
THREAT TO CIVIL LIBERTIES OR CONSTITUTIONAL SHIELD?

THREAT TO CIVIL LIBERTIES

ADVOCATE: David Cole, Professor of Law, Georgetown University Law Center

SOURCE: Testimony during hearings on, "Continued Oversight of the USA Patriot Act," U.S. Senate Committee on the Judiciary May 10, 2005

CONSTITUTIONAL SHIELD

ADVOCATE: Alberto R. Gonzales, U.S. Attorney General

SOURCE: Testimony during hearings on, "Oversight of the USA Patriot Act," U.S. House of Representatives Committee on the Judiciary April 6, 2005

For most Americans, September 11, 2001, began well. It was sunny and 66°F at 8:00 A.M. in New York City. On the East Coast, people were arriving at work and otherwise beginning their days. Around the rest of the country, most folks were getting up or enjoying that last hour or two of sleep. All was normal.

Then at 8:45 A.M. an airliner smashed into the north tower of the World Trade Center. Within little more than an hour, a another jet liner crashed into the south tower, a third dove into the Pentagon, and a fourth went down in a field near Pittsburgh. All tolled, 19 terrorists, 33 crewmembers, 219 passengers, and more than 3,000 people on the ground died that morning.

The impact on the Americans was profound. The attacks marked the "End of Illusion," as columnist Robert J. Samuelson entitled a *Washington Post* essay. In addition to the physical damage, he wrote, "What was destroyed...[was] Americans' dreamlike feeling [of being] insulated from the rest of the world."

The U.S. reaction was dramatic. President George W. Bush soon ordered U.S. forces into Afghanistan to attack al-Qaeda and the Taliban regime. Congress quickly approved military action, and polls found nearly 90% of Americans agreed. The impact of 9/11 on U.S. foreign policy also included the formulation of the Bush Doctrine and the subsequent invasion of Iraq.

The political shock waves from 9/11 also rippled inward. Amid their shattered sense of security, Americans sought safety and were willing, at least temporarily, to surrender some of their civil liberties to get it. When asked less than a week after the attack, "Would you support new laws to strengthen security measures against terrorism, even if that meant reducing privacy protections?" 78% said yes, 14% replied no, and 8% were unsure.

Americans soon got what they wanted. Bush proposed legislation to greatly increase the ability of government agencies to conduct wiretaps and other covert operations and to ease the barriers to U.S. intelligence agencies conducting investigations within the country. In an anxiety-ridden atmosphere, the USA Patriot Act ("The

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001”) quickly passed both houses of Congress by huge margins and was signed into law. Among other things, it:

- Eases the authorization process for wiretaps, searches, and other covert activity. Standards for judicially authorized actions are lower; in limited circumstances action can be taken on authorization of the U.S. Attorney General.
- Permits surveillance of electronic communications, including e-mail and voice-mail and of communications records, such as Web sites visited.
- Eases barriers to domestic operations by intelligence agencies. This can now occur when foreign intelligence is a significant, no longer the only, concern.
- Permits “roving” surveillance of whatever communications device a subject is using, rather than being restricted to a single device.
- Allows access to information such as library records, book store purchases, student records (of foreign students) and also many tangible item controlled by rental companies, such as automobiles previously rented by a suspect.
- Expands the use of searches conducted without an individual’s knowledge or a requirement that the government reveal what it seized during the search.

The following readings by advocates David Cole and Alberto Gonzales provide more detail on the Patriot Act. But you may want to see it in its entirety at: http://www.fincen.gov/pa_main.html. Detailed knowledge will help you evaluate the worries of some that without the act the country stands virtually defenseless before terrorism and the voices of others who claim that under the act, CIA agents will soon be bugging your home. Neither extreme is likely. So proceed with caution in your evaluation.

POINTS TO PONDER

- Read the following debates with almost two contradictory thoughts in mind. One is that it is healthy for citizens in a democracy to be leery of any form of covert government intrusion. At the same time, though, bear in mind that most of these methods are not new, only expanded, and the process for agencies to use them has been made less restrictive, not eliminated. This is an issue of balance, not right or wrong.
- One of the oft-quoted remarks of Benjamin Franklin is, “They that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety.” Is this a bit of enduring wisdom from the “sage of Philadelphia,” or is it a shibboleth from the man who also recommended the turkey become the national symbol? Would the maxim, “an ounce of prevention is worth a pound of cure,” be more appropriate?
- The ability of the government under the Patriot Act to monitor non-citizens, such as foreign students, is much greater than for citizens. Is this appropriate, or should most or all of the same civil liberties enjoyed by citizens also be extended for visiting foreign nationals?

Anti-Terrorist Legislation: Threat to Civil Liberties

DAVID COLE

I want to make three points. First, the Patriot Act debate must be understood in context. The debate is fundamentally driven by concerns not only about the four corners of the legislation itself, but by what it reflects about the Bush Administration's approach toward civil liberties in the "war on terrorism." Full Congressional consideration of the concerns expressed around the nation about the Patriot Act, therefore, must not be limited to the sixteen specific sunset provisions [those which expire at a set time unless reenacted], and not even to the Patriot Act itself, but should also consider the impact of executive initiatives outside the Act that have raised serious civil liberties issues. I will first seek to set out these broader concerns as background for the Patriot Act debate, and urge that Congress consider the Patriot Act inquiry the beginning, not the end, of its inquiry into civil liberties in the war on terrorism.

Second, while several of the Patriot Act provisions that are subject to the sunset raise substantial civil liberties concerns, other provisions, not sunsetted, raise even more grave constitutional problems. To my mind, the worst provisions from a civil liberties standpoint are those addressing immigration and material support to "terrorist organizations." I will spend the bulk of my time addressing these provisions, particularly as others on this panel will focus on the sunset provisions.

Third, in my view, of the Patriot Act's sunset provisions, Section 218 raises the most substantial constitutional questions, and calls for significant reforms.

That provision is often credited for bringing down "the wall" between foreign intelligence and law enforcement. That claim is greatly exaggerated. Moreover, Section 218's enactment creates a range of very serious constitutional concerns about the scope of FISA authority and the procedures for introducing FISA evidence in criminal trials that merit sustained Congressional consideration.

I. THE PATRIOT ACT DEBATE IN CONTEXT

Debate about the Patriot Act has been heated almost since its enactment. While only a single Senator, Russell Feingold, voted against it when it was passed just six weeks after 9/11, six states (Alaska, Hawaii, Idaho, Maine, Montana, and Vermont) and over 370 cities and towns have since then enacted resolutions condemning the civil liberties abuses of the Patriot Act and of the Bush Administration's war on terrorism more generally. A bipartisan coalition of liberal and conservative groups has formed an alliance to restore checks and balances, and a tripartisan caucus has formed in the House with the same goals in mind. A bipartisan coalition in the Senate has introduced the SAFE Act, designed to amend many of the surveillance provisions of the Patriot Act.

Defenders of the Patriot Act often lament that in this debate, the Act gets an undeservedly bad rap. It's true that the Act sometimes gets blamed for things with which it has nothing to do. Indeed, many of the worst human rights abuses committed by the Bush Administration in

the name of the “war on terror” are not attributable to the Patriot Act—including the pretextual use of immigration law and the material witness law to lock up thousands of Arab and Muslim foreign nationals who had nothing to do with terrorism; the indefinite detention of some persons, including U.S. citizens, as “enemy combatants,” without any trial or even hearing; the development and application of computer data mining programs that afford the government ready access to a wealth of private information about all of us without any basis for suspicion; the FBI’s monitoring of public meetings and religious services without any basis for suspecting criminal activity under guidelines relaxed by John Ashcroft; and the use of “coercive interrogation” to extract information from suspects in the war on terror, by such tactics as “waterboarding,” in which the suspect is made to fear that he is drowning in order to “encourage” him to talk.

To take just one example, consider the Administration’s use of immigration law to embark on a nationwide campaign of ethnic profiling targeting foreign nationals of Arab and Muslim descent. The Administration called in 80,000 men for “special registration,” simply because they came from Arab and Muslim countries. The FBI sought to interview 8,000 young men, again simply because they came from Arab and Muslim countries. And the government has admitted to detaining over 5,000 foreign nationals, nearly all of them Arab and Muslim, in anti-terrorism preventive detention initiatives since 9/11. Many of those detained were initially arrested without any charges at all. They were detained even where the government had no factual basis for believing that they were dangerous or a risk of flight. Men were locked up and designated “of interest” on the basis of such information as a

tip that “too many Middle Eastern men” were working at a convenience store. They were held in secret and tried in secret. And in many instances, they were held long after their immigration cases were resolved, simply because the FBI had not yet “cleared” them of connections to terrorism. These measures were putatively designed to identify terrorists. Yet of the 80,000 registered, 8,000 interviewed, and 5,000 detained, not a single one stands convicted of a terrorist crime to this day.

These and many other initiatives undertaken in our name unquestionably constitute abuses of basic liberties—from the right to privacy to the right not to be locked up arbitrarily to the right not to be tortured. But they did not stem from the Patriot Act. The Patriot Act has nonetheless become a symbol for the Administration’s disregard for basic civil liberties and constitutional principles because it was the Administration’s first salvo in the war on terrorism, and because its approach is emblematic of so much of the Administration’s subsequent actions. It infringes constitutional freedoms, discriminates against foreign nationals, and undermines checks and balances on executive power. Moreover, it was adopted, like so many other anti-terrorism initiatives, without sufficient deliberation, and with virtually no attention paid to the costs to liberty and freedom posed by its reforms. As such, it is a fitting symbol for a widespread unease with the Administration’s tactics in the war on terror.

The fact that so many civil liberties abuses have arisen outside the Patriot Act does not relieve Congress of its responsibility to investigate these abuses and to provide corrective legislation where appropriate. Congress could, for example, expressly bar the government from inflicting torture and cruel, inhuman, and degrading treatment on any of its detainees anywhere in

the world, but it has not. Congress could call for an Independent Commission to investigate the torture scandal, but it has not. Congress could place limits on political spying by the FBI, but it has not. Congress could ensure that data mining programs build in privacy protections, but again it has not. In short, the concerns expressed by many Americans about the Patriot Act go far beyond the literal terms of that document. So, too, should Congress's oversight and inquiry.

It is worth comparing judicial and legislative responses to the war on terrorism. The courts have begun to play an important checking role in the war on terror. They have rejected the Bush Administration's assertion that it could lock up anyone anywhere in the world without judicial review. They have required that the detainees at Guantanamo be provided with access to counsel. They have invalidated the processes employed by the Combatant Status Review Tribunals and the military tribunals. They have declared unconstitutional various provisions of the Patriot Act. They have rejected a Justice Department regulation that permitted immigration prosecutors to keep immigrants detained even after immigration judges found no basis for their detention. They have ruled that they have jurisdiction to consider a habeas petition from a U.S. citizen held for twenty months without charges in Saudi Arabia allegedly at U.S. behest. They have required the Pentagon, FBI, and CIA to disclose extensive records relating to the torture scandal. They have declared unconstitutional the government's practice of holding immigration hearings entirely in secret. And they have thrown out terrorism convictions based on prosecutorial misconduct.

Never before have courts played such an important checking role in the context of a national security crisis. Perhaps the courts

have learned the lesson of excessive deference in World War I, World War II, and the Cold War. Perhaps they have learned the lesson of the importance of checks and balances of the Watergate era. Whatever the reason, the courts have played an increasingly significant checking function.

But the courts are not the only branch with responsibility to uphold the Constitution and to check aggrandizing behavior by the Executive. Congress shares that responsibility. With a few exceptions, Congress has not played that role in the current crisis. The Patriot Act debate is a welcome start, but it should be only the beginning.

II. IMMIGRATION AND MATERIAL SUPPORT

Much of the Patriot Act is uncontroversial from a civil liberties perspective. Provisions increasing resources for patrolling the northern border, strengthening money laundering laws, eliminating some barriers to information sharing between law enforcement and intelligence officials, and improving visa processing, raise few concerns. But many provisions of the Patriot Act are deeply troubling from a civil liberties standpoint. And in many instances, the reforms they introduce have not been shown to have made us safer. I will focus my remarks on the immigration and material support provisions, because these provisions simultaneously raise the most significant constitutional concerns and have received the least attention.

A. Immigration Provisions

The immigration provisions of the Patriot Act, Sections 411 and 412, authorize exclusion of foreign nationals for speech, deportation for innocent associations with disfavored groups, and detention without charges. They go far beyond any legitimate need to protect the nation

from terrorist threats. And they infringe on basic rights of speech, association, and due process. Yet Congress has not taken up these concerns, and is poised to make the problems far worse in a little-noticed part of the Iraq supplemental appropriations bill approved by the House on May 5, 2005, and slated for a vote in the Senate this week.

1. Deportation for Associations

Section 411 of the Patriot Act allows the government to expel foreign nationals—even long-time lawful permanent residents—based solely on their association with a disfavored organization. The Act permits deportation for “material support” to any organization blacklisted as “terrorist” by the Secretary of State or the Attorney General. It is no defense to show that one’s support to the group furthered only lawful, nonviolent ends, nor is it any defense to show that the group has not engaged in any terrorist activities. If this law had been on the books in the 1980s, any foreign national who donated to the African National Congress for its largely lawful, nonviolent opposition to apartheid in South Africa would have been deportable, because the State Department designated the African National Congress a terrorist group until it came to power in South Africa with the fall of apartheid.

The reach of the Patriot Act deportation provisions is illustrated by a current case I am handling for the Center for Constitutional Rights. It involves Khader Hamide and Michel Shehadeh, two Palestinians in Los Angeles who have lived here as lawful permanent residents for more than thirty years each. They have never been charged with a crime. Yet the government is seeking their deportation under the Patriot Act, passed in 2001, for conduct they engaged in nearly two decades earlier, in the 1980s. The government alleges that they are deportable under

the Patriot Act for having distributed magazines of a Palestine Liberation Organization faction, and for having raised money for humanitarian aid to Palestinians in the West Bank and Lebanon. On the government’s view, it does not matter that these activities were lawful at the time they were engaged in, or that they are protected by the First Amendment.

A second case that illustrates how far-reaching this provision is involves the deportation of an Indian man. In that case, the court held that the Patriot Act authorized the man’s deportation for having set up a tent for religious services and food, simply because some unidentified members of a designated terrorist organization reportedly came to the services and partook of the food. There was no showing that the Indian man intended to further any terrorist activity by setting up the tent. Such deportations do not make the United States safer.

2. Ideological Exclusion

Section 411 is even more expansive with regard to the grounds for denying foreign nationals entry in the first place. It resurrects the practice of “ideological exclusion,” keeping people out of the country not for their past or current conduct, not even based on any reasonable concern that they might engage in criminal or terrorist conduct once here, but based solely on their speech. If they say something that the Secretary of State considers to “endorse terrorism,” they may be kept out. In 2004, the Bush Administration apparently invoked this provision in denying a visa to Tariq Ramadan, a highly respected Swiss scholar of Islam who had been offered a chair at Notre Dame.

3. Preventive Detention Without Charges

Section 412 of the Patriot Act allows the Attorney General to lock up foreign

nationals without charges for seven days, and indefinitely thereafter if they are charged with an immigration violation. The law does not require any showing that the foreign national poses a danger to the community or a risk of flight—the only two constitutionally valid reasons for preventive detention. And it permits the Attorney General to keep the foreign national locked up even after he has been granted relief from removal, which is akin to saying that the government can keep a prisoner behind bars even after the governor has granted him a pardon. The government has not yet invoked this provision, calling into question its claim that the authority was absolutely essential to fight terrorism....

B. Criminal Material Support Provisions

The Patriot Act also expanded the most expansive “anti-terrorism” criminal law on the books prior to its passage, which criminalizes the provision of “material support” to designated “terrorist organizations.” The Patriot Act expanded this already expansive law by criminalizing pure speech. It amended the criminal ban on material support to designated terrorist organizations by banning “expert advice or assistance”—without regard to what the advice consists of. In a case that I am handling for the Center for Constitutional Rights, a federal court declared this Patriot Act provision unconstitutional. In that case, I represent a human rights organization that seeks to provide human rights training to a Kurdish organization in Turkey that has been designated a “terrorist organization.” The government has argued that it may criminalize as “expert advice” this human rights organization’s advice on human rights advocacy, without regard to the fact that the advice was being offered to encourage the group to pursue peaceful

means to resolve its disputes and to discourage resort to violence. The court held the provision unconstitutionally vague.

In the first prosecution brought under this provision, the government argued that a student at the University of Idaho should be found guilty for operating a web site that featured links to other web sites that in turn included speeches preaching violent jihad. It was irrelevant, the government contended, that there was no evidence that the student himself had advocated any violence. An Idaho jury acquitted the student on all terrorism charges....

C. Administrative Material Support Provisions

Section 106 of the Patriot Act amends an administrative scheme that has also been used to target “material support” of organizations and individuals deemed “terrorist.” This provision authorizes the government to freeze assets of domestic corporations and individuals without showing any violation of law, and without any meaningful adversarial testing of its basis for doing so. It allows the government to freeze all assets of any individual or entity simply by declaring that it is “under investigation” for violating an economic embargo on providing goods or services to a designated “terrorist.” The government has placed such embargoes on dozens of organizations and hundreds of individuals, all around the world. The government claims that the authority to designate stems from the International Emergency Economic Powers Act, which never mentions the word “terrorist.” There is no statutory or even regulatory definition of a “terrorist” for purposes of IEEPA, and therefore a terrorist is whatever the Administration says it is.

Section 106 permits the Treasury Department to freeze all assets of a U.S.

citizen or corporation merely by stating that they are “under investigation” for having a financial transaction with such an embargoed entity. The provision then allows the Treasury Department to defend its actions in court by submitting secret evidence that the challenger cannot see or rebut. This authority has been used to freeze the assets of several of the largest Muslim charities in the United States. When the charities have sued in federal court to challenge their designation, they have been met with secret evidence. Moreover, given that there is no statutory or regulatory definition of a designated “terrorist” under IEEPA, it is entirely unclear what standard courts are to apply in assessing whether a designation is appropriate. This law gives the Executive branch a wide-ranging blank check to freeze the assets of any entity or person it chooses, under a literally standardless authority, and then to defend its actions in secret. It is possible that some or all of the half-dozen or so charities that the government has targeted were guilty of funneling money to further terrorism. But it is also possible that all of the charities are entirely innocent. We cannot know, because the Patriot Act eliminated any fair process for distinguishing the innocent from the guilty.

There is no question that funding terrorist activity should be prohibited. It was prohibited long before the Patriot Act. What the criminal and administrative provisions added by the Patriot Act do is extend government sanctions—including substantial prison sentences—to conduct that is not intended to further terrorist activity, and that in fact does not further terrorist activity. In addition, the Treasury Department provisions deprive those targeted of any fair opportunity to show that their actions had nothing to do with terrorism. In the name of cutting off funds for terrorism, then, these provisions crim-

inalize speech and deny citizens basic due process rights.

III. SECTION 218 AND “THE WALL”

Of the surveillance provisions that are subject to sunset, to my mind the most constitutionally dubious may be Section 218. That provision substantially expanded authority to conduct wiretaps and searches under the Foreign Intelligence Surveillance Act (FISA) without probable cause of criminal activity. The number of FISA searches has dramatically increased since the Patriot Act was passed, and for the first time now exceeds the number of wiretaps issued on probable cause of criminal activity. Yet because of the secrecy that surrounds FISA searches, we know virtually nothing about them. The target of a FISA search is never notified that he was searched, unless evidence from the search is subsequently used in a criminal prosecution. Even then the defendant cannot see the application for the search, and therefore cannot meaningfully test its legality in court. And while the Attorney General is required to file an extensive report on his use of criminal wiretaps, listing the legal basis for each wiretap, its duration, and whether it resulted in a criminal charge or conviction, no such information is required under FISA. The annual report detailing use of the criminal wiretap authority exceeds 100 pages; the report on the use of FISA is a one-page letter.

Section 218 of the Patriot Act expanded the reach of FISA searches and wiretaps by allowing their use even where the government’s primary purpose for investigating is criminal law enforcement. Prior to the Patriot Act, where the government’s primary focus was criminal law enforcement, it was required to satisfy the criminal probable cause standards set forth by the Fourth Amendment of the Constitution. It had to show probable

cause that the target of the search had evidence of crime in his possession, or had committed a crime. Where, by contrast, the government's principal purpose was not criminal law enforcement but foreign intelligence gathering, it could obtain a warrant for a search or wiretap under FISA simply by showing that the target was an "agent of a foreign power." That term is loosely defined to include any employee of any political organization made up of a majority of noncitizens. The warrant application need not show probable cause of criminal activity. Thus, literally applied, FISA would authorize a search or wiretap of a British lawyer working for Amnesty International, without any requirement of suspicion that the lawyer be engaged in illegal activity.

The Patriot Act extended that loose standard to investigations undertaken primarily for criminal law enforcement purposes, so long as "a significant purpose" of the search is also foreign intelligence gathering. A secret court upheld this amendment in a secret one-sided appeal by the government soon after the Patriot Act was enacted.

Defenders of this provision often claim that it eliminated a "wall" between criminal law enforcement and foreign intelligence agencies. But that is an exaggeration. FISA did not require such a wall before the Patriot Act was enacted. It did not bar prosecutors or law enforcement agents from turning over information to intelligence agents, nor did it stop foreign intelligence agents from sharing with criminal prosecutors evidence of crime that they had discovered in their investigations, whether under FISA or otherwise. Evidence obtained in FISA searches could be, and was, used in criminal trials long before the Patriot Act.

There were unquestionably many barriers to information sharing before 9/11.

But their principal source was not FISA, but administrative and bureaucratic culture. Agencies were engaged in turf wars, and there were few if any mechanisms or incentives in place to break down the institutional boundaries between agencies. Legitimate concerns about not revealing sources make information sharing difficult even in the most well organized operations. But the blame for these problems cannot be laid at the foot of FISA.

Critics of the wall sometimes suggest that before the Patriot Act, once a foreign intelligence investigation became primarily a criminal investigation, the government would have to take down the tap. But that is also not true. Once an investigation became primarily criminal in nature, government agents would simply have to satisfy the standards applicable to criminal investigations—namely, by showing that they had probable cause that the tap would reveal evidence of criminal conduct. The tap or the search could then continue. If an investigation has become primarily criminal in nature, it should not be too much to ask that the government show probable cause of criminal conduct to carry out a search or wiretap.

Indeed, the Constitution demands no less. FISA's constitutionality turns on an untested assumption that the government may engage in searches and wiretaps for foreign intelligence purposes on a lower showing of suspicion than is required for criminal law investigations. FISA does not require the government to show probable cause that evidence of a crime will be found, but only probable cause that the target of the search is an "agent of a foreign power." "Foreign power" is in turn defined so broadly that it encompasses any political organization comprised of a majority of noncitizens. Where "U.S. persons" are the target of a FISA search, the

government must make additional showings, but to search the home of a foreign national here on a work permit, for example, the government need only show that he's an employee of an organization made up principally of noncitizens. It need not show that the individual be engaged in any criminal wrongdoing whatsoever, much less terrorism.

If FISA searches are constitutional, then, they must be justified on the basis of some application of the “administrative search” exception to the general Fourth Amendment rule requiring probable cause and a warrant for criminal law enforcement searches. That exception permits searches in limited settings on less than probable cause where the search serves some special need beyond criminal law enforcement. The FISA Court of Review relied on precisely this exception to find FISA searches valid. But the Supreme Court has carefully limited the “administrative search” exception to situations in which the government is pursuing a special need divorced from criminal law enforcement—e.g., highway or railroad safety, secondary school discipline, or enforcement of an administrative regime. It has refused to apply the exception where the government is engaged in criminal law enforcement, as in a checkpoint to search for cars carrying drugs. And the Court has also refused to apply the exception where the government has a “special need,” but is using criminal law enforcement to further that need. Thus, it struck down a hospital program that subjected pregnant mothers to drug tests for the ultimate purpose of protecting the health of the fetus, where the hospital shared the test results with prosecutors in order to threaten the mothers with criminal prosecution if they did not seek drug treatment.

Where an investigation becomes primarily focused on criminal law enforce-

ment, therefore, the “administrative search” exception no longer applies, and Supreme Court doctrine would compel the government to meet the traditional standards of criminal probable cause. Before the Patriot Act, FISA conformed to that requirement. By abandoning that distinction and allowing searches on less than probable cause where the government is primarily seeking criminal prosecution, Section 218 raises a serious constitutional question. Thus, Section 218 was not only unnecessary to bring down the wall, but may render FISA unconstitutional.

Two reforms short of repeal are worth considering. First, if Section 218 is to be retained, thereby expanding the scope of FISA searches, Congress should revisit FISA's definition of “agent of a foreign power” and “foreign intelligence information.” Those terms, particularly as applied to non-U.S. persons, are sweeping, and have nothing to do with terrorism. As noted above, the definitions are so broad that they would authorize a tap of a British lawyer for Amnesty International, to gather any information that might relate to foreign affairs. It is one thing to claim that FISA authorities should be available to investigate terrorism; it is another matter entirely to extend those same powers to persons engaged in no criminal activity whatsoever. Thus, the definitions of “agent of foreign power” and “foreign intelligence information” should be narrowed.

Finally, Section 218 and other reforms have made it increasingly likely that information obtained through FISA wiretaps and searches will be used against defendants in criminal cases. In light of these developments, a useful reform at this point would be a provision permitting criminal defendants—or their cleared counsel—an opportunity to review the initial application for the FISA wiretap or search when contesting the admissibility

of evidence obtained through a FISA search. Under current law, they have no such opportunity. Without access to the warrant application, defendants and their attorneys cannot meaningfully challenge the legality of the tap or search in the first place. And when government officials know that their actions will never see the light of day, they are more likely to be tempted to cut corners. An amendment requiring disclosure of FISA applications where evidence is sought to be used in a criminal trial would encourage adherence to the law by putting federal officials on notice that at some point the legality of the FISA warrant would be subjected to adversarial testing. Concerns about confidentiality could be met by limiting access to cleared counsel where necessary, and/or by applying the protections of the Classified Information Procedures Act. But there is no good reason for the current blanket exemption against the production of all such applications in criminal cases.

The presumption should be in favor of adversarial testing where evidence is to be used in a criminal case.

CONCLUSION

In its treatment of foreign nationals, its expansive definition of “material support” to terrorist groups, and its authorization of surveillance not tied to probable cause of criminal activity, the Patriot Act has substantially eroded fundamental constitutional freedoms. It did so in the name of fighting terrorism, but many of its authorities are written far more broadly than that motive would warrant—penalizing speech and association, eliminating fair procedures for distinguishing the guilty from the innocent, and authorizing searches without probable cause and secrecy without compelling justification. Measures more carefully tailored to terrorist activity might well have been justified. But the last thing the Patriot Act could ever be accused of is careful tailoring.

Anti-Terrorist Legislation: Constitutional Shield:

ALBERTO R. GONZALES

It is my pleasure to discuss the USA Patriot Act. Approximately three-and-a-half years ago, our nation suffered a great tragedy. Thousands of our fellow citizens were murdered at the World Trade Center, the Pentagon, and a field in rural Pennsylvania. We will never forget that day or the heroes who perished on that hallowed ground. Forever in our nation's collective memory are stories of the New York City firefighters who rushed into burning buildings so that others might live and of the brave passengers who brought down United Airlines Flight 93 before it could reach Washington, DC, and the messages from those trapped in the World Trade Center saying their last goodbyes to loved ones as they faced certain death will stay forever in our hearts.

In the wake of this horrific attack on American soil, we mourned our nation's terrible loss. In addition, we came together in an effort to prevent such a tragedy from ever happening again. Members of both parties worked together on legislation to ensure that investigators and prosecutors would have the tools they need to uncover and disrupt terrorist plots. Additionally, members joined hands across the aisle to guarantee that our efforts to update and strengthen the laws governing the investigation and prosecution of terrorism remained firmly within the parameters of the Constitution and our fundamental national commitment to the protection of civil rights and civil liberties.

The result of this collaboration was the Patriot Act, which passed both Houses of the Congress with overwhelming biparti-

san majorities and was signed into law by President Bush on October 26, 2001. In the past three-and-a-half years, the Patriot Act has been an integral part of the federal government's successful prosecution of the war against terrorism. Thanks to the Act, we have been able to identify terrorist operatives, dismantle terrorist cells, disrupt terrorist plots, and capture terrorists before they have been able to strike.

Many of the most important provisions of the Patriot Act, however, are scheduled to expire at the end of this year. Therefore, I am here today primarily to convey one simple message: All provisions of the Patriot Act that are scheduled to sunset at the end of this year must be made permanent. While we have made considerable progress in the war against terrorism in the past three-and-a-half years, al Qaeda and other terrorist groups still pose a grave threat to the safety and security of the American people. The tools contained in the Patriot Act have proven to be essential weapons in our arsenal to combat the terrorists, and now is not the time for us to be engaging in unilateral disarmament. Moreover, many provisions in the Act simply updated the law to reflect recent technological developments and have been used, as was intended by Congress, not only in terrorism cases, but also to combat other serious criminal conduct. If these provisions are not renewed, the department's ability to combat serious offenses such as cybercrime, child pornography, and kidnappings will also be hindered....

I would like to explain how key provisions of the Patriot Act have helped to pro-

tect the American people. I will particularly focus on those sections of the Act that are scheduled to expire at the end of 2005. To begin with, I will discuss how the Patriot Act has enhanced the federal government's ability to share intelligence. Then, I will explain how the Patriot Act provided terrorism investigators with many of the same tools long available to investigators in traditional criminal cases. Additionally, I will explore how the Patriot Act updated the law to reflect new technology. And finally, I will review how the Act protects the civil liberties of the American people and respects the important role of checks and balances within the federal government.

INFORMATION SHARING

The most important reforms contained in the Patriot Act improved coordination and information sharing within the federal government. Prior to the attacks of September 11, 2001, our counterterrorism efforts were severely hampered by unnecessary obstacles and barriers to information sharing. These obstacles and barriers, taken together, have been described as a "wall" that largely separated intelligence personnel from law enforcement personnel, thus dramatically hampering the department's ability to detect and disrupt terrorist plots.

It is vitally to understand how the "wall" was developed and how it was dismantled, not for the purpose of placing blame but rather to ensure that it is never rebuilt. Before the passage of the Patriot Act, the Foreign Intelligence Surveillance Act (FISA) [1978] mandated that applications for orders authorizing electronic surveillance or physical searches under FISA were required to include a certification that "the purpose" of the surveillance or search was to gather foreign intelligence information. This requirement, however,

came to be interpreted by the courts and later the Department of Justice to require that the "primary purpose" of the collection was to obtain foreign intelligence information rather than evidence of a crime. And, because the courts evaluated the department's purpose for using FISA, in part, by examining the nature and extent of coordination between intelligence and law enforcement personnel, the more coordination that occurred, the more likely courts would find that law enforcement, rather than foreign intelligence, had become the primary purpose of the surveillance or search, a finding that would prevent the court from authorizing surveillance under FISA. As a result, over the years, the "primary purpose" standard had the effect of constructing a metaphorical "wall" between intelligence and law enforcement personnel.

During the 1980s, a set of largely unwritten rules only limited information sharing between intelligence and law enforcement officials to some degree. In 1995, however, the Department [of Justice] established formal procedures that limited the sharing of information between intelligence and law enforcement personnel. The promulgation of these procedures was motivated in part by the concern that the use of FISA authorities would not be allowed to continue in particular investigations if criminal prosecution began to overtake intelligence gathering as an investigation's primary purpose.

As they were originally designed, the procedures were intended to permit a degree of interaction and information sharing between prosecutors and intelligence officers, while at the same time ensuring that the FBI would be able to obtain or continue FISA surveillance and later use the fruits of that surveillance in a criminal prosecution. Over time, however, coordination and information sharing

between intelligence and law enforcement investigators became even more limited in practice than was permitted in theory. Due both to the complexities of the restrictions on information sharing and to a perception that improper information sharing could end a career, investigators often erred on the side of caution and refrained from sharing information. The end result was a culture within the department sharply limiting the exchange of information between intelligence and law enforcement officials.

In hindsight, it is difficult to overemphasize the negative impact of the “wall.” In order to uncover terrorist plots, it is essential that investigators have access to as much information as possible. Often, only by piecing together disparate and seemingly unrelated points of information are investigators able to detect suspicious patterns of activity, a phenomenon generally referred to as “connecting the dots.” If, however, one set of investigators has access to only one-half of the dots, and another set of investigators has access to the other half of the dots, the likelihood that either set of investigators will be able to connect the dots is significantly reduced.

The operation of the “wall” was vividly illustrated in testimony from Patrick Fitzgerald, U.S. Attorney for the Northern District of Illinois, before the Senate Judiciary Committee:

I was on a prosecution team in New York that began a criminal investigation of Osama Bin Laden in early 1996. The team—prosecutors and FBI agents assigned to the criminal case—had access to a number of sources. We could talk to citizens. We could talk to local police officers. We could talk to other U.S. government agencies. We could talk to foreign police officers. Even foreign intelligence personnel. And foreign citizens. And we did all those things as often as we could.

We could even talk to al Qaeda members—and we did. We actually called several members and associates of al Qaeda to testify before a grand jury in New York. And we even debriefed al Qaeda members overseas who agreed to become cooperating witnesses.

But there was one group of people we were not permitted to talk to. Who? The FBI agents across the street from us in lower Manhattan assigned to a parallel intelligence investigation of Osama Bin Laden and al Qaeda. We could not learn what information they had gathered. That was “the wall.”

Thanks in large part to the Patriot Act; this “wall” has been lowered. Section 218 of the Act, in particular, helped to tear down the “wall” by eliminating the “primary purpose” requirement under FISA and replacing it with a “significant purpose” test. Under section 218, the department may now conduct FISA surveillance or searches if foreign-intelligence gathering is a “significant purpose” of the surveillance or search. As a result, courts no longer need to compare the relative weight of the “foreign intelligence” and “law enforcement” purposes of a proposed surveillance or search and determine which is the primary purpose; they simply need to determine whether a significant purpose of the surveillance is to obtain foreign intelligence. The consequence is that intelligence and law enforcement personnel may share information much more freely without fear that such coordination will undermine the department’s ability to continue to gain authorization for surveillance under FISA.

Section 218 of the Patriot Act not only removed what was perceived at the time as the primary impediment to robust information sharing between intelligence and law enforcement personnel; it also provided the necessary impetus for the removal

of the formal administrative restrictions as well as the informal cultural restrictions on information sharing. Thanks to the Patriot Act, the department has been able to move from a culture where information sharing was viewed with a wary eye to one where it is an integral component of our counterterrorism strategy. Following passage of the Act, the department adopted new procedures specifically designed to increase information sharing between intelligence and law enforcement personnel. Moreover, Attorney General [John] Ashcroft instructed every U.S. Attorney across the country to review intelligence files to discover whether there was a basis for bringing criminal charges against the subjects of intelligence investigations. He also directed every U.S. Attorney to develop a plan to monitor intelligence investigations, to ensure that information about terrorist threats is shared with other agencies, and to consider criminal charges in those investigations.

The increased information sharing facilitated by section 218 of the Patriot Act has led to tangible results in the war against terrorism: plots have been disrupted; terrorists have been apprehended; and convictions have been obtained in terrorism cases. Information sharing between intelligence and law enforcement personnel, for example, was critical in successfully dismantling a terror cell in Portland, Oregon, popularly known as the “Portland Seven,” as well as a terror cell in Lackawanna, New York. Such information sharing has also been used in the prosecution of [numerous other individuals who have pled guilty or been convicted of crimes relating to terrorism]....

While the “wall” primarily blocked the flow of information from intelligence investigators to law enforcement investigators, another set of barriers, before the passage of the Patriot Act, often prevent-

ed law enforcement officials from sharing information with intelligence personnel and others in the government responsible for protecting the national security. Federal law, for example, was interpreted generally to prohibit federal prosecutors from disclosing information from grand jury testimony and criminal investigative wiretaps to intelligence and national defense officials even if that information indicated that terrorists were planning a future attack, unless such officials were actually assisting with the criminal investigation. Sections 203(a) and (b) of the Patriot Act, however, eliminated these obstacles to information sharing by allowing for the dissemination of that information to assist federal law enforcement, intelligence, protective, immigration, national defense, and national security officials in the performance of their official duties, even if their duties are unrelated to the criminal investigation. (Section 203(a) covers grand jury information, and section 203(b) covers wiretap information).

Section 203(d), likewise, ensures that important information that is obtained by law enforcement means may be shared with intelligence and other national security officials. This provision does so by creating a generic exception to any other law purporting to bar federal law enforcement, intelligence, immigration, national defense, or national security officials from receiving, for official use, information regarding foreign intelligence or counterintelligence obtained as part of a criminal investigation. Indeed, section 905 of the Patriot Act requires the Attorney General to expeditiously disclose to the Director of Central Intelligence foreign intelligence acquired by the Department of Justice in the course of a criminal investigation unless disclosure of such information would jeopardize an ongoing investigation

or impair other significant law enforcement interests.

The department has relied on section 203 in disclosing vital information to the intelligence community and other federal officials on many occasions. Such disclosures, for instance, have been used to assist in the dismantling of terror cells in Portland, Oregon and Lackawanna, New York, to support the revocation of suspected terrorists' visas, to track terrorists' funding sources, and to identify terrorist operatives overseas.

The information sharing provisions described above have been heralded by investigators in the field as the most important provisions of the Patriot Act. Their value has also been recognized by the 9/11 Commission, which stated in its official report that “[t]he provisions in the act that facilitate the sharing of information among intelligence agencies and between law enforcement and intelligence appear, on balance, to be beneficial.”

If Congress does not act by the end of the year, we will soon take a dramatic step back to the days when unnecessary obstacles blocked vital information sharing. Three of the key information sharing provisions of the Patriot Act, sections 203(b), 203(d), and 218, are scheduled to sunset at the end of the year. It is imperative that we not allow this to happen. To ensure that the “wall” is not reconstructed and investigators are able to “connect the dots” to prevent future terrorist attacks, these provisions must be made permanent.

USING PREEXISTING TOOLS IN TERRORISM INVESTIGATIONS

In addition to enhancing the information sharing capabilities of the department, the Patriot Act also permitted several existing investigative tools that had been used for years in a wide range of criminal investigations to be used in terrorism cases as well.

Essentially, these provisions gave investigators the ability to fight terrorism utilizing many of the same court-approved tools that have been used successfully and constitutionally for many years in drug, fraud, and organized crime cases.

Section 201 of the Patriot Act is one such provision. In the context of criminal law enforcement, federal investigators have long been able to obtain court orders to conduct wiretaps when investigating numerous traditional criminal offenses....Prior to the passage of the Patriot Act, however, certain extremely serious crimes that terrorists are likely to commit were not [permitted under federal law], which prevented law enforcement authorities from using wiretaps to investigate these serious terrorism-related offenses. As a result, law enforcement could obtain under appropriate circumstances a court order to intercept phone communications in a passport fraud investigation but not a chemical weapons investigation or an investigation into terrorism transcending national boundaries.

Section 201 of the Act ended this anomaly in the law by amending the criminal wiretap statute to add the following terrorism-related crimes to the list of wiretap predicates: (1) chemical-weapons offenses; (2) certain homicides and other acts of violence against Americans occurring outside of the country; (3) the use of weapons of mass destruction; (4) acts of terrorism transcending national borders; (5) financial transactions with countries which support terrorism; and (6) material support of terrorists and terrorist organizations.

This provision simply enables investigators to use wiretaps when looking into the full range of terrorism-related crimes. This authority makes as much, if not more, sense in the war against terrorism as it does in traditional criminal investigations; if wiretaps are an appropriate investigative tool to be

utilized in cases involving bribery, gambling, and obscenity, then surely investigators should be able to use them when investigating the use of weapons of mass destruction, acts of terrorism transcending national borders, chemical weapons offenses, and other serious crimes that terrorists are likely to commit.

It is also important to point out that section 201 preserved all of the pre-existing standards in the wiretap statute. For example, law enforcement must file an application with a court, and a court must find that: (1) there is probable cause to believe an individual is committing, has committed, or is about to commit a particular predicate offense; (2) there is probable cause to believe that particular communications concerning that offense will be obtained through the wiretap; and (3) “normal investigative procedures” have been tried and failed or reasonably appear to be unlikely to succeed or are too dangerous.

Section 206 of the Patriot Act, like section 201 discussed above, provided terrorism investigators with an authority that investigators have long possessed in traditional criminal investigations. Before the passage of the act, multipoint or so-called “roving” wiretap orders, which attach to a particular suspect rather than a particular phone or communications facility, were not available under FISA. As a result, each time an international terrorist or spy switched communications providers, for example, by changing cell phones or Internet accounts, investigators had to return to court to obtain a new surveillance order, often leaving investigators unable to monitor key conversations.

Section 206 of the Act amended the law to allow the FISA Court to authorize multi-point surveillance of a terrorist or spy when it finds that the target’s actions may thwart the identification of those specific individuals or companies, such as communications

providers, whose assistance may be needed to carry out the surveillance. Thus, the FISA Court does not have to name in the wiretap order each telecommunications company or other “specified person” whose assistance may be required.

A number of federal courts—including the Second, Fifth, and Ninth Circuits [of the U.S. Court of Appeals]—have squarely ruled that multi-point wiretaps are perfectly consistent with the Fourth Amendment. Section 206 simply authorizes the same constitutional techniques used to investigate ordinary crimes to be used in national-security investigations. Despite this fact, section 206 remains one of the more controversial provisions of the Patriot Act. However, as in the case of multi-point wiretaps used for traditional criminal investigations, section 206 contains ample safeguards to protect the privacy of innocent Americans.

First, section 206 did not change FISA’s requirement that the target of multi-point surveillance must be identified or described in the order. In fact, section 206 is always connected to a particular target of surveillance. For example, even if the Justice Department is not sure of the actual identity of the target of such a wiretap, FISA nonetheless requires our attorneys to provide a description of the target of the electronic surveillance to the FISA Court prior to obtaining multi-point surveillance order.

Second, just as the law required prior to the Act, the FISA Court must find that there is probable cause to believe the target of surveillance is either a foreign power or an agent of a foreign power, such as a terrorist or spy. In addition, the FISA Court must also find that the actions of the target of the application may have the effect of thwarting surveillance before multi-point surveillance may be authorized.

Third, section 206 in no way altered the robust FISA minimization procedures

that limit the acquisition, retention, and dissemination by the government of information or communications involving United States persons.

Section 214 is yet another provision of the Patriot Act that provides terrorism investigators with the same authority that investigators have long possessed in traditional criminal investigations. Specifically, this section allows the government to obtain a pen register or trap-and-trace order in national security investigations where the information to be obtained is likely to be relevant to an international terrorism or espionage investigation. A pen register or trap-and-trace device can track routing and addressing information about a communication—for example, which numbers are dialed from a particular telephone. Such devices, however, are not used to collect the content of communications.

Under FISA, intelligence officers may seek a court order for a pen register or trap-and-trace to gather foreign intelligence information or information about international terrorism. Prior to the enactment of the Patriot Act, however, FISA required government personnel to certify not just that the information they sought to obtain with a pen register or trap-and-trace device would be relevant to their investigation, but also that the particular facilities being monitored, such as phones, were being used by foreign governments, international terrorists, or spies. As a result, it was much more difficult to obtain a pen register or trap-and-trace device order under FISA than it was under the criminal wiretap statute, where the applicable standard was and remains simply one of relevance in an ongoing criminal investigation.

Section 214 of the Act simply harmonized the standard for obtaining a pen register order in a criminal investigation and a national-security investigation by

eliminating the restriction limiting FISA pen register and trap-and-trace orders to facilities used by foreign agents or agents of foreign powers. Applicants must still, however, certify that a pen register or trap-and-trace device is likely to reveal information relevant to an international terrorism or espionage investigation or foreign intelligence information not concerning a United States person. This provision made the standard contained in FISA for obtaining a pen register or trap-and-trace order parallel with the standard for obtaining those same orders in the criminal context. Now, as before, investigators cannot install a pen register or trap-and-trace device unless they apply for and receive permission from the FISA Court.

I will now turn to section 215, which I recognize has become the most controversial provision in the Patriot Act. This provision, however, simply granted national security investigators the same authority that criminal investigators have had for centuries—that is, to request the production of records that may be relevant to their investigation. For years, ordinary grand juries have issued subpoenas to obtain records from third parties that are relevant to criminal inquiries. But just as prosecutors need to obtain such records in order to advance traditional criminal investigations, so, too, must investigators in international terrorism and espionage cases have the ability, with appropriate safeguards, to request the production of relevant records.

While obtaining business records is a long-standing law enforcement tactic that has been considered an ordinary tool in criminal investigations, prior to the Patriot Act it was difficult for investigators to obtain access to the same types of records in connection with foreign intelligence investigations. Such records, for example, could be sought only from common carri-

ers, public accommodation providers, physical storage facility operators, and vehicle rental agencies. In addition, intelligence investigators had to meet a higher evidentiary standard to obtain an order requiring the production of such records than prosecutors had to meet to obtain a grand jury subpoena to require the production of those same records in a criminal investigation.

To address this anomaly in the law, section 215 of the Act made several important changes to the FISA business-records authority so that intelligence agents would be better able to obtain crucial information in important national-security investigations. Section 215 expanded the types of entities that can be compelled to disclose information. Under the old provision, the FBI could obtain records only from “a common carrier, public accommodation facility, physical storage facility or vehicle rental facility.” The new provision contains no such restrictions. Section 215 also expanded the types of items that can be requested. Under the old authority, the FBI could only seek “records.” Now, the FBI can seek “any tangible things (including books, records, papers, documents, and other items).”

I recognize that section 215 has been subject to a great deal of criticism because of its speculative application to libraries, and based on what some have said about the provision, I can understand why many Americans would be concerned. The government should not be obtaining the library records of law-abiding Americans, and I will do everything within my power to ensure that this will not happen on my watch.

Section 215 does not focus on libraries. Indeed, the Patriot Act nowhere mentions the word “library,” a fact that many Americans are surprised to learn. Section 215 simply does not exempt libraries from

the range of entities that may be required to produce records. Now some have suggested, since the department has no interest in the reading habits of law-abiding Americans, that section 215 should be amended to forbid us from using the provision to request the production of records from libraries and booksellers. This, however, would be a serious mistake.

Libraries are currently not safe havens for criminals. Grand jury subpoenas have long been used to obtain relevant records from libraries and bookstores in criminal investigations. In fact, law enforcement used this authority in investigating the Gianni Versace murder case as well as the case of the Zodiac gunman in order to determine who checked out particular books from public libraries that were relevant in those murder investigations. And if libraries are not safe havens for common criminals, neither should they be safe havens for international terrorists or spies, especially since we know that terrorists and spies have used libraries to plan and carry out activities that threaten our national security. The Justice Department, for instance, has confirmed that, as recently as the winter and spring of 2004, a member of a terrorist group closely affiliated with al Qaeda used Internet service provided by a public library to communicate with his confederates.

Section 215, moreover, contains very specific safeguards in order to ensure that the privacy of law-abiding Americans, both with respect to their library records as well as other types of records, is respected. First, section 215 expressly protects First Amendment rights, unlike grand jury subpoenas. Even though libraries and bookstores are not specifically mentioned in the provision, section 215 does prohibit the government from using this authority to conduct investigations “of a United States person solely on the basis of activi-

ties protected by the First Amendment to the Constitution of the United States.” In other words, the library habits of ordinary Americans are of no interest to those conducting terrorism investigations, nor are they permitted to be.

Second, any request for the production of records under section 215 must be issued through a court order. Therefore, investigators cannot use this authority unilaterally to compel any entity to turn over its records; rather, a judge must first approve the government’s request. By contrast, a grand jury subpoena is typically issued without any prior judicial review or approval. Both grand jury subpoenas and section 215 orders are also governed by a standard of relevance. Under section 215, agents may not seek records that are irrelevant to an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities.

Third, section 215 has a narrow scope. It can only be used in an authorized investigation (1) “to obtain foreign intelligence information not concerning a United States person”; or (2) “to protect against international terrorism or clandestine intelligence activities.” It cannot be used to investigate ordinary crimes, or even domestic terrorism. On the other hand, a grand jury may obtain business records in investigations of any federal crime.

Finally, section 215 provides for thorough congressional oversight that is not present with respect to grand-jury subpoenas. On a semi-annual basis, I must “fully inform” appropriate congressional committees concerning all requests for records under section 215 as well as the number of section 215 orders granted, modified, or denied. To date, the department has provided Congress with six reports regarding its use of section 215.

Admittedly, the recipient of an order under section 215 is not permitted to make that order publicly known, and this confidentiality requirement has generated some fear among the public. It is critical, however, that terrorists are not tipped off prematurely about sensitive investigations. Otherwise, their conspirators may flee and key information may be destroyed before the government’s investigation has been completed. As the U.S. Senate concluded when adopting FISA: “By its very nature, foreign intelligence surveillance must be conducted in secret.”

UPDATING THE LAW TO REFLECT NEW TECHNOLOGY

As well as providing terrorism investigators many of the same tools that law enforcement investigators had long possessed in traditional criminal investigations, many sections of the Patriot Act updated the law to reflect new technology and to prevent sophisticated terrorists and criminals from exploiting that new technology. Several of these provisions, some of which are currently set to sunset at the end of this year, simply updated tools available to law enforcement in the context of ordinary criminal investigations to address recent technological developments, while others sought to make existing criminal statutes technology-neutral. I wish to focus on five such provisions of the Act, which are currently set to expire at the end of 2005. The department believes that each of these provisions has proven valuable and should be made permanent.

Section 212 amended the Electronic Communications Privacy Act to authorize electronic communications service providers [such as AOL and other Internet service providers] to disclose communications and records relating to customers or subscribers in an emergency involving the

immediate danger of death or serious physical injury. Before the Patriot Act, for example, if an Internet service provider had learned that a customer was about to commit a terrorist act and notified law enforcement to that effect, the service provider could have been subject to civil lawsuits. Now, however, providers are permitted voluntarily to turn over information to the government in emergencies without fear of civil liability. It is important to point out that they are under no obligation whatsoever to review customer communications and records. This provision also corrected an anomaly in prior law under which an Internet service provider could voluntarily disclose the content of communications to protect itself against hacking, but could not voluntarily disclose customer records for the same purpose.

Communications providers have relied upon section 212 to disclose vital and time-sensitive information to the government on many occasions since the passage of the Patriot Act, thus saving lives. To give just one example, this provision was used to apprehend an individual threatening to destroy a Texas mosque before he could carry out his threat. Jared Bjarnason, a 30-year-old resident of El Paso, Texas, sent an e-mail message to the El Paso Islamic Center on April 18, 2004, threatening to burn the Islamic Center's mosque to the ground if hostages in Iraq were not freed within three days. Section 212 allowed FBI officers investigating the threat to obtain information quickly from electronic communications service providers, leading to the identification and arrest of Bjarnason before he could attack the mosque. It is not clear, however, that absent section 212 investigators would have been able to locate and apprehend Bjarnason in time.

Should section 212 expire, communications providers would be able to disclose the content of customers' communica-

tions in emergency situations but would not be able voluntarily to disclose non-content customer records pertaining to those communications. Such an outcome would defy common sense. Allowing section 212 to expire, moreover, would dramatically restrict communications providers' ability voluntarily to disclose life-saving information to the government in emergency situations.

Section 202, for its part, modernized the criminal code in light of the increased importance of telecommunications and digital communications. The provision allows law enforcement to use pre-existing wiretap authorities to intercept voice communications, such as telephone conversations, in the interception of felony offenses under the Computer Fraud and Abuse Act. These include many important cybercrime and cyberterrorism offenses, such as computer espionage and intentionally damaging a federal government computer. Significantly, section 202 preserved all of the pre-existing standards in the wiretap statute, meaning that law enforcement must file an application with a court, and a court must find that: (1) there is probable cause to believe an individual is committing, has committed, or is about to commit a particular predicate offense; (2) there is probable cause to believe that particular communications concerning that offense will be obtained through the wiretap; and (3) "normal investigative procedures" have been tried and failed or reasonably appear to be unlikely to succeed or are too dangerous. If wiretaps are an appropriate investigative tool to be utilized in cases involving bribery, gambling, and obscenity, as was the case prior to the passage of the Patriot Act, then surely investigators should be able to use them when investigating computer espionage, extortion, and other serious cybercrime and cyberterrorism offenses.

Turning to section 220, that provision allows courts, in investigations over which they have jurisdiction, to issue search warrants for electronic evidence stored outside of the district where they are located. Federal law requires investigators to use a search warrant to compel an Internet service provider to disclose unopened e-mail messages that are less than six months old. Prior to the Patriot Act, some courts interpreting Rule 41 of the Federal Rules of Criminal Procedure declined to issue search warrants for e-mail messages stored on servers in other districts, leading to delays in many time-sensitive investigations as investigators had to bring agents, prosecutors, and judges in another district up to speed. Requiring investigators to obtain warrants in distant jurisdictions also placed enormous administrative burdens on districts in which major Internet service providers are located, such as the Northern District of California and the Eastern District of Virginia.

Section 220 fixed this problem. It makes clear, for example, that a judge with jurisdiction over a murder investigation in Pennsylvania can issue a search warrant for e-mail messages pertaining to that investigation that were stored on a server in Silicon Valley [in California]....The department has already utilized section 220 in important terrorism investigations. [For example], section 220 was useful in the...infamous "shoebomber" terrorist Richard Reid [who tried to blow up a transatlantic flight in 2001].

Contrary to concerns voiced by some, section 220 does not promote forum-shopping; the provision may be used only in a court with jurisdiction over the investigation. Investigators may not ask any court in the country to issue a warrant to obtain electronic evidence.

It is imperative that section 220 be renewed; allowing the provision to expire

would delay many time-sensitive investigations and result in the inefficient use of investigators', prosecutors', and judges' time.

Moving to section 209, that provision made existing statutes technology-neutral by providing that voicemail messages stored with a third-party provider should be treated like e-mail messages and answering machine messages, which may be obtained through a search warrant. Previously, such messages fell under the rubric of the more restrictive provisions of the criminal wiretap statute, which apply to the interception of live conversations. Given that stored voice communications possess few of the sensitivities associated with the real-time interception of telephone communications, it was unreasonable to subject attempts to retrieve voice-mail message stored with third-party providers to the same burdensome process as requests for wiretaps. Section 209 simply allows investigators, upon a showing of probable cause, to apply for and receive a court-ordered search warrant to obtain voicemails held by a third-party provider, preserving all of the pre-existing standards for the availability of search warrants. Since the passage of the Patriot Act, such search warrants have been used in a variety of criminal cases to obtain key evidence, including voicemail messages left for foreign and domestic terrorists, and to investigate a large-scale Ecstasy smuggling ring based in the Netherlands.

The speed with which voicemail is seized and searched can often be critical to an investigation given that deleted messages are lost forever. Allowing section 209 to expire, as it is set to do in 2005, would once again require different treatment for stored voicemail messages than for messages stored on an answering machine in a person's home, needlessly hampering law

enforcement efforts to investigate crimes and obtain evidence in a timely manner.

Section 217 similarly makes criminal law technology-neutral, placing cyber-trespassers on the same footing as physical intruders by allowing victims of computer-hacking crimes voluntarily to request law enforcement assistance in monitoring trespassers on their computers. Just as burglary victims have long been able to invite officers into their homes to catch the thieves, hacking victims can now invite law enforcement assistance to assist them in combating cyber-intruders. Section 217 does not require computer operators to involve law enforcement if they detect trespassers on their systems; it simply gives them the option to do so. In so doing, section 217 also preserves the privacy of law-abiding computer users by sharply limiting the circumstances under which section 217 is available. Officers may not agree to help a computer owner unless (1) they are engaged in a lawful investigation; (2) there is reason to believe that the communications will be relevant to that investigation; and (3) their activities will not acquire the communications of non-trespassers. Moreover, the provision amended the wiretap statute to protect the privacy of an Internet service provider's customers by providing a definition of "computer trespasser" which excludes an individual who has a contractual relationship with the service provider. Therefore, for example, section 217 would not allow Earthlink to ask law enforcement to help monitor a hacking attack on its system that was initiated by one of its own subscribers.

Since its enactment, section 217 has played a key role in sensitive national security matters, including investigations into hackers' attempts to compromise military computer systems. Section 217 is also particularly helpful when computer hackers launch massive "denial of service"

attacks—which are designed to shut down individual web sites, computer networks, or even the entire Internet. Allowing section 217 to expire, which is set to occur in 2005, would lead to a bizarre world in which a computer hacker's supposed privacy right would trump the legitimate privacy rights of a hacker's victims, making it more difficult to combat hacking and cyberterrorism effectively.

PROTECTING CIVIL LIBERTIES

While the Patriot Act provided investigators and prosecutors with tools critical for protecting the American people, it is vital to note that it did so in a manner fully consistent with constitutional rights of the American people. In section 102 of the Patriot Act, Congress expressed its sense that "the civil rights and civil liberties of all Americans...must be protected," and the Patriot Act does just that.

In the first place, the Patriot Act contains several provisions specifically designed to provide additional protection to the civil rights and civil liberties of all Americans. Section 223, for example, allows individuals aggrieved by any willful violation of the criminal wiretap [restrictions to sue in federal court for] not less than \$10,000 in damages. This provision allows an individual whose privacy is violated to sue the United States for money damages if federal officers or employees disclose sensitive information without lawful authorization.

Section 223 also requires federal departments and agencies to initiate a proceeding to determine whether disciplinary action is warranted against an officer or employee whenever a court or agency finds that the circumstances surrounding a violation of Title III raise serious questions about whether that officer or employee willfully or intentionally violated Title III. To date, there have been no administrative

disciplinary proceedings or civil actions initiated under section 223 of the Patriot Act. I believe that this reflects the fact that employees of the Justice Department consistently strive to comply with their legal obligations. Nevertheless, section 223 provides an important mechanism for holding the Department of Justice accountable, and I strongly urge Congress not to allow it to sunset at the end of 2005.

Additionally, section 1001 of the Patriot Act requires the Justice Department's Inspector General to designate one official responsible for the review of complaints alleging abuses of civil rights and civil liberties by Justice Department employees. This individual is then responsible for conducting a public awareness campaign through the Internet, radio, television, and newspaper advertisements to ensure that individuals know how to file complaints with the Office of the Inspector General.

Section 1001 also directs the Office of Inspector General to submit to this Committee and the House Judiciary Committee on a semi-annual basis a report detailing any abuses of civil rights and civil liberties by department employees or officials. To date, six such reports have been submitted by the Office of the Inspector General. I am pleased to be able to state that the Office of the Inspector General has not documented in these reports any abuse of civil rights or civil liberties by the department related to the use of any substantive provision of the Patriot Act.

In addition to containing special provisions designed to ensure that the civil

rights and civil liberties of the American people are respected, the Patriot Act also respects the vital role of the judiciary by providing for ample judicial oversight to guarantee that the constitutional rights of all Americans are safeguarded [as described above]....I would note that the department has gone to great lengths to respond to congressional concerns about the implementation of the Patriot Act. The department has, for example, provided answers to more than 520 oversight questions from members of Congress regarding the Patriot Act. In the 108th Congress alone, in fact, the department sent 100 letters to Congress that specifically addressed the Patriot Act. The department also has provided witnesses at over 50 terrorism-related hearings, and its employees have conducted numerous formal and informal briefings with Members and staff on Patriot Act provisions.

CONCLUSION

In closing, the issues that we are discussing today are absolutely critical to our nation's future success in the war against terrorism. The Patriot Act has a proven record of success when it comes to protecting the safety and security of the American people, and we cannot afford to allow many of the Act's most important provisions to expire at the end of the year. For while we certainly wish that the terrorist threat would disappear on December 31, 2005, we all know that this will not be the case.

THE CONTINUING DEBATE: Anti-Terrorist Legislation

What Is New

In 2003, the Bush administration proposed the Domestic Security Enhancement Act of 2003 (dubbed Patriot Act II), which further expands the surveillance possibilities of Patriot Act I. The legislation did not pass in Congress, but critics charge that many of its provisions were slipped into other legislation, such as the Intelligence Authorization Act for 2004. The debate over the Patriot Act was renewed during the effort to renew it in 2005, as required by the initial act. The primary bill to do that, H.R. 3199 was passed by the House and passed as amended by the Senate. At this writing, the work to resolve the differences in the House and Senate versions is in a conference committee. Challenges to the Patriot Act have not yet made their way to the Supreme Court, but one, *Doe v. Gonzales*, relating to the ability of investigators to get library borrowing records, is in the U.S. Court of Appeals and is considered by many observers a good bet to soon be on the Supreme Court's docket.

The public is split on its view of the Patriot Act and civil liberties. A 2005 survey found that 30% of its respondents thought the act goes "too far" to restrict rights, 41% thought the restrictions are "about right," 21% thought the provisions "do not go far enough," and 8% were unsure.

Where to Find More

There are numerous Web sites lauding and decrying the Patriot Act. The fate of H.R. 3199 can be found on the now familiar Thomas site at <http://thomas.loc.gov/>. For a supportive view, go to the U.S. Department of Justice Web site at: <http://www.usdoj.gov/>. Select search and keyboard in "patriot act." For a critical perspective, visit the site of the American Civil Liberties Union at: <http://www.aclu.org/SafeandFree/>. Finally, for a balanced analysis of the Patriot Act, including an exposition of the surveillance possibilities prior to it, read Nathan C. Henderson, "Impact on the Government's Ability to Conduct Electronic Surveillance of Ongoing Domestic Communications," *Duke Law Journal*, October 2002. The article is available on the Web at: <http://www.law.duke.edu/journals/>.

What More to Do

One key thing to do is to get involved. Find out what has happened to H.R. 3199 in the 109th Congress. If it remains pending before Congress, decide what you think, and act on that conviction by telling your three representatives in Congress what your position is and why. If it has passed or been defeated, find out how your members of Congress voted.

Finally, do not just be "for" or "against" things. How would you simultaneously give the government the tools it needs to guard against terrorists and preserve the civil liberties the citizenry needs to guard against the government? Perhaps you and others in your class could write an act to Protect Americans' Traditional Rights while Investigating and Obstructing Terrorism, Patriot III.