KEN WAINSTEIN
UNITED STATES ATTORNEY
DISTRICT OF COLUMBIA
PREPARED REMARKS FOR THE
SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY
COMMITTEE ON THE JUDICIARY
UNITED STATES HOUSE OF REPRESENTATIVES
APRIL 28, 2005

I. Introduction

Mr. Chairman, Ranking Member Scott, and Members of the Subcommittee, thank you for the invitation to appear before you today to discuss two important provisions of the USA PATRIOT Act. Section 206 of the Act provides national security investigators with the ability to obtain roving surveillance orders from the Foreign Intelligence Surveillance Court ("FISA Court"), and section 215 authorizes the FISA Court to issue orders requiring the production of business records relevant to national security investigations. Criminal investigators have long enjoyed similar authorities for years, and I have seen firsthand how the ability to obtain roving wiretap orders and relevant business records have assisted law enforcement in combating serious crime.

Sections 206 and 215, however, are currently scheduled to sunset at the end of 2005. If this is allowed to happen, then we will once again be in a position where tools available to law enforcement in the fight against drugs, organized crime, and child pornography would not be at the disposal of national security investigators for use in the war against terrorism. Such an outcome would be a tragic mistake, and I am therefore here today to ask you to make permanent sections 206 and 215 of the USA PATRIOT Act.

II. Section 206

Section 206 of the USA PATRIOT Act allows the FISA Court to authorize "roving" surveillance of a foreign power or an agent of a foreign power, such as a terrorist or spy. A "roving" wiretap order attaches to a particular target rather than a particular phone or other communication facility. Since 1986, law enforcement has been able to utilize court-approved roving wiretaps in appropriate cases to investigate ordinary crimes, including drug offenses and racketeering. Investigators and prosecutors know from hard experience that a traditional wiretap order that applies to a single phone is often not effective because sophisticated criminals can change phones to thwart surveillance more quickly than investigators can go to court to obtain a new wiretap order.

Before the USA PATRIOT Act, however, while law enforcement investigators could utilize roving wiretaps in criminal investigations, national security investigators could not utilize such wiretaps in international terrorism or espionage investigations. To put it simply, this inconsistency in the law not only defied common sense, because well-trained terrorists and spies as a general matter are even more skilled at evading surveillance than the average criminal, it also significantly hampered our ability to effectively monitor terrorists and spies. We know that Al Qaeda members go to great lengths to foil our electronic surveillance efforts. A seized Al Qaeda training manual warns members that "communication . . . can be a knife dug into our back if we do not . . . take the necessary security measures." It then describes the means by which we conduct electronic surveillance and directs the Al Qaeda "brothers" to undertake a variety of measures to counter those efforts. Thankfully, however, section 206 remedied this

problem by authorizing the use of roving wiretap authority in national security investigations, thus putting investigators in a better position to keep up with international terrorists or spies, rather than falling one or two steps behind every time they change phones.

Because some, including Members of this Subcommittee, have expressed concerns about the use of roving wiretaps in national security investigations, I would like to discuss briefly the important privacy safeguards contained in section 206. To begin with, it is important to note that section 206 did not change the requirement that the target of roving surveillance must be identified or described in a surveillance order issued by the FISA Court. Therefore, a roving surveillance order is always connected to a particular target. To be clear, roving surveillance orders do not jump from target to target; rather, they follow a particular target as that target jumps from phone to phone. The FISA Court also must find that there is probable cause to believe the target of a roving surveillance order, just like any electronic surveillance order, is either a foreign power or an agent of a foreign power, such as a terrorist or a spy. To be sure, some have complained that FISA allows for the use of roving surveillance in cases where the government describes, rather than identifies, the target of surveillance. It is critical, however, to keep in mind that the government's description of the target must be sufficiently specific to convince the FISA Court that there is probable cause to believe that the target is a foreign power or agent of a foreign power.

Additionally, roving surveillance under section 206 can be authorized by the FISA Court only after it makes a finding that the actions of the target may have the effect of thwarting the identification of those, such as the telephone company, whose assistance

will be needed to carry out the surveillance. And finally, while there has been concern expressed that roving surveillance may intrude on the privacy of innocent Americans, section 206 in no way altered the requirement that FISA surveillance orders include court-approved minimization procedures to limit the acquisition, retention, and dissemination by the government of information or communications involving United States persons.

Whether in the criminal or national security realm, roving wiretaps recognize the technological realities of our modern age, in which a criminal or terrorist can change communications devices in the blink of an eye. Roving surveillance, however, also fits well within our longstanding and revered constitutional tradition of respecting civil liberties. For example, the United States Courts of Appeals for the Second, Fifth, and Ninth Circuits all have squarely ruled that "roving" wiretaps are perfectly consistent with the Fourth Amendment, and no court of appeals has reached a contrary conclusion.

III. Section 215

Section 215 provides national security investigators with the authority to ask the FISA Court to order the production of the same kinds of tangible things, such as business records, that prosecutors have long been able to acquire through grand-jury subpoenas in criminal investigations. As a prosecutor, I can tell you from firsthand experience that the ability to obtain records with grand-jury subpoenas is an essential tool for law enforcement. In criminal investigations, such subpoenas are routinely used to obtain all types of records. Asking law enforcement to effectively investigate and prosecute crime without using grand-jury subpoenas to obtain records would be like asking Tiger Woods to win the Masters without using a putter. The records obtained through grand jury

subpoenas often represent the critical building blocks of a successful criminal investigation and are used to determine whether the use of more intrusive investigative techniques, such as physical searches, are justified.

Before the USA PATRIOT Act, however, it was very difficult for national security investigators to request the production of business records in international terrorism and espionage investigations. For example, such investigators could only ask the FISA Court to order the production of records from "a common carrier, public accommodation facility, physical storage facility or vehicle rental facility." This patchwork of court order authority was confusing to investigators, who had to determine if the records they needed fit within one of these categories before deciding whether to seek a FISA Court order. Moreover, it left investigators without the ability to obtain a court order for records that could be vitally important to terrorism investigators. Under the prior law, for example, an investigator would not have been able to get a FISA court order to obtain records showing that a suspect purchased bulk quantities of fertilizer to produce a bomb because a feed store is not "a common carrier, public accommodation facility, physical storage facility or vehicle rental facility." Section 215 of the USA PATRIOT Act eliminated this restriction on the types of entities from whom records could be obtained. Now, investigators may ask the FISA Court to request the production of "any tangible things (including books, records, papers, documents, and other items)" from any type of entity. Section 215 therefore allows national security investigators to obtain the same types of records that grand juries have always been able to subpoena in the criminal context.

Because investigations into international spies and terrorists often can only be effective if the targets are unaware they are being investigated, court orders under this provision prohibit the recipient from telling others -- including the target -- about the order. This non-disclosure provision is akin to that which Congress has authorized for other types of process – such as subpoenas to financial institutions in criminal cases under the Right to Financial Privacy Act and under 18 U.S.C. 2703 relating to toll and subscriber records and stored wire and electronic communications. It only makes sense to apply a similar requirement in national security investigations, where the need for secrecy is greater and the stakes for the safety of our country is higher.

Given my experience as a prosecutor, I view section 215 as a common-sense investigative tool. I recognize, however, that the provision has been the subject of concern by many across the country. Part of the reason for this, I believe, is that many of the safeguards contained in section 215 to protect civil liberties are not widely known or understood.

Upon close examination, for instance, it is clear that orders requesting the production of records under section 215 are actually more protective of civil liberties than are grand jury subpoenas. Grand jury subpoenas and section 215 orders are governed by a similar standard of relevance; investigators may only seek to obtain records that are relevant to an ongoing investigation. To obtain any records under section 215, however, investigators must first obtain a court order. Grand jury subpoenas, by comparison, do not require prior judicial approval.

Section 215, unlike grand jury subpoenas, also explicitly protects First Amendment activities as investigations utilizing the provision may not be solely based on

such activities. For example, Americans may not be investigated under the provision solely because of their political speech. Section 215 also has a very narrow scope; it can only be used (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, as can grand jury subpoenas, to investigate domestic terrorism or ordinary crimes. And finally, section 215, unlike grand jury subpoenas, is subject to regular congressional oversight. The Attorney General is required to file reports with appropriate congressional committees on a semi-annual basis fully informing them of the Department's use of the provision.

To some, section 215 has become known as "the library provision". This moniker, however, is a gross distortion of the provision and makes about as much sense as calling all grand jury subpoenas "library subpoenas." Section 215 does not single out or mention libraries, and the Attorney General has recently declassified that as of March 30, 2005, the provision had never be used to obtain library records.

As explained above, section 215 can be used to request the production of a wide variety of records, and library records are simply one of the types of records to which the provision could theoretically be applied. While some have called for library and bookstore records to be exempted from section 215, I think that this course of action would be a serious mistake.

Libraries should not be carved out as safe havens for terrorists and spies. We know for a fact that terrorists and spies use public libraries. In the spring of 2004, to give one example, federal investigators in New York conducted surveillance on an individual who was associated with al Qaeda. In the course of tracking the individual, investigators

noted that, although he had a computer at his home, he repeatedly visited a library to use the computer. Investigators discovered that the individual was using the library computer to e-mail other terrorist associates around the world. The library's hard drives were scrubbed after each user finished, and he used the computer at the library because he believed that the library permitted him to communicate free of any monitoring. Thankfully, this individual is now in federal custody. But this example should teach us that we should not make it more difficult to investigate a terrorist's use of a library computer than his or her use of a home computer.

In criminal investigations, prosecutors have subpoenaed library records for years. For example, in the 1997 Gianni Versace murder case, a Florida grand jury subpoenaed records from public libraries in Miami Beach. Similarly, in the Zodiac gunman investigation, after investigators came to believe that a Scottish occult poet inspired the gunman, they prompted a grand jury in New York to subpoena library records to learn who had checked out the poet's books. And the Iowa Supreme Court has even upheld the use of subpoenas to obtain library records in an investigation of cattle mutilation. Surely, if grand jury subpoenas could be used to obtain such records in these criminal investigations, national security investigators, with court approval, should have the option of obtaining these records in appropriate international terrorism or espionage investigations.

Just as prosecutors use grand jury subpoenas in a responsible manner, information recently declassified by the Justice Department reveals that the Department has used section 215 in a judicious manner. As of March 30, 2005, federal judges have reviewed and granted the Department's request for a section 215 order 35 times. To date, the

provision has only been used to obtain driver's license records, public accommodations records, apartment leasing records, credit card records, and subscriber information, such as names and addresses, for telephone numbers captured through court-authorized pen registers and trap-and-trace orders (a pen register records the numbers a telephone dials and a trap-and-trace device records the numbers from which it receives calls). The Department has not requested a section 215 order to obtain library or bookstore records, medical records, or gun sale records.

Like section 206, section 215 is scheduled to sunset at the end of 2005, and it is important that the provision is made permanent. If section 215 were allowed to expire, it would be easier for prosecutors to obtain relevant records in investigations of non-violent crimes than for national security investigators to obtain relevant records in international terrorism investigations. Given the threat to the safety and security of the American people posed by terrorist groups such as al Qaeda, Congress must not let this happen.

IV. Conclusion

Thank you once again for the opportunity to discuss sections 206 and 215 of the USA PATRIOT Act. These two provisions are critical to the Department's efforts to protect Americans from terrorism, and from my experience as a prosecutor, I know firsthand the importance of roving wiretap orders and the ability to obtain relevant records in criminal investigations. I look forward to answering any questions you might have.