Testimony of

ROBERT S. KHUZAMI
Former Assistant United States Attorney
United States Attorney's Office
Southern District of New York

Before the
House Judiciary Committee
Subcommittee on Crime, Terrorism and Homeland Security
April 28, 2005

Chairman Coble, Representative Scott, and members of the Subcommittee on Crime, Terrorism and Homeland Security, thank you for inviting me here this morning. It is an honor to testify before you, particularly on a matter of such importance to our national security.

I am currently a lawyer in private practice in the New York area. For nearly 12 years, I was an Assistant United States Attorney in the United States Attorney's Office for the Southern District of New York, and spent a significant amount of time working on counterterrorism cases. From shortly after the February 26, 1993 bombing of the World Trade Center through early 1996, I was a member of the team that prosecuted Sheik Omar Abdel Rahman -- the blind cleric who led the Egyptian-based Islamic Group and played a key role in the 1981 assassination of President Sadat -- and eleven others for conducting a war of urban terrorism against the United States. Their acts included, among other things, the WTC bombing, the 1990 murder of Rabbi Meir Kahane (the founder of the Jewish Defense League), plots to murder various political and judicial leaders, and a conspiracy to carry out a "Day of Terror" – the simultaneous bombing of various New York City landmarks, including the United Nations complex, the Lincoln and Holland Tunnels (through which thousands of commuters travel daily between lower Manhattan and New Jersey), and the Jacob K. Javits Federal Building that houses the FBI's New York Headquarters.

Following the events of 9/11, I assisted in supervising the U.S. Attorney's Command Post in lower Manhattan, where hundreds of law enforcement and intelligence personnel worked tirelessly to investigate that attack and to prevent another.

The changes set forth in the PATRIOT Act, as well as the events of 9/11 in general, have brought about significant public debate about the appropriate balance of civil liberties, privacy and security. That debate is undeniably healthy, a fact which Congress recognized when it sunsetted certain PATRIOT Act provisions in order to provide an opportunity for an informed evaluation of their impact.

Two PATRIOT Act provisions are being considered this morning -- Section 206, the so-called "roving wiretap" provision and Section 215, the access to records provision. I approach my analysis from two perspectives. The first is that of an ex-prosecutor of terrorism crimes, who believes firmly that we must fully identify and utilize every lawful tool to prevent terrorist attacks and capture those involved. The second is as an American citizen who recognizes the fundamental importance of the privacy rights and civil liberties of all Americans. Balancing these two perspectives, I conclude that, with two amendments recently embraced by the Department of Justice ("DOJ"), Sections 215 and 206 should be reauthorized.

Section 215

Section 215 authorizes the Foreign Intelligence Surveillance Court to order the production of "tangible things (including books, records, papers, documents and other items)" as long as they are "sought for" an "authorized investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities." In its most common application, Section 215 permits the government in terrorism investigations to obtain business records held by third parties, including those held by banks, hotels, landlords, credit card companies and, yes, libraries and bookstores. Somewhat surprisingly, Section

215 is viewed by many Americans as a radical extension of government authority that permits unprecedented snooping into the library records and private reading habits of Americans, and threatens to sweep up innocent Americans into secret investigations of terrorist activity. It has caused such angst amongst librarians that it has been labeled the "Angry Librarians Provision."

Four points need to be made. First, Section 215 permits a court to order the production of standard business records from third parties. These are the same records that prosecutors across the country routinely obtain every day in drug, larceny, fraud, corruption and all manner of standard criminal investigations. They include credit card receipts, bank statements, hotel bills, leases, subscriber information for phones, and the list goes on and on. There is nothing unusual or accusatory about requiring third parties possessing these records -- innocent third parties all of them – to produce them in a terrorism investigation of another person. That is all Section 215 does.

Second, Section 215 is agnostic about libraries and bookstores – it neither targets nor exempts them, and the word "library" is nowhere mentioned in its text. In fact, rather than aggressively use Section 215 to collect information about library patrons, as some have feared, the government recently reported that it has obtained Section 215 orders on 35 occasions, but never once for library records. Presumably, this reflects the fact that library records are rarely relevant to terrorism investigations, a fact that should assuage its critics.

Third, terrorists use libraries. The 9/11 Commission found that some of the 9/11 conspirators used Internet access through a Hamburg, Germany library. A recent espionage prosecution revealed that a spy used computer terminals at various public

libraries to send classified information. An Al Qaeda terrorist used library computer terminals to send electronic messages. Terrorists and their sympathizers also create, collect and disseminate writings and speeches that train, recruit and incite others to participate in terrorist acts. In the Blind Sheik prosecution, for example, evidence consisting of bomb-making manuals, including pages containing the fingerprints of co-conspirators, was introduced at trial. In his written sermons, the Blind Sheik extolled the virtues of violent *jihad* against the United States with "the sword, with the cannon, with the grenades and with the missile," and urged his followers to embrace the terrorist label:

> Why do we fear the word 'terrorist?' If the terrorist is the person who defends his right, so we are terrorists. And if the terrorist is the one who struggles for the sake of God, then we are terrorists. . . . They may say 'he is a terrorist, he uses violence, he uses force.' Let them say that.

It is for this reason that library records, writings and other literature have long been available to criminal investigators through the use of a grand jury subpoena. The "Unabomber," Ted Kaczynski, was captured based on a tip from his brother, who thought he recognized the writing in the Unabomber's "manifesto" as that of his brother. Law enforcement corroborated the brother's suspicion in part by examining library records, from which they learned that Kaczynski had checked out little-known books referenced in the manifesto. Section 215 simply extends to terrorism investigations the same authority available to criminal investigators.

Fourth, it does not follow that because the government's has not to date used Section 215 authority to obtain library records, that Section 215 should sunset, or be amended to exempt libraries and bookstores. This would turn libraries into sanctuaries, where would-be terrorists could communicate with their cohorts without fear of

detection. This is not mere speculation – an Al Qaeda terrorist reportedly used library computer terminals to send messages to his associates around the world specifically because he knew the digital records were deleted nightly, thus concealing his activity. Unfortunately, some library representatives are creating de facto sanctuaries by ordering daily shredding of library log-in and other records, in response to misplaced fears about Section 215.

This "use it or lose it" argument is also specious because it equates lack of usage with lack of importance. The mere fact that Section 215 has not been "used" historically to obtain information from libraries or bookstores does not mean that such authority could not be critically important in the next case. More so than criminal prosecutions, terrorism plots, however speculative or nascent, must be zealously pursued by investigators armed with the option of using the fullest arsenal of lawful investigative tools. That is because even a single missed investigative opportunity or misstep can have catastrophic consequences. In contrast, in criminal investigations, for example, it is unfortunate but not fatal if before a stockbroker is arrested, he executes one more stock purchase using inside information. That is not being falsely alarmist; the horrific consequences of the detonation of a dirty bomb over a major urban center, or the Blind Sheik's plan to bomb multiple New York City landmarks simultaneously, are undeniable.

In sum, the four points establish a compelling case for Section 215 reauthorization. They show that Section 215 is not about libraries, but provides for routine document collection in terrorism cases; that as far as libraries are concerned, terrorists use them and library records can provide evidence of that; and that the

catastrophic consequences of a successful terrorist attack demand that we have available all lawful investigative tools.

In addition to these points, the provisions of Section 215 should mollify critics, since they set forth a sensible framework to permit intelligence agents to obtain business records. Section 215 requires the government to certify that the records are "sought for an authorized investigation to obtain foreign intelligence information [not against a United States person] . . . to protect against international terrorism or clandestine intelligence activities." The DOJ interprets this provision as requiring that the records be "relevant" to such investigations, and has endorsed an amendment to that effect. In recognition of First Amendment concerns, Section 215 cannot be used to conduct an investigation based solely on the activities protected by the First Amendment.

The Foreign Intelligence Surveillance Court must approve Section 215 applications. While the level of that judicial review is not high, it is appropriate given the type of records under consideration in Section 215 proceedings. Business and library records are preexisting documents that belong, will be given, or are available, to third parties – banks, landlords, rental car agencies and even librarians – and thus persons lack a reasonable expectation of privacy in them. For that reason, they are obtainable in a criminal investigation with a grand jury subpoena alone, which is issued without judicial review or supervision. From the perspective of judicial review, Section 215 provides more protection, not less, for library patrons than they enjoy in parallel criminal proceedings involving the same records.

To be sure, Section 215 expanded the government's pre-PATRIOT Act authority to obtain records in terrorism cases. This change was overdue, since the prior law was

unnecessarily restrictive. Whereas Section 215 now permits the government to obtain with court approval all "tangible things (including books, records, papers, documents and other items)," the prior provision limited the government to obtaining records from lodging and vehicle rental and storage facilities. Again, criminal investigators have long been permitted to obtain the broader range of records now provided for in Section 215. Comparisons with criminal investigations aside, the expansion of authority under Section 215 makes sense in its own right, since it would be irrational, for example, to permit the government in a terrorism investigation to obtain under Section 215 a would-be terrorist's motel records, but deny it the ability to obtain receipts evidencing purchases of fertilizer or precursor chemicals, or to learn that he obtained books on how to manufacture explosive devices or detect surveillance.

Another expansion of authority in Section 215 was the elimination of the requirement that the government provide "specific articulable facts" that the subject of the investigation was an "agent of a foreign power." Critics assert that elimination of this particularized showing allows the government to use Section 215 to obtain records from persons without showing that they relate to a real terrorist or spy. Of course, as noted above, the third-party records at issue here do not implicate a recognized expectation of privacy. The government should generally be required to make a particularized showing only in circumstances where this is necessary to overcome some legally recognized privacy interest. There may be some instances where a departure from that general rule is warranted, but national security is not one of them – it is where the public interest in government access is most urgent. Leaving that aside, this change recognizes the reality that targets of terrorism investigations are trained to operate through multiple aliases and

identities. It would serve no purpose to delay obtaining what might be records critical to uncovering a terrorist plot simply because the target's real name, or associational connections, has not yet been ascertained. Evidence of the purchase of detonators is equally relevant to preventing a terrorist plot, regardless of whether the government yet knows that the purchaser has ties to Al Qaeda. Once again, elimination of the requirement that a particularized showing be made places terrorism investigations on the same footing as criminal investigations, where no such showing is required to obtain the exact same records.

Critics cite excessive confidentiality – a "gag order" – as another flaw in Section 215. It prohibits persons receiving Section 215 orders from disclosing to third parties those orders or that the FBI has sought or obtained them. Section 215 detractors suggest that the threat of government overreaching in Section 215 would be less troubling if the statute allowed for more transparency, such that the public could understood what records the government sought and why. Critics also contrast Section 215's confidentiality provision with the grand jury process, where they claim the recipient receives notice of the subpoena and can move to quash it in court.

It is unassailable that real and potentially catastrophic harm can result from the premature disclosure of a terrorism investigation. I agree, however, that this risk does not justify barring recipients of Section 215 orders from consulting with attorneys, and from challenging the order before the Foreign Intelligence Surveillance Court. The DOJ has publicly agreed with this position. If such consultation and challenge were permitted, it would place Section 215 proceedings on a par with grand jury proceedings, where the

subpoena recipient obviously knows of its existence and can challenge it in court, but at the same time may be prohibited from disclosing its existence to others.

Beyond this amendment, however, the confidentiality provisions of Section 215 should not be disturbed. You do not want potential terrorists to know you are investigating them or are aware of their plans. A leak could cause conspirators to accelerate the plot to a point where authorities are less prepared to prevent it or protect American lives. Or terrorists might abandon the plot, destroying evidence and taking flight, which would hinder prevention, capture and prosecution. The plot might later resurface, at a point when we are less prepared and more vulnerable. Each and all of these scenarios present a missed opportunity to protect innocent Americans from harm. Premature disclosure also risks harm to agents, witnesses and undercover operatives. Against this risk of harm must be weighed the interests that are served from permitting the recipient of a Section 215 order to disclose it to persons other than an attorney. Whatever that interest is, it does not in my view outweigh the risk that flows from wrongful disclosure.

Some Section 215 criticisms assume the existence of large numbers of "rogue agents," who are characterized as inclined, given the opportunity, to violate the civil liberties and privacy rights of Americans by searching for and exploiting legal and administrative loopholes to browse through their reading materials and subscription and membership lists. This hypothetical rogue agent then becomes, so the argument goes, the justification for additional Section 215 restrictions. It is not apparent to what extent, if at all, such rogue agents exist. As Andy McCarthy wrote, agents "generally lack voyeuristic interest in the public's reading and viewing habits . . . and voluminous

information streams and finite resources leave no time for this sort of malfeasance."[1] The agents, analysts, translators and surveillance specialists with whom I worked were dedicated, talented and law-abiding. And the gauntlet of administrative guidelines, directives, policies, laws and committees applicable to the FBI and DOJ, as well as congressional and judicial oversight, all deter rogues by providing training, oversight, and a mechanism for redress and discipline.

Even assuming rogues present the threat identified by Section 215 critics, it hardly follows that the restrictions they suggest would have the desired effect. Those determined to break rules are not easily deterred, and the real impact of such restrictions may be to unnecessarily burden the conscientious, law-abiding agent trying to do his job effectively. In the end, the best response to the "rogue agent" concern is the empirical evidence -- according to the DOJ's Inspector General, who was required under Section 1001 of the PATRIOT Act to investigate complaints of abuse of civil rights and liberties under the Act, there have been no documented cases of abuse of civil rights or liberties from the PATRIOT Act in the more than three and one-half years since its passage.

In sum, Section 215 orders are useful investigative tools in combating terrorism. Most of what the statute permits is already available in criminal investigations, and any differences either make good investigative sense and, given the DOJ's willingness to consider two amendments, do not threaten the legitimate privacy and civil liberty interests of Americans.

[1] Patriot Debates: A Sourceblog for the USA PATRIOT Debate (available at http://www.patriotdebates.com/214-and-215)

Section 206

Section 206 of the PATRIOT Act provides for so-called "roving" wiretaps and other electronic surveillance in foreign intelligence and counterterrorism investigations. Prior to PATRIOT, once having obtained the approval of the Foreign Intelligence Surveillance Court for a wiretap, agents had to return to that Court each time the subject of that surveillance switched phones, in order to amend the order to direct the new electronic communications provider to give the technical assistance necessary to install and maintain the new wiretap. Due to concerns that targets were rapidly changing phones to avoid detection, including prior to important conversations and meetings, Section 206 eliminated the need for agents to return to the Court each time a target switched devices. It accomplished this by permitting the government, upon a showing that the subject is taking steps to thwart surveillance, to include in the original order a general directive that any electronic communications provider extending services to the target in the future must provide the necessary technical assistance.

In part because authority for "roving" wiretaps has long been available in criminal cases, the only serious criticism of section 206 is that it allows intelligence investigators to conduct "John Doe" roving surveillance that permits the FBI to wiretap every single phone line, mobile communications device, or Internet connection the suspect may use without having to identify the suspect by name. This criticism ignores hurdles that guard against overly-broad wiretapping. First, "roving" wiretaps are available only upon a showing that the subject is taking steps to avoid surveillance. Second, where agents cannot identify by name the target of a proposed wiretap, they must describe the subject with sufficient particularity to convince the FISA Court that there is probable cause to

believe the subject is a "foreign power" or an "agent of a foreign power." That is, the wiretap order applies only to a specific person, even if the government has not yet ascertained his or her identity. The alternative – to make wiretaps unavailable until the target is identified – is a highly risky restriction, since valuable intelligence may be lost while a person's identity is investigated, especially given that terrorists operate in a clandestine world and are trained to use multiple aliases and identities. Third, if the government wants to conduct a wiretap of a new target, it must return to the Court with a new application. Finally, agents conducting wiretap investigations must abide by "minimization" requirements, which strictly control the monitoring and retention of conversations by innocent persons not involved in the wrongful conduct.

These provisions provide adequate safeguards to protect the civil liberties and privacy interests of Americans.

Conclusion

I strongly urge the Committee to reauthorize Sections 206 and 215 of the PATRIOT Act. These provisions strike the correct balance between homeland security and civil liberties.

I thank the Committee for its time and attention, and would be happy to answer any questions.