Note: Hypertext and text-only copy of the complete draft of the "Domestic Security Enhancement Act of 2003," is available here on ratical.org. Each section cited below is linked to its text section in the draft source. References to the USA 'PATRIOT' Act are likewise linked to local copy of their respective text sections of the law.

Section-by-Section Analysis of Justice Department draft

"Domestic Security Enhancement Act of 2003," also known as "PATRIOT Act II"

American Civil Liberties Union

14 February 2003

To: Interested Persons
From: Timothy H. Edgar, Legislative Counsel
Date: February 14, 2003
Re: Section-by-Section Analysis of Justice Department draft "Domestic Security Enhancement Act of 2003," also known as "Patriot Act II"

The Department of Justice (DOJ) has been drafting comprehensive anti-terrorism legislation for the past several months. The draft legislation, dated January 9, 2003, grants sweeping powers to the government, eliminating or weakening many of the checks and balances that remained on government surveillance, wiretapping, detention and criminal prosecution even after passage of the USA PATRIOT Act, Pub. L. No. 107-56, in 2001.

Among its most severe problems, the bill

Diminishes personal privacy by removing checks on government power, specifically by

- Making it easier for the government to initiate surveillance and wiretapping of U.S. citizens under the authority of the shadowy, top-secret Foreign Intelligence Surveillance Court. (Sections 101, 102 and 107)
- Permitting the government, under certain circumstances, to bypass the Foreign Intelligence Surveillance Court altogether and conduct warrantless wiretaps and searches. (Sections 103 and 104)
- Sheltering federal agents engaged in illegal surveillance without a court order from criminal prosecution if they are following orders of high Executive Branch officials. (Section 106)
- Creating a new category of "domestic security surveillance" that permits electronic eavesdropping of entirely domestic activity under looser standards than are provided for ordinary criminal surveillance under Title III. (Section 122)
- Using an overbroad definition of terrorism that could cover some protest tactics such as those used by Operation Rescue or protesters at Vieques Island, Puerto Rico as a new predicate for criminal wiretapping and other electronic surveillance. (Sections 120 and 121)
- Providing for general surveillance orders covering multiple functions of high tech devices, and by further expanding pen register and trap and trace authority for intelligence surveillance of United States citizens and lawful permanent residents. (Sections 107 and 124)

- Creating a new, separate crime of using encryption technology that could add five years to any sentence for crimes committed with a computer. (Section 404)
- Expanding nationwide search warrants so they do not have to meet even the broad definition of terrorism in the USA PATRIOT Act. (Section 125)
- Giving the government secret access to credit reports without consent and without judicial process. (Section 126)
- Enhancing the government's ability to obtain sensitive information without prior judicial approval by creating administrative subpoenas and providing new penalties for failure to comply with written demands for records. (Sections 128 and 129)
- Allowing for the sampling and cataloguing of innocent Americans' genetic information without court order and without consent. (Sections 301-306)
- Permitting, without any connection to anti-terrorism efforts, sensitive personal information about U.S. citizens to be shared with local and state law enforcement. (Section 311)
- Terminating court-approved limits on police spying, which were initially put in place to prevent McCarthy-style law enforcement persecution based on political or religious affiliation. (Section 312)
- Permitting searches, wiretaps and surveillance of United States citizens on behalf of foreign governments -- including dictatorships and human rights abusers -- in the absence of Senate-approved treaties. (Sections 321-22)

Diminishes public accountability by increasing government secrecy; specifically, by

- Authorizing secret arrests in immigration and other cases, such as material witness warrants, where the detained person is not criminally charged. (Section 201)
- Threatening public health by severely restricting access to crucial information about environmental health risks posed by facilities that use dangerous chemicals. (Section 202)
- Harming fair trial rights for American citizens and other defendants by limiting defense attorneys from challenging the use of secret evidence in criminal cases. (Section 204)
- Gagging grand jury witnesses in terrorism cases to bar them from discussing their testimony with the media or the general public, thus preventing them from defending themselves against rumor-mongering and denying the public information it has a right to receive under the First Amendment. (Section 206)

Diminishes corporate accountability under the pretext of fighting terrorism; specifically, by

- Granting immunity to businesses that provide information to the government in terrorism investigations, even if their actions are taken with disregard for their customers' privacy or other rights and show reckless disregard for the truth. Such immunity could provide an incentive for neighbor to spy on neighbor and pose problems similar to those inherent in Attorney General Ashcroft's "Operation TIPS." (Section 313)

Undermines fundamental constitutional rights of Americans under overbroad definitions of "terrorism" and "terrorist organization" or under a terrorism pretext; specifically by

- Stripping even native-born Americans of all of the rights of United States citizenship if they provide support to unpopular organizations labeled as terrorist by our government, even if they support only the lawful activities of such organizations, allowing them to be indefinitely imprisoned in their own country as undocumented aliens. (Section 501)
- Creating 15 new death penalties, including a new death penalty for "terrorism" under a definition which could cover acts of protest such as those used by Operation Rescue or protesters at Vieques Island, Puerto Rico, if death results. (Section 411)
- Further criminalizing association -- without any intent to commit specific terrorism crimes -- by broadening the crime of providing material support to terrorism, even if support is not given to any organization listed as a terrorist organization by the government. (Section 402)
- Permitting arrests and extraditions of Americans to any foreign country -- including those whose governments do not respect the rule of law or human rights -- in the absence of a Senate-approved treaty

and without allowing an American judge to consider the extraditing country's legal system or human rights record. (Section 322)

Unfairly targets immigrants under the pretext of fighting terrorism; specifically by

- Undercutting trust between police departments and immigrant communities by opening sensitive visa files to local police for the enforcement of complex immigration laws. (Section 311)
- Targeting undocumented workers with extended jail terms for common immigration offenses. (Section 502)
- Providing for summary deportations without evidence of crime, criminal intent or terrorism, even of lawful permanent residents, whom the Attorney General says are a threat to national security. (Section 503)
- Completely abolishing fair hearings for lawful permanent residents convicted of even minor criminal offenses through a retroactive "expedited removal" procedure, and preventing any court from questioning the government's unlawful actions by explicitly exempting these cases from habeas corpus review. Congress has not exempted any person from habeas corpus -- a protection guaranteed by the Constitution -- since the Civil War. (Section 504)
- Allowing the Attorney General to deport an immigrant to any country in the world, even if there is no effective government in such a country. (Section 506)

Given the bipartisan controversy that has arisen in the past from DOJ's attempts to weaken basic checks and balances that protect personal privacy and liberty, the DOJ's reluctance to share the draft legislation is perhaps understandable. The DOJ's highly one-sided section-by-section analysis reveals the Administration's strategy is to minimize far-reaching changes in basic powers, as it did in seeking passage of the USA PATRIOT Act, by characterizing them as minor tinkering with statutory language designed to bring government surveillance authorities, detention and deportation powers, and criminal penalties "up to date."

This ACLU section-by-section analysis of the text of the legislation, however, reveals that the DOJ's modest descriptions of the powers it is seeking, and the actual scope of the authorities it seeks, are miles apart. The USA PATRIOT Act undercut many of the traditional checks and balances on government power. The new draft legislation threatens to fundamentally alter the constitutional protections that allow us as Americans to be both safe and free. If adopted, the bill would diminish personal privacy by removing important checks on government surveillance authority, reduce the accountability of government to the public by increasing government secrecy, further undermine fundamental constitutional rights of Americans under an already overbroad definition of "terrorism," and seriously erode the right of all persons to due process of law.

Our detailed section-by-section analysis follows.

Title I -- Diminishing Personal Privacy by Removing Checks on Government Intelligence and Criminal Surveillance Powers

Title I amends critical statutes that govern intelligence surveillance and criminal surveillance. Both forms of surveillance are subject to Fourth Amendment limitations. *See Katz v United States*, 389 U.S. 347 (1967) (criminal surveillance); *United States v United States District Court ("Keith")*, 407 U.S. 297 (1972) (intelligence surveillance). Yet while traditional searches are governed by warrant procedures largely drawn from the common law, wiretapping and other forms of electronic surveillance are governed by standards and procedures embodied in two federal statutes that respond to *Katz* and *Keith* -- Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 28 U.S.C. §§ 2510-22, which governs surveillance of criminal suspects, and the Foreign Intelligence Surveillance Act of 1978 (FISA), 50 U.S.C. §§ 1801-63 which governs surveillance of foreign powers and agents of a foreign power for intelligence purposes.

Making it easier for the government to initiate surveillance and wiretapping, including of United States citizens and lawful permanent residents, through the secret Foreign Intelligence Surveillance Court (Sections 101-111).

The draft bill's proposed amendments to FISA attack key statutory concepts that are critical to providing appropriate limits and meaningful judicial supervision over wiretapping and other intrusive electronic surveillance for intelligence purposes. These limits were approved by Congress in 1978 because of a history of abuse by government agents who placed wiretaps and other listening devices on political activists, journalists, rival political parties and candidates, and other innocent targets. These so-called "national security wiretaps" and other covert surveillance were undertaken without any court supervision and without even the slightest suspicion that the targets of such surveillance were involved in criminal activities or were acting on behalf of any foreign government or political organization. This pattern of abuse culminated in the crimes of Watergate, which led to substantial reforms and limits on spying for intelligence purposes.

FISA represented a compromise between civil libertarians, who wanted to ban "national security wiretaps" altogether, and apologists for Presidential authority, who claimed such unchecked intelligence surveillance authority was inherent in the President's Article II power over foreign relations. The Congress chose to authorize intelligence wiretaps without evidence of crime, subject to a number of key restraints. One of these restraints, separating intelligence gathering from criminal investigations, has been significantly weakened by the USA PATRIOT Act. The USA PATRIOT Act abolished the "primary purpose" test -- the requirement that FISA surveillance could only be used if the primary purpose of surveillance was gathering of foreign intelligence, and not criminal prosecution or some other purpose.

The draft bill eliminates or substantially weakens a number of the remaining constraints on intelligence surveillance approved by Congress. Taken as a whole, these changes go a long way to undermine limits on intelligence surveillance essential to preserving civil liberties and to preventing a repeat of the wiretapping abuses of the J. Edgar Hoover and Watergate eras.

Authorizing the government to initiate wiretaps and other electronic surveillance on Americans who have no ties to foreign governments or powers (sec. 101).

This section would permit the government to obtain a wiretap, search warrant or electronic surveillance orders targeting American citizens and lawful permanent residents even if they have no ties to a foreign government or other foreign power. Under FISA, the government need not show, in many circumstances, probable cause that the target of a wiretap is involved in any criminal activity. FISA requires an alternate showing -- probable cause that the target is acting on behalf of a foreign government or organization, i.e., a "foreign power." Section 101 of the draft bill eliminates this requirement for individuals, including United States citizens, suspected of engaging in "international terrorism." It does so by redefining individuals, including United States citizens or lawful residents, as "foreign powers" even if they are not acting on behalf of any foreign government or organization. The "foreign power" requirement was a key reason FISA was upheld in a recent constitutional challenge. *See In re Sealed Case No. 02-001*, slip op. at 42 (Foreign Intelligence Surveillance Ct. of Rev. Nov. 18, 2002) (while FISA requires no showing of probable cause of crime, it is constitutional in part because it provides "another safeguard . . . that is, the requirement that there be probable cause to believe the target is acting 'for or on behalf of a foreign power.'") [1]

Permitting surveillance of the lawful activities of United States citizens and lawful permanent residents if they are suspected of gathering information for a foreign power (sec. 102).

United States citizens and lawful permanent residents who are not violating any law should not be subject to wiretapping or other intrusive electronic surveillance. The FISA contains dual standards for non-U.S. persons and for U.S. persons with respect to surveillance of "intelligence gathering activities," i.e., the gathering of information for a foreign government or organization. These standards reflect the judgment of Congress that U.S. persons should not face electronic surveillance unless their activities "involve or may involve" some violation of law (as, for example, would certainly be the case with respect to any activity in furtherance of terrorism or other crime). For non-U.S. persons, this showing does not have to be made, i.e., the gathering of information by foreign persons for foreign powers is enough to trigger FISA. The draft bill (at section 102) applies the lower standard to U.S. persons.

Lawful gathering of information for a foreign organization does not necessarily pose any threat to national security. This amendment would permit electronic surveillance of a local activist who was preparing a report on human rights for London-based Amnesty International, a "foreign political organization," even if the activist was not engaged in any violation of law. By eliminating this need to show some violation of law may be involved before authorizing surveillance of U.S. persons, Congress could well succeed in rendering FISA unconstitutional, by eliminating another key reason FISA was upheld in a recent court challenge. See *In re Sealed Case No. 02-001*, slip op. at 42 (Foreign Intelligence Surveillance Ct. of Rev. Nov. 18, 2002) (holding that FISA surveillance of U.S. persons meets Fourth Amendment standards in part because a surveillance order may not be granted unless there is probable cause to believe the target is involved in activity that may involve a violation of law).

Permitting the government, under some circumstances, to bypass the Foreign Intelligence Surveillance Court altogether (Sections 103, 104).

Section 103 gives the Attorney General the power to authorize intelligence wiretaps and other electronic surveillance without permission from any court, including the Foreign Intelligence Surveillance Court, for fifteen days, after an attack on the United States or force authorization resolution from the Congress. Under existing federal statutes, a formal declaration of war by the Congress triggers a host of civil liberties consequences, including authorization by the Attorney General to engage in intrusive electronic surveillance for up to fifteen days without any court order at all. The draft bill expands this power dramatically by eliminating judicial review for any surveillance under FISA for a period up to fifteen days pursuant to (1) an authorization of force resolution by the Congress or (2) a "national emergency" created by an attack on the United States. For surveillance under the latter circumstance, no action by Congress would be required. Once the President has unilaterally decided such an attack has occurred, the Attorney General could unilaterally decide what constitutes an "attack" on the United States, creating an emergency that justifies what would otherwise be plainly illegal wiretaps.

DOJ's rationale for this change is that declarations of war are rare and the statute should be updated to reflect this. This argument fundamentally misconstrues the purpose of this provision. The normal FISA process, including review by the Foreign Intelligence Surveillance Court, was Congress's attempt to impose meaningful limits over national security surveillance conducted without a formal declaration of war and for continuing threats that cannot easily by defined by reference to traditional war powers. To use Congress' grant of surveillance authority following a declaration of war as an argument to permit surveillance even in the absence of such action by Congress is a fundamental intrusion on Congress's war powers.

The draft bill (at section 104) also expands special surveillance authority, available for up to a year with no court order at all, for property "under the open and exclusive control of a foreign power" by permitting eavesdropping on "spoken communications." This expansion of authority leaves intact the current requirement that such surveillance can go forward only if the Attorney General certifies under oath that "there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party." Still, the new authority would plainly involve eavesdropping on communications protected by the Fourth Amendment, as it would inevitably result in listening -- without any court order -- to the conversations in the United States of anyone who might be using telephones, computers, or other devices owned by a foreign government, political organization, or company owned by a foreign government.

There are serious questions about whether the secret review of surveillance orders by the Foreign Intelligence Surveillance Court, which by its nature can only hear the government's side of the case, is effective in protecting Americans' civil liberties. These amendments would bypass judicial review under FISA altogether.

Sheltering federal agents engaged in illegal surveillance without a court order from criminal prosecution if they are following orders of high Executive Branch officials (Section 106).

This section would encourage unlawful intelligence wiretaps and secret searches by immunizing agents from criminal sanctions if they conduct such surveillance, even if a reasonable official would know it is illegal, by claiming they were acting in "good faith" based on the orders of the President or the Attorney General. In order to ensure that FISA was successful in bringing national security surveillance under the rule of law, Congress not only provided a process for legal intelligence surveillance, but also imposed criminal penalties on any government agent who engages in electronic surveillance outside that process. Congress also provided a "safe harbor" for agents who engaged in surveillance that was approved by the Foreign Intelligence Surveillance Court, even if such surveillance was not in fact authorized by FISA. The draft bill (at section 106) substantially undercuts the deterrent effect of criminal sanctions for illegal wiretaps or electronic surveillance by expanding the "safe harbor" to include surveillance not approved by any court, but simply on the authorization of the Attorney General or the President.

Of course, the very spying abuses FISA was designed to prevent were undertaken with the authorization of high-ranking government officials, including the President. For example, President Nixon authorized just such a covert search of the Brookings Institution, whom he and his staff suspected of possessing classified information that had been leaked to the press. As described by Nixon biographer Richard Reeves:

> Nixon sat up. "Now if you remember Huston's plan [to engage in covert surveillance] . . ."
>
> "Yeah, why?" Haldeman said.
>
> Kissinger said: "But couldn't we go over? Now, Brookings has no right to classified("
>
> The President cut him off, saying, "I want it implemented. . . . Goddamit get in there and get those files. Blow the safe and get them." [2]

Any government official acting within the scope of his employment already enjoys "qualified immunity" from charges of violating Fourth Amendment or other constitutional rights -- i.e., an official cannot be punished or held civilly liable if a reasonable government official would not have known his or her conduct was illegal. *See Harlow v Fitzgerald*, 457 U.S. 800, 818 (1982). Providing additional protection to government officials who engage in wiretaps or searches without a court order, where a reasonable official would know those wiretaps or searches were clearly illegal, would take away any incentive for such officials to question an illegal authorization by the President, Attorney General or other high official.

Further expanding pen register and trap and trace authority for intelligence surveillance of United States citizens and lawful permanent residents beyond terrorism investigations (Section 107).

This section allows the government to use intelligence pen registers and trap and trace surveillance devices to obtain detailed information on American citizens and lawful permanent residents, including telephone numbers dialed, Internet addresses to which e-mail is sent or received, and the web addresses a person enters into a web browser, even in an investigation that is entirely unrelated to terrorism or counterintelligence. In so doing, it erodes a limitation on this authority that was part of the USA PATRIOT Act.

The standard for obtaining a pen register or trap and trace order is very low, requiring merely that a government official certify that the information it would reveal is "relevant" to an investigation. Under section 216 the USA PATRIOT Act, the government was given new power to obtain this sensitive information for Internet communications merely by making this certification. This expansion was a serious erosion of meaningful judicial oversight of government surveillance because it expanded the authority to get court orders for pen registers and trap and trace devices in a way that permitted the government to access far more detailed content than was available before such authority was extended to the Internet.

For United States citizens and lawful permanent residents, Congress limited the new authority to terrorism and counterintelligence investigations. This section would remove that limitation, opening the door to expanded government surveillance of United States citizens and lawful permanent residents under controversial government law enforcement technologies like CARNIVORE and the Total Information Awareness Pentagon "super-snoop" program whose development Congress just voted to limit.

Providing cleared, appointed counsel for the Foreign Intelligence Surveillance Court of Review (Section 108).

While we welcome the provision providing for an appointed, cleared counsel to argue in favor of a ruling of the Foreign Intelligence Surveillance Court when the government appeals its decisions, it should not substitute for participation, in appropriate cases, by interested civil liberties organizations. The Foreign Intelligence Surveillance Court approves government orders for electronic surveillance and physical searches under FISA. It meets in secret and never hears from anyone other than the government officials seeking its approval. If an order is denied, the government has the right to seek review of that denial in a special three-judge court of appeals, called the Foreign Intelligence Surveillance Court of Review. No one can appeal the approval of a surveillance order, as the target of the surveillance is not notified. Instead, the only challenge to an approved order would occur later, if the information obtained is to be used in a criminal prosecution, in a suppression motion before the district court. If the information is used only for intelligence purposes, there is never an opportunity to challenge the lawfulness of an order approving surveillance.

This section seeks to remedy the problems inherent in a one-sided proceeding, at least with respect to appeals before the Court of Review, by permitting the court to appoint an advocate with security credentials to defend the decision reached in the initial hearing before the Foreign Intelligence Surveillance Court. While the ACLU welcomes this effort to inject an adversary process into the Court of Review’s proceedings, it warns that appointing a cleared lawyer should not be a substitute for independent advocacy by civil liberties or other interested organizations. Organizations independent of the government should be permitted to file briefs amicus curiae and, in appropriate cases, to participate in oral argument as interveners on behalf of Americans who may face increased surveillance as a result of an interpretation of FISA being urged by the government. For this reason, Congress should adopt legislation providing clear procedures that require the publication of opinions by the Foreign Intelligence Surveillance Court and the Court of Review, with redactions for classified information.

Providing new contempt powers for Foreign Intelligence Surveillance Court without sufficient due process (Section 109).

This section seeks to give the Foreign Intelligence Surveillance Court the power to enforce its judgments through explicit contempt powers. While the ACLU does not object to the enforcement of lawful court orders, the draft bill does not specify a means by which parties seeking to challenge an order of the court can vindicate their rights, such as by a motion to quash. If the court is to be given this authority, both the Fourth Amendment and due process require a mechanism, which currently does not exist, for a party facing a possible contempt sanction to appear before the Foreign Intelligence Surveillance Court and be heard, prior to the imposition of any sanctions. [3]

Using an overbroad definition of terrorism that could cover tactics used by some protest groups as a predicate for criminal wiretapping and other surveillance under Title III (Sections 120, 121).

Current law provides, at 18 U.S.C. § 2516, a list of "predicate offenses" that permit the government to conduct wiretaps and other intrusive surveillance. The list is quite lengthy, but reflects the judgment of Congress that electronic surveillance is a particularly intrusive investigative method that is not appropriate for all criminal investigations but should be reserved only for the most serious crimes.

Title 18 already provides that any terrorism crime defined by federal law is a predicate for Title III surveillance. *See* 18 U.S.C. § 2516(q) (providing that any violation of sections 2332, 2332a, 2332b, 2339A, or 2339B is a predicate offense for Title III surveillance). The draft bill, however, extends the predicate even further, to cover offenses that are *not* defined as terrorism *crimes* under federal law, but do fit the definition of either international or domestic terrorism, i.e., they involve acts that are a violation of federal or state law, are committed with the intent of affecting government policy, and are potentially dangerous. *See* 18 U.S.C. § 2331. It is this broad definition that sweeps in the activities of a number of protest organizations that engage in civil disobedience, including People for the Ethical Treatment of Animals and Operation Rescue. Since true crimes of terrorism are already predicates for Title III surveillance, providing this authority is not necessary to listen to the telephone conversations and monitor the e-mail traffic of terrorist groups. To ensure Title III wiretaps are not used to monitor the activities of protest organizations, Congress should reject this provision and should also amend the definition of "terrorism."

Creating a new category of "domestic security surveillance" that relaxes judicial oversight of electronic surveillance of Americans engaged in entirely domestic activity (Section 122).

This section authorizes looser standards for judicial oversight of wiretaps of electronic surveillance orders of Americans for entirely domestic activity under a new theory of domestic intelligence gathering. Intelligence-based surveillance and criminal surveillance are conducted under different rationales, but both are subject to Fourth Amendment protections. *See Katz* and *Keith*, *supra*. Title III, which governs criminal surveillance, provides significantly more robust protections than those afforded for surveillance of foreign intelligence conducted in the United States pursuant to FISA. Title III requires more frequent and continuing supervision of the surveillance order by the authorizing judge, and subsequent notice to the target of the surveillance order unless the government shows adverse results would occur if notice were given.

Title III governs electronic surveillance in domestic criminal and terrorism cases; the looser intelligence standards provided by FISA, including the ability to conduct surveillance in virtually complete secrecy, have always been reserved for "agents of a foreign power." The proposed amendment would fundamentally redefine domestic intelligence gathering through wiretaps and other intrusive surveillance to include entirely domestic security investigations. In so doing, DOJ claims it is accepting the "invitation" of the Supreme Court in *Keith* to devise specific standards for domestic intelligence investigations. It is far from clear the Supreme Court ever issued such an "invitation" because of the ambiguity of the term "domestic intelligence." FISA is, in one sense, a purely domestic intelligence gathering power; it governs gathering of intelligence on United States soil and authorizes surveillance of United States citizens. Under this understanding of "domestic intelligence," Congress has already provided far looser standards for such surveillance than it has for criminal investigations.

In any event, the draft bill's redefinition of intelligence creates what is in essence a twilight zone between the criminal standards provided in Title III and the foreign intelligence standards for targets involved with "foreign powers" in FISA. That twilight zone, as conceived by the draft bill, has significant implications for Americans' right to privacy. Under the DOJ's proposed standards, for domestic terrorism, the normal time period for domestic surveillance orders under Title III would triple from 30 days to 90 days, or, in the case of pen registers and trap and trace devices, from 60 days to 120 days; the judge would be prevented from requiring more frequent reports than once every 30 days, limiting the judge's ability to provide meaningful supervision, and absolute secrecy could be imposed on the government's claim of harm to the "national security," a standard that provides no meaningful judicial check.

Providing for general surveillance orders covering users of high technology devices with multiple functions, thus lowering the bar to surveillance (Section 124).

This section would, in some cases, relieve the government from showing probable cause that would justify reading a person's e-mail if it had shown probable cause that a person's telephone conversations would be relevant to criminal activity. It authorizes a general warrant that, in the physical world, would allow officers who could show probable cause to search only one drawer of a desk to obtain a court order allowing a search of the entire building.

The proposed change would erode the privacy rights of users of multi-function devices. Multi-function devices represent an important advance in communications technology. Such devices can combine the functions of a telephone, fax machine and computer with Internet access, or those of a mobile phone and text messaging service. Another example is the popular TiVo video storage device which both records television programs received through a cable or satellite system and communicates a user's preferences through a computer modem.

Unfortunately, the draft bill continues a DOJ trend of using advances in technology to justify eroding privacy standards. While technology is constantly changing, the principles of the Constitution remain constant. Specificity is a basic requirement for any constitutional judicial process permitting government searches or seizures. The Fourth Amendment states that "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." The fact that the government can show probable cause to monitor e-mail, for example, does not mean that it should also have authority to listen to the target's telephone conversations. Of course, if the government can satisfy the probable cause or other application standard with respect to all of the functions of a device, there is no reason it cannot be granted approval to monitor those functions in a single order. However, the draft bill would make approval for each function automatic, providing that "communications transmitted or received through any function performed by the device may be intercepted and accessed *unless the order specifies otherwise . . .*"

In addition, an order that covers, for example, a personal computer that carries voice or data transmission, also permits "upon a showing as for a search warrant . . . the retrieval of other information (whether or not constituting or derived from a communication whose interception the order authorizes)." While somewhat oblique, this language would permit the seizure of any information stored on a computer's hard drive if the government obtains a order to intercept communications through *any* of the computer's communications functions and makes the required showing.

There is no reason that the purchase of new technology should diminish the user's privacy. Whether one owns one device with several communications functions, or separate communications devices, the government's obligations to show probable cause that the monitoring of communications or the seizure of data will provide some evidence of crime should be the same.

Expanding nationwide search warrants so they do not have to meet even the broad definition of terrorism in the USA PATRIOT Act (Section 125).

The USA PATRIOT Act gave the government authority to issue nationwide search warrants in terrorism investigations, based on the extremely broad definition of domestic and international terrorism contained in 18 U.S.C. § 2331. This definition covers any violation of law, state or federal, that involves "acts dangerous to human life" and is committed with the requisite intent. The draft bill (at section 125) expands the use of nationwide search warrants to cover any offense listed as a federal terrorism crime under 18 U.S.C. § 2332b(g)(5)(B). In general, this is unlikely to be needed as the crimes listed as terrorism crimes are either violent offenses or at least "involve" dangerous acts. To the extent such offenses do not at least "involve" violence or dangerous acts, they should not be terrorism crimes at all and should not trigger special terrorism powers that are unavailable in order criminal investigations. If Congress grants additional authority for nationwide search warrants for certain offenses listed as terrorism crimes, its authority to get nationwide search warrants under an overbroad definition of international and domestic terrorism should be curtailed, by, for example, eliminating that authority or amending the definition of terrorism.

Giving the government secret access to credit reports without consent and without judicial process (Section 126).

This section would allow the government to secretly obtain anyone's credit report without their consent and without any judicial procedure.

The government should not have access to sensitive personal information which has been collected for business purposes on the same basis as businesses, because the government's powers -- for example, to compel questioning before a grand jury, arrest, deport, or incarcerate -- are far greater than the powers of any business.

In any event, the draft bill does *not*, as the heading states, provide "equal access" for government to such reports; rather, the statute greatly expands access to credit reports by authorizing the government to obtain these reports without consent, notice to the person to whom the credit report pertains, and without a court order. Credit reports are available to business with a "legitimate business need" but only with the consent of the person whose credit report is being examined, such as when that person applies for a loan or a job.

Anyone who has applied for a job or a mortgage and encountered a problem because of a false credit report -- which could the result of identity theft, simple error, or malice -- knows how difficult it can be to get errors corrected. Under this provision, however, the consequences of an erroneous credit report are far more serious than when credit reports are used for business purposes. Under this provision, because credit reports can be obtained without notice or consent, there is no opportunity for the person to contest an erroneous report.

Creating new terrorism "administrative subpoenas" and providing new penalties for failure to comply with written demands for records that permit the government to obtain information without prior judicial approval (Sections 128 and 129).

Under these sections, government can demand -- and enforce its demands through civil and criminal penalties -- documents and other information from a business, such as an Internet Service Provider, or any individual without prior court approval. Administrative subpoenas provide the government with the ability to compel production of documents or information without obtaining a court order. While such subpoenas can be challenged, after they are issued, through a motion to quash, such a motion must be brought by the party challenging the subpoena, who incurs the trouble and expense of challenging the subpoena.

The draft bill authorizes the use of administrative subpoenas and what the DOJ calls "national security letters" to obtain information in terrorism investigations. These sections reduce judicial oversight of terrorism investigations by relegating the role of the judge to considering challenges to orders already issued, rather than ensuring such orders are drawn with due regard for the privacy and other interests of the target. Furthermore, by granting the government power to compel production of records or other information, such as computer files, without first going to court, the draft bill will likely increase the administrative burden imposed on small businesses, particularly high-technology firms, who are facing ever-increasing demands for records in both civil cases and criminal investigations.

Title II -- Diminishes Public Accountability and Due Process By Increasing Government Secrecy

Authorizing secret arrests in immigration and other cases where the detained person is not criminally charged (Section 201).

After September 11, 2001, well over a thousand persons whom the government said were connected to its terrorism investigation were detained on immigration charges or material witness warrants without the government revealing who they were or other basic information about their arrests that has always been available to the public and the press. Never before had our government sought to detain persons within the United States in secret; a public process for depriving any individual of liberty is an essential component of the rule of law in a democratic society. As Alexander Hamilton made clear in the Federalist papers more than two centuries ago, a policy that allows "confinement of the person, by secretly hurrying him to jail, where his sufferings are unknown or forgotten" is a "*dangerous engine* of arbitrary government." [4] "The requirement that arrest books be open to the public is to prevent any 'secret arrests,' a concept odious to a democratic society . . . ." *Morrowv. District of Columbia*, 417 F.2d 728, 741-42 (D.C. Cir. 1969).

The government's policy of secret arrests came under fire in both federal and state court in lawsuits brought by the American Civil Liberties Union and other civil liberties and press freedom groups. So far, every court to reach the merits of the argument has agreed that the government's secret arrests policy is not supported by law, is not necessary to protect national security, and violates fundamental principles reflected in state and federal open records laws. [5] When confronted with the ruling in New Jersey state court, the DOJ responded not by complying or appealing the ruling to a higher court, but by issuing a regulation preempting that state's law. It has now chosen to ask Congress to cut short the federal lawsuit in the much the same way.

Threatening public health by severely restricting access to crucial information about environmental health risks posed by facilities that use dangerous chemicals (Section 202).

This section would deprive communities and environmental organizations of critical information concerning risks to the community contained in "worst case scenarios" prepared under federal environmental laws. Under section 112(r) the Clean Air Act, 47 U.S.C. § 7212(r), corporations that use potentially dangerous chemicals must prepare an analysis of consequences of the release of such chemicals to surrounding communities. This information is absolutely critical for community activists and environmental organizations seeking to protect public health and safety, and the environment, and by ensuring compliance by private corporations with environmental and health standards and alerting local residents to the hazards to which they may be exposed.

The proposed amendment (sec. 202) severely restricts access to such information, limiting such access to reading rooms in which copies could not be made and notes could not be taken, and excising from the reports such basic information as "the identity or location of any facility or any information from which the identity or location of the facility could be deduced." "Official users" are given greater access, but these users only include *government* officials, and government whistleblowers who reveal any information restricted under this section commit a criminal offense, even if their motivation was to protect the public from corporate wrongdoing or government neglect.

Harming fair trial rights for American citizens and other defendants by limiting defense attorneys from challenging the use of secret evidence in criminal cases (Section 204).

This section would inhibit the ability of the accused to defend themselves against criminal charges based in part on classified information. The Classified Information Procedures Act (CIPA), 18 U.S.C. App. 3 §§ 1-16, provides a special procedure to govern an extraordinary situation -- where the government seeks to use information in a criminal case which is classified by Executive Order without revealing in open court any more information than is necessary to provide the defendant with a fair trial under the Sixth Amendment. [6]

CIPA entrusts to federal district judges the "gatekeeper" function of determining what classified information can be excluded from open court, what information can be given to the defense in summary form, and what essential information must be disclosed to the defendant to ensure his right to contest the accusations against him and to ensure that evidence the jury or other factfinder considers is reliable, having been tested in an adversarial proceeding. The judge has the power to consider a government request to delete information or substitute a summary in an ex parte proceeding, i.e., without the benefit of hearing from the defense. CIPA does *not* give the government a right to make its case in the absence of the defense; instead, the judge determines how much of the prosecution's submission to examine ex parte and in camera, i.e., in secret. The proposed amendment (sec. 204) would seriously undermine the judge's initial gatekeeping role by compelling a judge, at the request of the prosecution, to determine whether and how to redact classified information without the benefit of an adversary hearing. In other words, the amendment would take away the judge's authority, under current law, to hear defense objections to a prosecution request for authorization to delete specified items of classified information from documents relevant to the defense's case.

CIPA strikes the right balance between the government's national security interests and the defendant's right to see the evidence against him or her. This amendment undermines that balance.

Gagging grand jury witnesses in terrorism from discussing their testimony with the media or the general public, thus preventing them from defending themselves and denying the public information it has a right to receive under the First Amendment (Section 206).

This section would gag grand jury witnesses so that they could not publicly respond to false information about them leaked to the press. Rule 6(e) of the Federal Rules of Criminal Procedure imposes a general obligation of secrecy requiring attorneys and grand jurors to refrain from commenting on "matters occurring before the grand jury." In theory, grand jury secrecy is imposed primarily to protect the reputation of individuals who become subject to a grand jury investigation. In practice, such secrecy does not always afford much protection, as law enforcement officials who leak information to reporters in violation of Rule 6(e) are rarely discovered and prosecuted.

Grand jury secrecy is *not* imposed on witnesses, who are free to speak about their testimony to friends, associates or to the media. In practice, this limitation is essential to afford targets of a grand jury investigation the opportunity to defend themselves against leaked accusations and media speculation. Under the proposed amendment (section 206), witnesses in terrorism investigations could be unfairly smeared in the media and be deprived from the ability to defend themselves under pain of a criminal sanction.

Title III -- Diminishing Personal Privacy by Removing Checks on Local Police Spying; Undermining Genetic Privacy; Removing Checks on Foreign-Directed Searches and Arrests, Even for Dictatorships; Sharing Sensitive Immigration Information With Local Police

Allowing for the sampling and cataloguing of innocent Americans' genetic information without court order and without consent (Sections 301-306).

The proposed bill authorizes collection of genetic information of persons who have not been convicted of a crime for terrorism investigation purposes, and the entering of that sensitive information into a database. At a minimum, such collection should not be permitted on persons who have not be convicted of serious crimes unless a judge decides to permit such collection by issuing a court order on the basis of probable cause to believe the information will assist in a criminal investigation. Furthermore, personal genetic information must be destroyed within a reasonable time, such as when a suspect is cleared, to ensure it is not available for misuse by the government or private industry at a later date.

Drawing a DNA sample involves an intrusion on personal privacy that is far more invasive than simply taking a fingerprint. A fingerprint is useful only as a form of identification. By contrast, a DNA sample includes such intimate, personal information as the markers for thousands of diseases, legitimacy at birth, or (as science advances) aspects of an individual's personality such as his or her temperament. In addition, this personal information is not unique to the individual alone, but also provides clues to the genetic traits of everyone in that individual's bloodline. Genetic discrimination is not merely a distant artifact of the discredited eugenics movement of the first half of the Twentieth Century, but is widespread today among private employers, and is (in most states) perfectly legal. [7]

The potential misuse of DNA information contained in a database requires careful safeguards before such information is collected, and concerning the storage of such information. For example, no forensic purpose is served by saving the DNA itself, as opposed to just the information contained in the DNA that proves identity. The proposed legislation fails to include such safeguards.

Permitting, without any connection to anti-terrorism efforts, sensitive personal information to be shared with local and state law enforcement; opening sensitive visa files to local police (Section 311).

This section would authorize the sharing of sensitive consumer credit information and educational records with state and local officials without any limits and without any connection to a terrorism investigation. While sharing of sensitive information in the possession of the federal government should be permitted in some circumstances to accomplish anti-terrorism objectives, such records should not be disseminated broadly for other purposes. The draft legislation contains no requirement that sharing of sensitive information with state and local officials be limited to anti-terrorism investigations; instead, such information can be shared simply "to assist the official receiving that information in the performance of official duties of that official." Special authority to share sensitive personal records should not be granted so blithely.

The draft legislation also provides for sharing of sensitive visa information with state and local officials, including state and local law enforcement, on a broad basis, without requirement that such sharing of information be connected to anti-terrorism investigations. In authorizing such sharing of sensitive immigration files, DOJ is at odds with the views of many state and local police departments, who fear involvement in immigration enforcement matters may undermine their ability to establish the trust and confidence of immigrant communities. Absent such trust, many local and state police are concerned that members of immigrant communities will fear contacting the police if they are a victim of crime or a witness to crime. [8]

DOJ also appears to be at odds with the White House, which has assured the public that the Bush Administration was not interested in expanding the role of state or local law enforcement in immigration matters except with respect to terrorism investigations. As White House Counsel Alberto Gonzalez made clear last year, "Only high-risk aliens who fit a terrorist profile" would be placed in the National Crime Information Center (NCIC) database, which is available to state and local law enforcement officials, and the Administration's conclusion that state and local police had "inherent authority" to arrest such persons was limited to this group of non-citizens. [9] Such a narrow policy would be completely undermined by the adoption of this broad language.

Terminating court-approved limits on police spying designed to prevent McCarthy-style law enforcement persecution based on political or religious affiliation (Section 312).

In the name of "intelligence gathering," police departments in many cities spied on innocent members of the public who were active in churches, community groups and political organizations. Federal courts, responding to civil rights lawsuits urging an end to such spying, issued decrees prohibiting this spying absent some reason to believe those individuals were involved in criminal or terrorist activity.

Police spying on political and religious activity is not a relic of some distant past. Recently, citizens in Denver, Colorado, were shocked to learn that the Denver Police Department had kept approximately 3,048 illegal files on peaceful protest groups including Amnesty International and the Nobel Peace Prize-winning American Friends Service Committee. The file on the American Friends Service Committee labeled them a "criminal extremist" group. The files pre-dated September 11, 2001, and were not collected as a response to the terrorist attacks.

The draft bill ends these decrees using language patterned after the Prison Litigation Reform Act. Eliminating these sensible, court-approved limits on local police spying would chill dissent, making Americans afraid to join protest groups and activist organizations, attend rallies, or express their views on controversial policies such as abortion or the war in Iraq.

Loosening sensible protections on police monitoring of political and religious activity will not make us safer from terrorism. During the years the FBI illegally spied on individuals exercising their rights under the First Amendment, including such civil rights leaders as Dr. Martin Luther King, Jr., resources were diverted and not a single instance of violence was prevented. Freeing local police to spy on innocent individuals is not likely to be any more productive. It only makes us less safe as resources are diverted from more productive investigations, and less free, as individuals find themselves entered into a police database for activities that are constitutionally protected.

Granting immunity to businesses that provide information to the government in terrorism investigations, even if their actions are taken with disregard for their customers' privacy or other rights and show reckless disregard for the truth (Section 313).

This section would prevent a person harmed by a business's disclosure of information about them, including false information, from holding the business accountable. It would encourage false terrorism tips that could result in ruined reputations, lengthy detentions and even violence. Under this section, a business is given immunity from liability if it shares information voluntarily with the government, based on merely on its "reasonable belief" that its actions would help the government prevent or investigate terrorism.

This section resurrects many of the same problems with Operation TIPS that led Congress to ban that program last year. Enormous controversy was sparked by the Bush Administration's Operation TIPS plan to enlist businesses with access to private homes or otherwise able to obtain sensitive personal information without any court supervision. Under the plan, utility operators or others would be encouraged to report "suspicious activity" through a special federal hotline, where the reports would be placed in a central computer database. The program was rife with potential for abuse, including the reporting of false or erroneous information, and the concern that businesses and private individuals would allow their private prejudices to determine who qualifies as "suspicious." When Congress learned of "Operation TIPS" and considered its potential dangers, it banned the program in legislation creating the new Department of Homeland Security. *See* Homeland Security Act of 2002, § 880, Pub. L. No. 107-296, 116 Stat. 2135, 2245 (2002).

The draft legislation poses many of the same dangers as the government's earlier, more elaborate private spying program. False information can ruin a person's reputation, lead to an erroneous arrest and even to violence. Those who are subject to such false reports should have legal recourse if the business or individual responsible for making the report acted irresponsibly. Defamation is the most likely legal action resulting from a false tip to law enforcement. Further protection for defamation defendants would weaken the incentive for a business to think twice before using a false tip to law enforcement to settle a private score or indulge in invidious discrimination. The proposed language paradoxically would increase the incentive for reports of information of dubious validity, diverting law enforcement from more serious potential crimes.

Granting additional immunity is unnecessary because there is already ample protection in state law against frivolous lawsuits. Truth is always a defense to defamation and states also generally provide a qualified privilege against defamation claims involving reports to law enforcement even where the information proves to be false, protecting a defendant against liability unless malice can be shown. *See, e.g.,* Restatement (Second) of Torts §§ 598, 600.

Permitting searches, wiretaps and surveillance of United States citizens on behalf of foreign governments -- including human rights abusers -- in the absence of Senate-approved treaties (Sections 321-22).

This section would authorize the DOJ to help foreign governments -- including those that systematically abuse human rights and do not respect the rule of law -- invade Americans' privacy even when the United States Senate has failed or refused to approve a treaty allowing such assistance with such a government. Under current law, the United States does not engage in covert surveillance or issue search warrants on behalf of foreign nations unless the Senate has approved a mutual legal assistance treaty. If a foreign nation with which the United States does not have such a treaty requires information from a United States citizen or resident for its own judicial process, it may still obtain that information by asking the assistance of a United States district court in issuing an order to take testimony or obtain "a document or other thing" under 28 U.S.C. § 1782, but it may not issue search warrants or certain surveillance orders. This limitation ensures that that the Senate consents to more intrusive surveillance on behalf of a foreign nation before Americans' privacy can be invaded at the behest of a foreign government. The draft bill (at section 321) sweeps aside this sensible limitation altogether.

These limitations on foreign-directed searches, wiretaps and surveillance orders do not need to substantially impede the investigation and prosecution of terrorism, as Congress has provided "universal jurisdiction" over many serious terrorism offenses. In other words, such offenses are a crime under United States law and subject to U.S. jurisdiction even if committed in a foreign nation. For such offenses, a United States Attorney could obtain the full panoply of searches and surveillance orders to aid in the investigation of that crime, even if such a crime was also being investigated by a foreign nation under its own laws. Such information could then easily be shared with the foreign nation, under information sharing provisions approved by Congress in the Homeland Security Act. *See* Homeland Security Act of 2002, §§ 891-99, Pub. L. No. 107-296, 116 Stat. 2135, 2252-58.

Permitting arrests and extraditions of United States citizens and other persons to a foreign country in the absence of a Senate-approved treaty and without judicial inquiry into the extraditing country's human rights record (Section 322).

Among other things, this section allows, on the determination of the Attorney General, a United States citizen or other person to be sent to a foreign dictatorship to be prosecuted even if an American judge would find that the extradition request was made on account of his or her race, nationality or political opinions. It allows the government to send Americans and others abroad to face foreign criminal charges in foreign criminal courts for a host of charges without any of the protections that normally appear in Senate-approved extradition treaties, and strips any judge hearing an extradition request of the authority to consider the fairness of the requesting country's judicial system or its human rights record.

Section 322 authorizes extradition in the absence of an extradition treaty or in excess of limits imposed by existing extradition treaties. Extradition involves arresting an individual, including a United States citizen, because a foreign government accuses that person of violating a foreign law. It is subject to basic constitutional limitations. *See, e.g.*, *Valentine v. United States ex rel. Neidecker*, 299 U.S. 5, 8 (1936) (holding that extradition may take place only in accordance with law because of "the fundamental consideration that the Constitution creates no executive prerogative to dispose of the liberty of the individual"). One important safeguard that protects Americans from facing trial in a potentially unfriendly nation, or in a nation that does not respect fundamental fair trial principles or abuses human rights, is the requirement that such extradition take place where the Senate has, by ratifying an extradition treaty, approved of the practice of a foreign nation sufficiently to permit such extradition.

Another, critical safeguard is the requirement of judicial supervision of extradition requests. This section expressly prohibits the judge from considering any of the following:

- "humanitarian concerns,"
- "the nature of the judicial system of the requesting foreign government," and
- "whether the foreign government is seeking extradition of a person for the purpose of prosecuting or punishing the person because of race, nationality or political opinions of that person."

Under this legislation, an American can be sent abroad to face trial under before the courts of a foreign dictatorship, and an American judge has no ability under the statute to even inquire as to the fairness of that country's court system or the reasons behind its criminal accusations.

Current basic due process and constitutional limits on extradition do not need to substantially impede the prosecution of terrorism, as Congress has provided "universal jurisdiction" over many serious terrorism offenses. In order words, such offenses are a crime under United States law even if committed in a foreign nation. For such offenses, a United States Attorney could charge a person suspected of a terrorism crime committed in a foreign nation if the United States lacked an extradition treaty.

Title IV -- Undermining Fundamental Constitutional Rights Of Americans Under Overbroad Definitions Of "Terrorism" And "Terrorist Organization"; Reducing Due Process in Administrative Proceedings for Pilots; Undermining Financial Privacy and Due Process

Further criminalizing association -- without any intent to commit specific terrorism crimes -- by broadening the crime of providing material support to terrorism, even if support is not given to any organization listed as a terrorist organization by the government (Section 402).

Under this section, a person who provides "material support" for "terrorism" as defined under the USA PATRIOT Act, could face a conviction, and lengthy prison terms, even if they did not provide any support for an organization listed as a terrorist organization. The definition of terrorism is not linked to any specific crimes, but covers all dangerous acts that are a violation of any federal or state law and are committed to influence government policy. *See* 18 U.S.C. § 2331. The definition arguably covers some protest activities, such as those used by Operation Rescue or by protesters in Vieques Island, Puerto Rico, as such tactics involve dangerous acts that are a violation of law and are committed to influence the government.

This section modifies the requirement to the crime of providing material support for terrorism, 18 U.S.C. § 2339A, which is a separate crime from providing material support for a designated terrorist organization, 18 U.S.C. § 2339B. Under current law, a person, including an American citizen, can only be prosecuted for providing material support for terrorism if the support is provided with the intent to further one of a list of terrorism crimes. A person can be prosecuted for providing resources to a terrorist organization that is designated by the government under the much broader definition of terrorism that arguably covers some protest groups, but only if such an organization has been designated as an international terrorist organization by the Secretary of State. *See* 18 U.S.C. § 2339B. In each case, the person effectively has some notice that what they are doing is prohibited: either the activity they support is a crime or the group whose lawful activities they would support has been publicly designated a terrorist organization. The amendment takes away this notice by permitting prosecution for providing support for the activities of an undesignated organization.

Groups such as Greenpeace arguably could be designated an international terrorist organization, because of the overbroad definition, but the government has not so designated them. Under this provision, however, the determination of whether to apply the terrorism definition to protest groups belongs not with high Executive Branch officials, but to the prosecutor who chooses to invoke the new criminal definition.

Creating a new, separate crime of using encryption technology that could add five years or more to any sentence for crimes committed with a computer (Section 404).

Under this section, any federal felony committed with encryption technology that is now commonly part of computer software could be punished by an additional five years (or more, for a repeat offense.) The criminal conduct will not be any different; the only reason for additional penalties will be that the defendant used a certain technology to commit the offense. Here again, the DOJ's description of the crime differs from the language proposed in the draft text. DOJ says it makes it a separate federal crime for a person to "knowingly and willfully use[] an encryption technology *to conceal* any incriminating communication . . . ." However, the draft text contains no requirement that the defendant intend to conceal anything; the crime is complete if the defendant intentionally uses an encryption technology in the commission of a crime. Thus, a simple fraud crime could, if committed using garden-variety encryption technology available with most standard web browsers, carry an additional jail term of up to five years regardless of whether the defendant intended to conceal his activity by using encryption.

Shifting burden of proof to defendant to obtain pretrial release for a laundry list of terrorism crimes (Section 405).

Under this section, the right to bail, protected by the Eighth Amendment, is denied for a host of crimes said to be likely to be committed by terrorists unless the defendant is able to overcome the presumption created by the statute. A major reason for the Constitution's prohibition against excessive bail is that defendants are presumed innocent until and unless they have been convicted in a court of law. Despite this, under certain circumstances, the Constitution permits pretrial detention. In general, the government must establish, by clear and convincing evidence, that no release conditions can adequately ensure the appearance of the defendant at trial or the safety of the community. [10]

There is no reason to exacerbate the constitutional problems posed by the presumption against pretrial release for some drug crimes by expanding that presumption to additional crimes. Before the government imprisons a person who has not been convicted of any crime, the government must bear the burden of establishing that the defendant is a flight risk or a danger to the community. This should not be hard to convince a court with respect to true terrorism defendants; there is no need to apply a pretrial detention presumption to a laundry list of offenses that are simply said to be likely to be committed by terrorists.

Imposing potentially life-long supervision and eliminating statute of limitations for nonviolent crimes listed as terrorism crimes, even where they create no risk of death or serious injury (Sections 408 and 410).

Under section 408, a defendant who has served his or her sentence for a nonviolent crime listed as a terrorism crime could face life-long supervision, and possible reincarceration if those supervision conditions are violated, even if the crime for which he or she was convicted posed no risk of death or even serious injury. Likewise, section 410 removes entirely the statute of limitations for such nonviolent offenses. Under the USA PATRIOT Act, certain severe consequences follow from the commission of certain terrorism crimes, including the potential for life-long supervision, even after serving a full criminal sentence. In drafting the USA PATRIOT Act, Congress provided for a modest and very sensible limitation for such consequences -- they only follow where the offense results in, or creates a foreseeable risk of, death or serious injury.

Indeed, it is not clear why any offense that would not at least create a risk of serious injury deserves to be labeled terrorism at all. The draft bill (at sections 408 and 410) eliminates this sensible restriction, by applying the severe consequence of lifetime supervision and removal of the statute of limitations even for crimes which do not create even a risk of death or serious injury. While DOJ uses the example of a computer crime causing severe financial damage or the provision of material support to an organization labeled as terrorist, it does not explain why such actions, if they truly were serious enough to be considered terrorism under a common sense rather than a legal definition, would not easily meet the requirement of causing at least a risk of serious injury.

Creating 15 new death penalties, including a new death penalty for "terrorism" under a definition which could cover acts of protest such as those used by Operation Rescue or protesters at Vieques Island, Puerto Rico, if death results (Section 411).

The draft bill dramatically expands the death penalty, creating fifteen separate new death penalty crimes by defining a new death sentence that sweeps in the remaining crimes listed as federal crimes of terrorism in 18 U.S.C. § 2332b(g)(5)(B) that do not provide for the death penalty. Among others, these include the provision of material support for the lawful activities of an organization labeled a terrorist organization by the government, 18 U.S.C. § 2339B. While the DOJ labels this provision as providing for the death penalty for terrorist "murders," there is no language in the text that requires any showing by the government of an intent by the defendant to kill; it is sufficient that death results from the defendant's actions.

Even more troubling, the draft bill is not content to create fifteen new death penalties, but also contains language that sweeps in *any* violation of state or federal law that is committed under the definition of domestic or international terrorism contained in 18 U.S.C. § 2331. As a result, activities that (1) involve "acts dangerous to human life," (2) are a violation of any state or federal law, and (3) are committed in order to influence government or the population by intimidation or coercion become death-penalty eligible if death results. Arguably, this definition could fit some protest activities, such as those used by Operation Rescue, People for the Ethical Treatment of Animals, or Greenpeace. For example:

- If protesters at Vieques Island, Puerto Rico, a military bombing range unpopular with local residents, cut a fence to trespass on the military's bombing range, and a bomb killed one of the demonstrators, a prosecutor could charge the survivors with a eligible crime for which the sentence could be death.
- If Greenpeace activists attempted to block an oil tanker entering a port to protest the company's safety record, and a member of the tanker's crew drowned attempting to ward off the activists' boat, the protesters could be charged with a crime for which the sentence could be death.
- If an Operation Rescue anti-abortion demonstration succeeded in blocking a woman seeking follow-up treatment for complications following her abortion, and the woman died, the protestors could be charged with a crime the sentence for which could be death.

Under this provision, protesters could be charged with the death penalty as the result of a tragedy. While dangerous protest tactics can be punished under the law, they are not terrorism and should not be treated as if they were.

Reducing due process for pilots accused of posing a security threat (sec. 409).

While the government has authority to revoke a pilot's license on a sufficient showing that the pilot presents a risk to air security, such denials must be accompanied by a fair opportunity for the accused pilot to be heard in an administrative hearing and to have judicial review of any final determination. The draft bill's procedures for revoking pilot licenses are deficient in this respect. They do not clearly provide for an administrative hearing (as opposed to an administrative determination), and judicial review is provided only through a direct appeal to the United States Courts of Appeals, who are unlikely to have the time or resources to conduct a thorough review of the administrative record.

Further undermining privacy in financial transactions and due process in asset forfeiture and other civil proceedings (subtitle B; secs. 421-28).

Continued amendment of money laundering and asset forfeiture laws have resulted in a serious erosion of financial privacy and of due process rights in asset forfeiture and other proceedings. These sections continue that trend:

- Section 421 multiplies by five times the maximum civil penalty for violating economic sanctions or trade embargoes from $10,000 to $50,000. This provision would severely penalize the thousands of Americans who travel to Cuba every year (often without fully appreciating that their travel is prohibited). It would also penalize physicians or other activists who wish to protest our sanctions on other countries, such as Iraq, by bringing medicine or other humanitarian aid to those nations in violation of such an embargo.
- Section 422 targets "hawalas" -- traditional money transfer systems used for entirely legitimate reasons in many Muslim cultures -- by undermining key concepts of the money laundering statutes. Under this provision, money can be deemed "laundered" even if the funds involved are not proceeds of a crime.
- Section 423 further undermines due process for organizations unfortunate enough to be labeled as "terrorist organizations" by the government, by depriving them of the ability to defend their status as legitimate charities in a proceeding to revoke their tax-exempt status.

- Section 427 and 428 expand civil asset forfeiture -- a procedure rife with due process problems that the government can use to seize property without proving that the owner is guilty of any crime and without a pre-seizure hearing. Under this provision, the assets of a protest group that arguably fits the USA PATRIOT Act's overbroad definition of terrorism could be more easily seized by the government, and the use of secret evidence is explicitly authorized to permit such seizures.

Title V -- Stripping Americans of All Their Rights as U.S. Citizens; Unfairly Targeting Immigrants Under the Pretext of Fighting Terrorism

Stripping even native-born Americans of all of the rights of United States citizenship if they provide support for "terrorism," allowing them to be indefinitely imprisoned in their own country as undocumented aliens. (Section 501).

This section would permit the government to punish certain criminal activity by stripping even native-born Americans of U.S. citizenship, thereby depriving them of any nationality at all and potentially relegating them forever to imprisonment as undocumented immigrants in their own country. Among the activities that could be punished this way are providing material support for an organization -- including a domestic organization -- labeled as a terrorist organization by the government, even if the support was only for the lawful activities of that organization.

The Fourteenth Amendment provides that "All persons born or naturalized in the United States, and subject to the jurisdiction thereof, are citizens of the United States and of the State wherein they reside." While Americans do have the right to give up their citizenship in the United States, the Constitution does not give Congress any power to take away from an American his or her status as a citizen even for participating in crime in time of war. *See Trop v. Dulles*, 356 U.S. 86 (1958) (conviction by court martial of crime of desertion during World War II could not constitutionally lead to loss of citizenship, even though crime was committed voluntarily). Rather, as the Supreme Court has made clear, every citizen of the United States enjoys "a constitutional right to remain a citizen . . . unless he voluntarily relinquishes that citizenship." *Afroyim v. Rusk*, 387 U.S. 253 (1967) (citizenship could not be forfeited merely by voting in foreign election without the requisite intent to abandon U.S. citizenship).

While DOJ is correct to observe that certain voluntary acts, such as serving in a foreign army, can serve to terminate U.S. citizenship, these "expatriating acts" must indicate some desire to show an affinity with a foreign sovereign. Only acts that indicate such a desire to relinquish American nationality can be made the basis for a finding that strips an American of his or her citizenship. *See Vance v. Terrazas*, 444 U.S. 252, 262 (1980).

Moreover, it is the government's burden to establish that the expatriating act was committed with the intent of relinquishing citizenship, a showing this section attempts to short-circuit. *See id.* at 261 (holding that the "trier of fact must . . . conclude that the citizen not only voluntarily committed the expatriating act prescribed in the statute, but also intended to relinquish his citizenship.") Expatriating acts are not defined by reference to how repugnant or offensive they are, or by whether they constitute serious crimes, but by whether they show the individual has an intent to attach himself or herself to another sovereignty. Thus, while serving in a foreign army or voting in a foreign election may indicate an intent to abandon American nationality, the commission of a series of grisly murders, or the control of a vast criminal enterprise plainly do not, although the former are legal while the latter are serious crimes.

Providing support to a terrorist organization, which possesses no sovereignty under international law, is a crime, *see* 18 U.S.C. § 2339A, but plainly does not indicate that the individual desires to attach himself or herself to the allegiance of a foreign nation or to abandon U.S. citizenship in the way that, for example, serving in a foreign army might. Indeed, expatriation in the draft bill is not even limited to providing material support to **foreign** terrorist organizations, as wholly domestic organizations can be designated as terrorist organizations under 8 U.S.C. § 1182(a)(3). In addition, expatriation could result from support of organizations "engaged in hostilities" against the "national security interests" of the United States -- which could mean anything -- not just against the United States or its people. Finally, the draft bill would allow expatriation even for support of the lawful, humanitarian activities of an organization that the United States has labeled a "terrorist organization," which belies DOJ's analogy of supporting terrorism by serving in a foreign army engaged in hostilities against the United States.

Targeting undocumented workers with extended jail terms for common immigration offenses (Sections 502 and 505).

Under the pretext of fighting terrorism, this section -- which applies to low-level, garden variety immigration offenses that have nothing to do with terrorism at all -- unfairly targets undocumented workers. The United States census revealed that more than seven million undocumented immigrants are living in the United States. At present, the United States is engaged in negotiations with Mexico in part to decide whether to permit greater numbers of temporary workers to come to the United States legally, and whether such a program would also provide a path to legal status for undocumented Mexicans or other undocumented immigrants.

Under the pretext of fighting terrorism, this section short-circuits the national debate over immigration policy by substantially increasing penalties for a number of very common immigration crimes often committed by undocumented immigrants. These include unlawful entry (INA § 275(a)(1)), reentry after removal (INA § 276), and failing to register with the immigration authorities (INA § 264(e)). The draft bill (at sec. 505) also provides that the offense of failing to depart after a deportation order (INA § 243) is a continuing offense -- meaning that, in practice, no statute of limitations will apply. Increasing these penalties now would almost certainly not prove an effective deterrent to illegal immigration, as the threat of penalties for illegal immigration has never been sufficient to outweigh the causes of immigration including the pull of economic opportunity and the conditions in the home country, but could frustrate our relations with Mexico and other important U.S. allies seeking to negotiate a new framework for immigration policy.

Providing for summary deportations, even of lawful permanent residents, whom the Attorney General says are a threat to national security (Section 503).

Under this provision, any immigrant, including longtime lawful permanent residents, may be expelled from the United States on the unilateral determination of the Attorney General that they are a threat to "national security," which is defined as "the national defense, foreign relations, or economic interests of the United States." INA § 219(c)(2). A person facing removal under this section will be separated from his or her family and community without ever being able to effectively answer the government's true reasons for labeling him or her a security risk.

Immigrants and other non-citizens involved in terrorism are deportable under current law, [11] and suspected terrorists are subject to mandatory detention during any immigration or criminal proceedings. [12] The purpose of this amendment is to eliminate due process entirely for immigrants, including lawful permanent residents, accused of crimes or terrorism by permitting their expulsion merely on the Attorney General's fiat. It is based on the fundamentally flawed notion that non-citizens in the United States do not possess the right to fair treatment under the law, a notion that the Supreme Court has repeatedly rejected. *See Zadvydas v. Davis* 533 U.S. 678, 693 (2001) (reiterating long-standing constitutional rule that "the Due Process Clause applies to all 'persons' within the United States, including aliens, whether their presence here is lawful, unlawful, temporary, or permanent").

The proposal is another DOJ initiative that flies in the face of President Bush's stated opposition to the use of secret evidence in immigration proceedings on the basis that fair treatment should be afforded everyone in America. Under the proposal, a non-citizen, including a lawful permanent resident, accused of posing a risk to national security could be detained and deported without having committed any violation of law and without ever knowing the basis of the accusation against him or her. The provision would essentially authorize a repeat of the "Palmer raids," a discredited episode in the 1920s that involved widespread mass deportations and widespread abuse of the rights of law abiding Russian and other immigrants during a wave of anti-immigrant and nativist hysteria.

DOJ originally asked for this summary deportation power shortly after September 11 in its initial drafts of the USA PATRIOT Act. It was firmly rejected, on a bipartisan basis, by a Congress deeply concerned about the use of secret evidence and core due process in immigration proceedings. It should be rejected again.

Completely abolishing fair hearings for lawful permanent residents convicted of even minor criminal offenses through a retoractive "expedited removal" procedure, and preventing any court from questioning the government's unlawful actions by explicitly exempting these cases from habeas corpus (Section 504).

Under this new "expedited removal" provision, any immigrant who was convicted even of a minor criminal offense long ago could be deported under a special procedure that provides for no immigration hearing at all and restricts the federal courts from questioning whether the government's actions are within the law. The expedited removal provision, which currently applies only to some classes of undocumented immigrants, would now apply to all immigrants, including lawful permanent residents. "Expedited removal" would be available for crimes which are called "aggravated felonies" (and other crimes) but can be as minor as a shoplifting offense for which a suspended sentence of one year or more is imposed. No discretionary relief is available, regardless of the compelling humanitarian circumstances of any particular case, and the provision applies retroactively. The provision also unconstitutionally exempts these cases entirely from habeas corpus, 28 U.S.C. § 2241, which protects the right of all persons in custody -- including immigrants -- to a judicial determination of the legality of the government's actions.

In 1996, Congress adopted harsh laws that greatly expanded the number and types of crimes that could lead to *automatic* deportation -- i.e., deportation without any possibility to even apply for discretionary relief from the Attorney General. At that time, DOJ went even further than Congress, arguing that the law applied retroactively, so that even immigrants who had been granted relief for crimes committed years or decades earlier and had turned their lives around would now face automatic deportation. DOJ also argued that its controversial retroactive interpretation of the law could not be questioned by any federal court, including the Supreme Court.

In 2001, the Supreme Court firmly rejected DOJ's position, finding both that Congress had not intended the 1996 immigration laws to apply retroactively and that restrictions on judicial review still left intact the federal court's power to correct unlawful government action through a writ of habeas corpus under 28 U.S.C. § 2241. *See INS v. St. Cyr,* 533 U.S. 289 (2001). ("Judicial intervention in deportation cases is unquestionably required by the Constitution.") At the same time, in Congress, a growing number of members of Congress, on both sides of the aisle, began to reconsider the scope of the 1996 laws, culminating the decision of the House Judiciary Committee in 2002 to approve H.R. 1452, the Family Reunification Act, which would restore discretionary relief for some lawful permanent residents accused of relatively minor offenses, particularly if they had come to the United States at an early age.

The draft bill would seriously undermine fair treatment of lawful permanent residents. It would deny fundamental due process in immigration proceedings by completely eliminating an actual hearing. It would disregard the Supreme Court's *St. Cyr* ruling, stripping the judiciary of its core functions in such cases.

The provision attempts to insulate the Attorney General's "expedited removal" decision from judicial review by taking a step never taken by Congress since the Civil War -- expressly denying access to habeas corpus, 28 U.S.C. § 2241 , to prevent the federal courts from correcting unlawful actions by the immigration authorities. Because of the jurisdiction provided by by 28 U.S.C. § 2241, the Supreme Court in *St. Cyr* was able to consider the merits and found that Congress had not intended to apply the 1996 laws retroactively. This court-stripping provision violates the Constitution, because the Constitution protects habeas corpus -- the Great Writ that keeps detention within the boundaries of the rule of law. [13]

Expanding the Attorney General's authority to designate a country to which an immigrant could be deported, and permitting such deportation even if there is no effective government in such a country (Section 506).

This section would authorize the Attorney General to dump immigrants ordered removed in any country in the world, and even to areas which are lawless and have no governing authority whatsoever. This section would have a devastating effect on Somalis and other Africans. While the world's attention is focused elsewhere, a tragedy of extraordinary proportions has been building in Africa, where in Somalia, for example, effective government has broken down as rival armed groups vie for power. For this reason, a federal district court is now entertaining a plea from Somalis to halt deportations to that country. The

Immigration and Nationality Act does not provide for forced deportation of anyone to a country or region that lacks any form of government, nor should it. Deportation should not be a death sentence, as such deportation could easily become. Nor is it good foreign policy to simply dump into lawless regions non-citizens ordered removed from the United States because such a policy that will simply exacerbate the severe challenges facing such areas of the world.

ENDNOTES

1. This and other similarities to criminal wiretap requirements were essential to the review court's holding that "FISA as amended is constitutional because the surveillances it authorizes are reasonable." *Id.* at 56. The ACLU does not agree with that conclusion, but simply notes that even a court with the broadest view of the government's surveillance power has found the requirement that the government show probable cause that a target is acting for a foreign power is constitutionally based.

2. Richard Reeves, PRESIDENT NIXON: ALONE IN THE WHITE HOUSE 335 (2001). The plan was apparently *not* implemented, despite President Nixon's order, but certainly contributed to the pattern of abuse that finally lead to the Watergate break-in and cover up.

3. In the absence of such a process, a party could well be barred from challenging the lawfulness of the underlying order in any proceeding to enforce contempt sanctions. *See Walker v. City of Birmingham*, 388 U.S. 307, 317 (1967) (holding civil rights marchers could not challenge the lawfulness of an injunction forbidding a peaceful march in proceedings to enforce contempt sanctions).

4. THE FEDERALIST No. 84 (Hamilton) (emphasis in original) (quoting 1 Blackstone, COMMENTARIES ON THE LAWS OF ENGLAND 335).

5. See *American Civil Liberties Union of New Jersey v. County of Hudson*, No. HUD-L-463-02 (N.J. Super. Ct. Law Div. April 12, 2002), *rev'd on other grounds*, 779 A.2d 629 (N.J. Super. App. Div. 2002); *Center for National Security Studies v United States Dep't of Justice*, 215 F. Supp. 2d 94 (D.D.C. 2002) (appeal pending before D.C. Circuit).

6. "In all criminal prosecutions, the accused shall enjoy the right . . . to be informed of the nature and cause of the accusation; to be confronted with the witnesses against him; [and] to have compulsory process for obtaining witnesses in his favor . . . ." U.S. Const. amend. 6.

7. *See* Testimony of Barry Steinhardt, Associate Director of the American Civil Liberties Union, Before the House Judiciary Committee, Subcommittee on Crime, March 23, 2000 (reporting an American Management Association survey in 1997 that reported that six out of ten employers responding use genetic screening information for employment purposes.)

8. The National Immigration Forum has posted on its website a list of statements by local and state police from across the country, all opposing any attempt to enlist them in the enforcement of immigration laws. *See* Opposition to Local Enforcement of Immigration Laws, updated October 1, 2002, available at: http://www.immigrationforum.org/currentissues/articles/100102_quotes.htm

9. *See* Letter from White House Counsel Alberto R. Gonzalez to Migration Policy Institute, June 24, 2002, available at: http://www.migrationpolicy.org/files/whitehouse.pdf

10. *See United States v. Salerno*, 481 U.S. 739, 751 (1987) (holding that pretrial detention is constitutional "[w]hen the Government proves by clear and convincing evidence that an arrestee presents an identified and articulable threat to an individual or the community").

11. *See* INA § 237(a)(4)(B) ("Any alien who has engaged, is engaged, or at any time after admission engages in any terrorist activity . . . is deportable.")

12. USA PATRIOT Act, § 412, Pub. L. No. 107-56, 115 Stat. 321 (2001), codified at INA § 236A.

13. Another court-stripping provision, in Section 504(d), would give the government power to deport people before a federal judge could hear their challenges, even where the law clearly allows judicial review, by posing serious barriers to the judge's ability to stay deportation while considering the case. The provision would overturn rulings of four federal appeals courts that found that the very stringent standard that applies for a judge to grant a request to stop deportation altogether under by INA § 242(f)(2) does not apply to a court's ability to temporarily delay deportation while it considers the case. See, e.g., Mohammed v. Reno, 309 F.3d 95 (2d Cir. 2002) (on appeal from habeas review of removal order); Beijani v. INS, 271 F.3d 670 (6th Cir. 2001); Andreiu v. Ashcroft, 253 F.3d 477 (9th Cir. 2001) (en banc); Lal v. Reno, 2000 WL 831801 (7th Cir. June 26, 2000) (unpublished); but see Weng v. Attorney General, 287 F.3d 1335 (11th Cir. 2002). As one court noted, in rejecting the interpretation the DOJ is now seeking to enact in this legislation, "This would effectively require the automatic deportation of large numbers of people with meritorious claims, including every applicant who presented a case of first impression." Andreiu, 253 F.3d at 48