Testimony of

Mr. Robert Cleary

November 18, 2003

STATEMENT OF
ROBERT J. CLEARY
PARTNER, PROSKAUER ROSE LLP
FORMER UNITED STATES ATTORNEY
FOR THE DISTRICT OF NEW JERSEY
AND THE SOUTHERN DISTRICT OF ILLINOIS

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

PRESENTED ON

NOVEMBER 18, 2003

Mr. Chairman and Members of the Committee: It is an honor to appear before you today. I appreciate this opportunity to speak before the Committee about my experience as a prosecutor as it relates to the tools provided under the USA Patriot Act and their indispensable role in the investigation and prosecution of terrorists.

I am an attorney currently engaged in the private practice of law as a member of the law firm of Proskauer Rose LLP. From 1999 to 2002, I was privileged to serve first as the United States Attorney for the District of New Jersey and later as the United States Attorney for the Southern District of Illinois. Prior to being appointed as United States Attorney, I was the lead prosecutor in the Unabomb case, United States v. Theodore J. Kaczynski. In total, I spent 18 years as a federal prosecutor.

The September 11, 2001, terrorist attacks on our country occurred during my tenure as United States Attorney in New Jersey. In that capacity, I supervised a massive deployment of investigative and prosecutorial resources to the global terrorism investigation that followed. I believe my experience in supervising the New Jersey "9/11 investigation" and in leading the Unabomb prosecution team gives me unique insight into the benefits the USA Patriot Act provides prosecutors and agents in the field in domestic and international terrorism cases.

In the days and weeks following the unspeakable tragedy of September 11, the New Jersey investigative team was consumed with a fear that another horrific attack had been planned and that its execution was imminent. Our investigative team - which consisted of over 500 investigators and prosecutors - literally worked around the clock, seven days a week, at a frenetic pace in an effort to detect and dismantle any terrorist plot before more blood was spilled. Tensions were heightened by several reports from the intelligence community and from law enforcement sources that, in fact, another devastating attack might be on the horizon. As a result, the investigative team felt constant pressure to move at breakneck speed.

This concern underscores a bedrock principle of terrorism investigations: the need to move quickly and efficiently. This necessity is borne, as suggested above, by the fear of another terrorist attack. The necessity of speed and efficiency is further bolstered by the realization that the investigative trail to terrorists and their confederates quickly grows very cold. In order to increase the odds of bringing terrorists to justice, investigators and prosecutors must be able to operate with enhanced efficiency. In the Patriot Act, Congress has given them the tools to do so.

I would like to focus my remarks this morning on how the Patriot Act enables terrorism investigators and prosecutors to move more nimbly and expeditiously. The Act has accomplished this by eliminating needless administrative burdens and mechanical impediments (see Section III, below). Earlier in these

hearings, my former colleagues from the Department of Justice pointed out that in waging its war on terrorism, the Government needs strong laws and laws that are modernized to fit the state of technological advancement. The Patriot Act provides those tools as well. I would like to spend a few moments reviewing some of those statutory provisions before addressing the ways in which the Patriot Act has increased the efficiency of terrorism investigations.

I. Stronger Laws Combating Terrorism And Terrorist Support Networks

As the Committee is well aware, the Patriot Act has been vital to strengthening criminal laws in the fight against terrorism. For example, the Act increased the maximum prison sentences for terrorism offenses. The leverage of stronger penalties provides greater incentive to cooperate against confederates. The Act also has eliminated the statute of limitations for certain terrorism crimes. Terrorists, like murderers, should never be free from prosecution, no matter how long it takes to track them down. Additionally, federal jurisdiction now extends to American facilities abroad, including our diplomatic and consular facilities and the related private residences overseas, with respect to crimes committed by or against United States nationals. With the broader jurisdictional reach, we can now prosecute these crimes in the United States, instead of relying on foreign courts. In these days, when our diplomatic and consular facilities and personnel are subject to an increased threat of attack, this is an especially useful law.

Government intelligence suggests that for every person who commits a terrorist act, there are as many as 35 individuals who provide support to that terrorist. In order to maintain an infrastructure for his criminal enterprise, the terrorist must rely on a wide array of assistance -- housing, technical support (such as expert advice and false documentation), and financial support. The Patriot Act targets this support network. Federal prosecutors can now criminally charge those who house, harbor, or conceal terrorists or those who are about to commit terrorist acts. They can also prosecute those who provide technical expertise to terrorists. The Act strengthened the law against providing material support to terrorists by broadening the definition of "material support" to include expert advice and assistance. For example, if a civil engineer advises terrorists on how to destroy a building, that now constitutes material support. The material support statute has also been amended so that support provided outside the United States is now proscribed as well.

Further, the Act increased the Government's ability to target terrorists' financial support. Thus, the Act authorizes the forfeiture of assets of terrorists and terrorist organizations. The Government can confiscate terrorists' assets, regardless of the source of the property, and regardless of whether the property has been used to commit a terrorist act or whether the assets were proceeds of terrorist acts. The Government can also forfeit all assets that have been used or, more importantly, are intended to be used to facilitate a terrorist act. This critical provision enables the Government to disrupt a terrorist plot before it occurs by seizing the resources that are intended to support that criminal activity.

Finally, counterterrorism efforts are now afforded the full arsenal of powers that are used to combat other crimes. The most important illustration of this is that the Patriot Act added terrorism offenses to the list of the only crimes for which the Government may seek wiretap authorization. This enactment eliminates a glaring -- and inexplicable -- omission in the law. As another example, terrorism offenses are now included as RICO predicates. This amendment allows the Government to utilize the powers under the RICO statutes, which were traditionally used to combat organized crime, in the war against terrorism as well.

II. Modernization of the Law

Prior to the Patriot Act, our laws providing investigative tools to law enforcement did not keep pace with the development of new technologies. This problem led to a number of anomalous results, several of which are discussed below. The Patriot Act modernized our laws, allowing for Government investigative techniques to apply equally to new technologies - to obtain the same information in the digital age that they could in earlier times, under the same standards that traditionally have been in place.

Cable Companies: Before the passage of the Act, special rules applied to attempts to gather information from cable companies, including notifying the subject of the Government inquiry and providing that person an opportunity to contest it in court. As a result, such investigative steps were rarely conducted. Before the internet era, this was not problematic for law enforcement because cable companies had provided only cable television programming. When cable companies began providing digital services, including the internet, law enforcement sought to obtain the same types of information, under the same process, which they obtained from internet companies. The cable companies, however, took the position that the old rules still governed. As a result, if the target of the investigation had internet service through an Internet Service Provider ("ISP"), such as AOL, the Government could obtain certain information using the normal processes -- subpoenas, court orders, and search warrants. As an example, law enforcement could obtain the contents of a target's e-mail account with a court-authorized search warrant if the target used an ISP

such as AOL. If, on the other hand, the target had internet service through a cable company, as many people do today, the Government could not access the same information. This illogical dichotomy frustrated law enforcement efforts to investigate criminals who fortuitously, or perhaps even intentionally, chose cable internet service.

The Patriot Act changed this by rationalizing the process. For traditional cable services, such as pay-per-view and television programming, the old rules protecting viewer privacy still apply. For other services, however, such as the internet, the general rules that apply to all other ISPs apply to the cable internet services as well. Here, the Patriot Act simply moved the law into step with the changing technologies - cable internet service - nothing more.

Internet Pen Registers and Trap and Traces: As another example, pen registers and trap and traces on telephone lines are well-recognized, time-honored, critical investigative tools of law enforcement. A traditional pen register records in real time all telephone numbers dialed from a telephone. The content of the calls are not disclosed. A trap and trace records all the telephone numbers making calls into the target telephone line. As with the pen register, the content of the calls are not disclosed. Law enforcement can then obtain subscriber information, such as the name and address, on the incoming and outgoing telephone numbers. In establishing a conspiracy, it is imperative to prove who is talking to whom and when. Together with surveillance and other investigative techniques, pen registers and trap and traces (collectively, "pens") are often critical tools to prove those crucial facts. Pens are also essential in developing evidence for other investigative devices, such as wire taps. Providing pen analysis -- an analysis of the telephone call logs -- is all but mandatory in affidavits for authorization to obtain a wire tap.

Pens require a court order. To obtain subscriber information, the Government must establish reasonable cause to believe, based on specific and articulable facts, that the subject of the investigation had violated or was violating federal law, and was using the target phone line to further criminal activity. Prior to the Patriot Act, the controlling statutes -- which were enacted in 1986 -- did not explicitly provide for pens on e-mail traffic or other internet activity inasmuch as they were unknown communication vehicles at that time. As a result of section 216 of the Act, law enforcement now has the statutory authority to install pens on the internet. Law enforcement, with the still-required court order, under the same standards, can obtain in-box and out-box information from an e-mail account, along with the subscriber information on those e-mail accounts. The Government cannot get the subject line of the e-mail, or any other content of the e-mail with a pen, but may only obtain the equivalent information that can be obtained from a pen on a telephone line. Thus, this is no more intrusive than the traditional law enforcement devices on the telephone lines -- law enforcement is simply able to obtain the equivalent, critical information from this modern method of communication.

Voice Mail and Other Stored Voice Communications: Under the prior laws, law enforcement could not use search warrants to obtain voice and wire communications stored by electronic communication service providers, for example, voice mail messages stored and maintained by AT&T or Verizon for a subscriber. Rather, to acquire that evidence, the prosecutor had to undertake the much more difficult, labor intensive, and time-consuming process of obtaining a wiretap order from the court. This led to some anomalous results. If the target of an investigation had a traditional answering machine at home, law enforcement could obtain a copy of his or her taped messages with a search warrant. If, on the other hand, the target had a private voice mail service with a telephone company, the Government needed a wiretap to listen to the same recorded voice messages. Similarly, if law enforcement had a search warrant to obtain the contents of a target's e-mail account, it could read the e-mails and the attachments to the e-mails, such as pictures, documents, and other written communications that were attached to the e-mails. However, if there was a voice recording attached to the e-mail, the Government arguably was prohibited from listening to that voice message in the absence of a court-ordered wiretap.

Section 209 of the Act eliminated the different treatment with respect to the storage of wire communications versus the storage of other electronic communications. Now, voice mail services are treated no differently than answering machines. The Government's ability to listen to voice mail messages should not depend on whether the target uses an answering machine or a voice mail service. The privacy concerns relating to messages on answering machines are the same as those relating to messages on voice mail services. Similarly, the content of voice mail attachments are appropriately treated as equivalent to other content-based e-mail attachments.

III. Speed and Efficiency

The Patriot Act has reduced purely administrative and mechanical burdens on investigators and prosecutors. This, in turn, has increased the efficiency of law enforcement without circumventing or

undermining the protections and safeguards of civil liberties.

Single-Jurisdiction Pen Registers: Prior to the passage of the Patriot Act, if a federal prosecutor in New Jersey needed a pen register on a cellular phone with a New York area code, the prosecutor would be required to obtain a court order from New York. This entailed contacting a federal prosecutor in New York and having that prosecutor submit the application to a Magistrate Judge in New York. In some instances, the requesting prosecutors must meet certain peculiar stylistic or other non-substantive requirements of the district in which the application is made. Consequently, it is a much more time consuming and burdensome process. In New Jersey, where many areas serve as suburbs to New York City or Philadelphia, countless investigations involve phone numbers that cross state lines. Cumulatively, substantial resources were wasted as a result. I would guess that the federal prosecutors in Washington, DC, Virginia, and Maryland have had similar experiences.

Now, under section 216 of the Patriot Act, if New Jersey has jurisdiction over the crime under investigation, the New Jersey prosecutor could obtain a pen register on any telephone in the country with an order signed by a Magistrate Judge in the District of New Jersey. This process only eliminates the red tape, but not the substance - it requires the same court order, under the same legal standards, but fewer administrative hurdles. Consequently, the investigation is conducted with greater speed and efficiency, without sacrificing privacy protections.

Single Order for Multiple Service Providers: Prior to the Patriot Act, law enforcement could track someone's internet activity with a court's permission. Once the Government identified the target's internet account, it could obtain an order that required the ISP, such as AOL, to disclose the internet sites visited by the person using his or her internet account. This investigative tool can provide important evidence, for example, if two co-conspirators are using a particular chat room to communicate, or if the target has visited a website that explains how to make a pipe bomb. Under the old rules, an order was only valid for a single ISP. In other words, if the target had an internet account with AOL, the Government obtained an order requiring AOL to provide the requested information. The problem arose if the target used AOL to enter one internet site ("site A"), and then used a link to jump to a second site ("site B") -- AOL could only disclose that the target visited site A. Only site A's ISP could reveal that the target jumped to site B from site A. Because the court order was only valid for AOL, the Government would need another order for site A's ISP. If the target continuously jumped from site to site, investigators would need an order for every ISP the target used. When you multiplied this by potentially hundreds of sites and ISPs, tracking down this information became prohibitive.

The Patriot Act changed this by giving federal courts the authority to issue one order on an internet account that is binding across the country. Under section 216, the order compels assistance from any ISP through which the target internet account travels. The Government can take the single court order and serve it on the ISP for each site visited by the target. Through the connection information provided by each site, the Government is able to follow the target from site to site without having to prepare multiple applications and obtain separate court authorizations for each ISP.

Under this new provision, the same evidentiary standards are in place. The only difference is one of process efficiency. Instead of potentially having to write hundreds of substantively duplicative orders for each and every ISP, regurgitating the same information in multiple orders, and repeatedly obtaining an audience with the Court to sign such orders, the Government can now prepare a single order that binds all ISPs.

Nationwide Search Warrants for E-Mail: Prior to the Patriot Act, federal prosecutors who wanted to obtain the equivalent of a search warrant for an e-mail account to access the contents of a target's e-mails frequently encountered substantial administrative impediments. They were required to go to the district where the search and seizure would take place -- where the information was physically stored by the ISP -- to get a judge in that district to sign the search warrant. In the days following September 11, this requirement imposed an enormous bureaucratic burden and caused a significant bottleneck to the progress of the terrorism investigation. During the course of the 9/11 investigation, on many occasions, we needed a search warrant to examine the contents of an e-mail account. These search warrants had to be signed and executed in the districts where the ISPs, such as AOL, were located. Two of the three largest ISPs that we dealt with were in the Northern District of California. As a result, e-mail search warrants from all over the country, involving virtually every aspect of the global terrorism investigation, were filed in that judicial district. In short order, that court was overrun by applications for search warrants and other court orders involving these ISPs. In an effort to manage this staggering workload, the court implemented certain procedures. These procedures, in turn, imposed additional burdens on the out-of-district prosecutors. As a result, however -- and through no fault of the court in the Northern District of California -- the processing

of one of these applications, which would have taken mere hours in New Jersey, in fact, took an entire day or more, and required the efforts of several extra hands. In terrorism cases, when time is of the essence -- possible confederates may be fleeing the country, shedding aliases, obtaining new false documents, or otherwise disappearing, or worse yet, a terrorist plot may not be thwarted - such an unnecessary delay is simply unacceptable.

Section 220 of the Act changed that by providing nationwide search warrants for e-mail accounts. Now, when a New Jersey investigation needs the contents of an e-mail account, a federal prosecutor in New Jersey can file the application for a search warrant with a Magistrate Judge in New Jersey. The search of the e-mail account can then be conducted in the Northern District of California. This change merely reduces administrative hassles. The same constitutional standards still apply -- a federal Magistrate Judge must still find that there exists probable cause to believe that criminal activity is occurring, and probable cause to believe that evidence, fruits, or instrumentalities of the specified federal offenses will be found in the location to be searched.

Single-Jurisdiction Search Warrants for Terrorism Cases: Another change regarding search warrants is found in Section 219 of the Act, which provides for single-jurisdiction search warrants for terrorism cases. Whether an e-mail account, a storage facility just across the state lines, or any other property had to be searched, under the old rules, prosecutors had to present the search warrant application to a Magistrate Judge in the district in which the search was to be conducted. Similar to the problems with e-mail searches, this requirement frequently necessitated substantial coordination among different prosecutors' offices and the court, resulting in bureaucratic burdens and invariable delays.

Now, as a result of section 219, a search warrant in a terrorism case can be obtained in the investigating district to search property in another district, as long as events related to the terrorism activities have occurred in the investigating district. Again, no safeguards are sacrificed or diminished under this section. A United States Magistrate Judge still must make the same probable cause finding. Particularly in terrorism investigations, where delay could be catastrophic, reducing the red tape without reducing the protections to civil liberties is an obvious benefit.

Easing the Restrictions to Information Sharing: Prior to passage of the Act, the law required that the "primary purpose" of the use of the investigative tools authorized under the Foreign Intelligence Surveillance Act ("FISA") was for foreign intelligence. This standard constrained the intelligence community's ability to share information with law enforcement.

Not surprisingly, in certain instances, the use of FISA (e.g., a wiretap authorized by the FISA Court) developed evidence of criminal conduct by the targets of such surveillance. The problem arose if the agents working on the intelligence investigation wanted to turn FISA-derived information over to criminal investigative agents and prosecutors. In particular, the Government was concerned that if a parallel criminal investigation resulted and began to progress, based on that fact, the FISA Court might determine that the primary purpose of the FISA wire was no longer foreign intelligence. In such a case, the FISA Court could then shut down the FISA wire, thereby compromising an on-going intelligence investigation. Due to these concerns, the "primary purpose" standard had the effect of preventing the dissemination of FISA-derived evidence for use in criminal investigations.

Section 218 of the Act changed the standard for using FISA to gather intelligence. Now, as long as a significant purpose is foreign intelligence, FISA may be used. This allows, in a greater number of situations, for FISA-derived information to be used in criminal cases. In fact, I know of at least one instance in which the Government was able to prosecute a fundraiser for terrorist organization as a result of information gathered from a FISA wire -- a prosecution that probably would not have happened without the Patriot Act.

The Act included another important change that increased the flow of information between the criminal and intelligence communities. Federal Rules of Criminal Procedure 6(e), which regulates grand jury secrecy, was amended to allow the disclosure, to members of the intelligence community, of information developed through a grand jury investigation that relates to foreign intelligence. Whereas the change in the FISA requirements allowed criminal investigators to benefit from information developed during intelligence investigations, the change in the grand jury secrecy rules allowed the intelligence community to benefit from information obtained from grand jury investigations. Additionally, the change to Rule 6(e) also allows the CIA to participate on the Joint Terrorism Task Forces throughout the country. The potential benefits of these measures, which have helped to open up the avenues of communication between the intelligence and criminal investigators, cannot be overstated.

IV. Closing

I applaud the open and constructive debate over the details of the Patriot Act and the tools it provides in the war against terrorism. To be sure, as with any other substantial legislative package, reasonable people can and do disagree about some of the specifics of the Patriot Act. There is one thing, however, about which there can be no reasonable divergence of opinion: The American people deserve the protections afforded by the Patriot Act. As a citizen, I would like to express my appreciation to this Committee and to your colleagues in Congress for enacting this important piece of legislation.

This completes my prepared remarks. I would be pleased to attempt to answer any questions that you may have at this time.