Project on Government Secrecy
http://www.fas.org/main/content.jsp?formAction=325&projectId=5

B. Not Just the Patriot Act: Other Threats to Liberty since 9/11

The White House: Statements, press releases, documents and index of government information
Available online at: www.whitehouse.gov

The National Archives: Executive Orders Disposition Tables: January 8, 1937 – May 12, 2005
Online at: http://www.archives.gov/federal_register/executive_orders/disposition_tables.html

Federation of American Scientists: Intelligence Resource Program: Executive Orders.
Available online at: http://fas.org/irp/offdocs/eo/

Report for Congress, "Homeland Security Act of 2002: Critical Infrastructure Information Act," by Gina Marie Stevens, Congressional Research Services, February 28, 2003.
Available online at: http://www.fas.org/sgp/crs/RL31762.pdf

"The Dept. of Homeland Security," SourceWatch: Center for Media and Democracy. Available online at: http://www.sourcewatch.org/index.php?title=Office_of_Homeland_Security

The Center for Public Integrity: Online at www.publicintegrity.org

ContractWatch.org: http://www.contractwatch.org/index.htm

"Behind The Homefront: A daily chronicle of news in homeland security and military operations affecting newsgathering, access to information and the public's right to know."
Available online at: http://www.rcfp.org/behindthehomefront/archive/2005_02.html

"Homefront Confidential: How the War on Terrorism Affects Access to Information and the Public's Right to Know", Reporters Committee for Freedom of the Press, September 2004
Available online at: http://www.rcfp.org/homefrontconfidential/index.html

"Secrecy in the Bush Administration," Report Prepared for Rep. Henry A. Waxman by the United States House of Representatives Committee on Government Reform Minority Staff Special Investigations Division.
Available Online at: http://www.fas.org/sgp/library/waxman.pdf

BushSecrecy.org, a project by Public Citizen. Online at: http://www.bushsecrecy.org/intro.cfm

"Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement," by Chris Jay Hoofnagle, 29 N.C.J. Int'l L. L.& Com. Reg. 595 (Summer 2004). Available online at www.epic.org/privacy/choicepoint

"No Place to Hide," by Robert O'Harrow, Jr., Free Press, Copyright 2005 (see also: http://www.noplacetohide.net)

"The Surveillance-Industrial Complex: How the American Government Is Conscripting Businesses and Individuals in the Construction of a Surveilliance Society," A Report by The American Civil Liberties Union, Written by Jay Stanley, August 2004. Available online at: http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=16226&c=282.

"Bigger Monster, Weaker Chains: The Growth of The American Survellance Society," A Report by The American Civil Liberties Union, Written by Jay Stanley and Barry Steinhardt, January 2003. Available online at: http://www.aclu.org/Privacy/Privacy.cfm?ID=11573&c=39.

Report for Congress, "Privacy: Total Information Awareness Programs and Related Information Access, Collection, and Protection Laws," by Gina Marie Stevens, Congressional Research Services, March 21, 2003. Available online at: http://www.fas.org/irp/crs/RL31730.pdf

Report for Congress, "Interstate Travel: Constitutional Challenges to the Identification Requirement and Other Transportation Security Regulations," by Todd B. Tatelman, Congressional Research Services, December 21, 2004. Available online at: http://www.fas.org/sgp/crs/RL32664.pdf

"PATRIOT Act II Analysis," Electronic Frontier Foundation, available online at: http://www.eff.org/Censorship/Terrorism_militias/patriot-act-II-analysis.php

"ACLU Interested Person Memo Updating the Status of Pieces of PATRIOT II Proposal," October 8, 2003. Available online at: http://www.aclu.org/SafeandFree/safeandfree.cfm?ID=14000&c=206