Department of Justice

STATEMENT

OF

ALBERTO R. GONZALES
ATTORNEY GENERAL

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

CONCERNING

THE USA PATRIOT ACT

PRESENTED ON

APRIL 5, 2005

STATEMENT OF ALBERTO R. GONZALES
ATTORNEY GENERAL OF THE UNITED STATES
BEFORE THE UNITED STATES SENATE
COMMITTEE ON THE JUDICIARY
APRIL 5, 2005

Chairman Specter, Ranking Member Leahy, and Members of the Committee:

It is my pleasure to appear before you this morning 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 USA PATRIOT Act, which passed both Houses of the Congress with overwhelming bipartisan majorities and was signed into law by President Bush on October 26, 2001. In the past three-and-a-half years, the USA 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 USA 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 USA 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 USA 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.

As Congress considers whether to renew key USA PATRIOT Act provisions, I also wish to stress that I am open to any ideas that may be offered for improving these

provisions. If members of this Committee or other members of Congress wish to offer proposals in this regard, I and others at the Department of Justice would be happy to consult with you and review your ideas. However, let me be clear about one thing: I will not support any proposal that would undermine the ability of investigators and prosecutors to disrupt terrorist plots and combat terrorism effectively.

It is also my sincere hope that we will be able to consider these crucial issues in a calm and thoughtful fashion. All of us seek to ensure the safety and security of the American people and to protect their civil liberties as well. As this debate goes forward, I will treat those who express concerns about the USA PATRIOT Act with respect and listen to their concerns with an open mind. I also hope that all who participate in the debate will stick to the facts and avoid overheated rhetoric that inevitably tends to obfuscate rather than elucidate the truth.

Today, I would like to use the rest of my testimony to explain how key provisions of the USA PATRIOT Act have helped to protect 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 USA PATRIOT Act has enhanced the federal government's ability to share intelligence. Then, I will explain how the USA 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 USA 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 USA 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 important for this Committee 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 USA PATRIOT Act, the Foreign Intelligence Surveillance Act (FISA) 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 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 overcome 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 Usama 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 Usama Bin Laden and al Qaeda. We could not learn what information they had gathered. That was "the wall."

Thanks in large part to the USA 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 USA 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 USA 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 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 USA 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: several persons involved in al Qaeda drugs-for-weapons plot in San Diego, two of whom have pleaded guilty; nine associates in Northern Virginia of a violent extremist group known as Lashkar-e-Taiba that has ties to al Qaeda, who were convicted and sentenced to prison terms ranging from four years to life imprisonment; two Yemeni citizens, Mohammed Ali Hasan Al-Moayad and Mohshen Yahya Zayed, who were charged and convicted for conspiring to provide material support to al Qaeda and HAMAS; Khaled Abdel Latif Dumeisi, who was convicted by a jury in January 2004 of illegally acting as an agent of the former government of Iraq as well as two counts of perjury; and Enaam Arnaout, the Executive Director of the Illinois-based Benevolence International Foundation, who had a long-standing relationship with Osama Bin Laden and pleaded guilty to a racketeering charge, admitting that he diverted thousands of dollars from his charity organization to support Islamic militant groups in Bosnia and Chechnya. Information sharing between intelligence and law enforcement personnel has also been extremely valuable in a number of other ongoing or otherwise sensitive investigations that I am not at liberty to discuss today.

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 USA PATRIOT Act, often prevented 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 USA 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 USA 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 USA 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."

Since the passage of the USA PATRIOT Act, Congress has taken in the Homeland Security Act of 2002 and the Intelligence Reform and Terrorism Prevention Act of 2004 other important steps forward to improve coordination and information sharing throughout the Federal Government. If Congress does not act by the end of the year, however, 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 USA 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 USA 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 USA 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. Specifically, these orders have authorized the interception of certain communications to investigate the predicate offenses listed in the federal wiretap statute, 18 U.S.C. § 2516(1). The listed offenses include numerous crimes, such as drug crimes, mail fraud, passport fraud, embezzlement from pension and welfare funds, the transmission of wagering information, and obscenity offenses.

Prior to the passage of the USA PATRIOT Act, however, certain extremely serious crimes that terrorists are likely to commit were not included in this list, 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 USA 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.

Congress eliminated this problem with respect to traditional criminal crimes, such as drug offenses and racketeering, in 1986 when it authorized the use of multi-point or "roving" wiretaps in criminal investigations. But from 1986 until the passage of the USA PATRIOT Act in 2001, such authority was not available under FISA for cases involving terrorists and spies. Multi-point wiretaps could be used to conduct surveillance of drug dealers but not international terrorists. However, such authority was needed under FISA. International terrorists and foreign intelligence officers are trained to thwart surveillance by changing the communications facilities they use, thus making vital the ability to obtain "roving" surveillance. Without such surveillance, investigators were often left two steps behind sophisticated terrorists.

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 – 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 USA 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 USA 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 USA 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 USA 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 USA 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 carriers, 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 USA 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 activities 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 many 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 USA 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 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 USA 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 USA 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.

Section 212 of the USA PATRIOT Act governed both the voluntary disclosure of the content of communications and the voluntary disclosure of non-content customer records in emergency situations; but in 2002, the Homeland Security Act repealed that portion of section 212 governing the disclosure of the content of communications in emergency situations and placed similar authority in a separate statutory provision that is not scheduled to sunset. The remaining portion of section 212, governing the disclosure of customer records, however, is set to expire at the end of 2005. Should section 212 expire, communications providers would be able to disclose the content of customers' communications 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 USA 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 USA 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. Thus, investigators in Pennsylvania, under this scenario, can ask a judge familiar with the investigation to issue the warrant rather than having to ask Assistant United States Attorneys in California, who are unfamiliar with the case, to ask a judge in the United States District Court for the Northern District of California, who is also unfamiliar with the case, to issue the warrant.

The Department has already utilized section 220 in important terrorism investigations. As Assistant Attorney General Christopher Wray testified before this committee on October 21, 2003, section 220 was useful in the Portland terror cell case

because "the judge who was most familiar with the case was able to issue the search warrants for the defendants' e-mail accounts from providers in other districts, which dramatically sped up the investigation and reduced all sorts of unnecessary burdens on other prosecutors, agents and courts." This section has been similarly useful in the "Virginia Jihad" case involving a Northern Virginia terror cell and in the case of the infamous "shoebomber" terrorist Richard Reid. Moreover, the ability to obtain search warrants in the jurisdiction of the investigation has proven critical to the success of complex, multi-jurisdictional child pornography cases.

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 USA 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 USA 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 USA PATRIOT Act, Congress expressed its sense that "the civil rights and civil liberties of all Americans . . . must be protected," and the USA PATRIOT Act does just that.

In the first place, the USA 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 statute (Title III), the Electronic Communications Privacy Act, or certain provisions the FISA, to file an action in United States District Court to recover 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 USA 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 USA 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 pursuant to section 1001; they were transmitted in July 2002, January 2003, July 2003, January 2004, September 2004, and March 2005. 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 USA 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 USA 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 and that the important role of checks and balances within our Federal Government is preserved. As reviewed above, under section 214 of the Act, investigators cannot utilize a pen register or trap-and-trace device unless they apply for and receive permission from the FISA Court. Section 215 of the Act requires investigators to obtain a court order to request the production of business records in national security investigations. Section 206 requires the Foreign Intelligence Surveillance Court to approve the use of "roving" surveillance in national security investigations. Sections 201 and 202 require a Federal court to approve the use of a criminal investigative wiretap, and sections 209 and 220 require a Federal court to issue search warrants to obtain evidence in a criminal investigation.

Besides safeguarding the vital role of the judiciary, the USA PATRIOT Act also recognizes the crucial importance of congressional oversight. On a semiannual basis, for example, as noted before, I am required to report to this Committee and the House Judiciary Committee the number of applications made for orders requiring the production of business records under section 215 as well as the number of such orders granted, modified or denied. I am also required to fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate on a semiannual basis concerning all requests for the production of business records under section 215. These reports were transmitted by the Department to the appropriate committees in April 2002, January 2003, September 2003, December 2003, September 2004, and December 2004. Moreover, I am required by statute to submit a comprehensive report on a semiannual basis to the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate regarding the Department's use of FISA. These reports contain valuable information concerning the Department's use of USA PATRIOT Act provisions, including sections 207, 214, and 218.

Finally, I would note that the Department has gone to great lengths to respond to congressional concerns about the implementation of the USA PATRIOT Act. The Department has, for example, provided answers to more than 520 oversight questions from Members of Congress regarding the USA PATRIOT Act. In the 108th Congress alone, in fact, the Department sent 100 letters to Congress that specifically addressed the USA 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 USA PATRIOT Act provisions. In short, the Department has been responsive and will continue to be responsive as Congress considers whether key sections of the USA PATRIOT Act will be made permanent.

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 USA 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. I look forward to working with the Members of this Committee closely in the weeks and months ahead, listening to your concerns, and joining together again on a bipartisan basis to ensure that those in the field have the tools that they need to effectively prosecute the war against terrorism. I also look forward to answering your questions today.