Prepared Remarks for Attorney General Michael B. Mukasey at the American Bar Association National Security Law Breakfast

The University Club
December 19, 2007 - 8:30AM

Thank you Stewart for that introduction. It's a pleasure to be here with you today. I want to talk to you this morning about the need to put in place—permanently—the national security tools that we use for the war on terror—and in particular, about the need to modernize the Foreign Intelligence Surveillance Act, or "FISA" as it's commonly called.

Since becoming Attorney General, I've learned quite a lot, from my perspective, about how vital it is that we get timely intelligence to protect Americans from those who think it is their religious duty to do us harm. We have seen what happens when terrorists go undetected. We have to do everything possible, within the law, to prevent terrorists from translating their warped beliefs into action.

To stop them, we have to know their intentions, and one of the best ways to do that is by intercepting their communications. The United States has tremendous technological capabilities in such disciplines as computer science, telecommunications, and cryptology, but we've not been allowed to use that capability to full advantage. The same cannot be said of our enemies. Our adversaries adhere to fanatical ideologies based on their tortured views of teachings from the seventh century. But they take full advantage of twenty-first century technologies to recruit, organize, and command their international network of terrorist operatives. It is critical that we leverage our capabilities to intercept and monitor their communications to the fullest extent.

The main law that governs our ability to intercept communications of foreign powers and agents of foreign powers, including international terrorists, is outdated. That statute, FISA, was enacted in 1978, and thus is almost thirty years old. FISA, as many of you know, regulates when the Government must obtain a court order to conduct foreign intelligence surveillance, including the interceptions of communication of our foreign adversaries.

Much has changed from the time when FISA was enacted.

First, the statute was enacted before some of the most dramatic changes in communications technology in world history. For example, the statute was passed long before the use of the internet and cell phones became commonplace. It was also written at a time when international communications traveled more frequently by radio, as opposed to by wire.

FISA defined key terms—most notably its definition of "electronic surveillance," which establishes the circumstances under which court approval is required—by reference to the technologies of that time. The dramatic changes in telecommunications technology since 1978 resulted in an expansion of the scope of activities covered by FISA, and caused FISA to apply increasingly to our efforts to surveil the communications of terrorists and other intelligence targets located overseas.

The government often had to obtain an order from the FISA Court – a process that includes the burdensome completion of detailed paperwork and can result in significant delays—before monitoring the communications of these foreign targets. In certain cases, this requirement of obtaining a court order slowed, and in some cases may have blocked, surveillance efforts that were potentially vital to the national security.

As the Director of National Intelligence has stated publicly, these requirements resulted in an intelligence gap.

These requirements also gave terrorists located in foreign countries the protections Americans enjoy, and diverted resources that would have been better spent on protecting the privacy interests of people here in the United States.

Second, when FISA was passed in 1978, the United States had not yet been subjected to major terrorist attacks on U.S. soil. At the time, the faces of terrorism were seen in such groups as Black September, the Baader-Meinhof Group, and the Japanese Red Army. It was a time when Congress was worried that, if a terrorist hijacked an airplane, the purpose would be "to force the release a certain class of prisoners or to suspend aid to a particular country." Sounds almost quaint today. It was not a time in which we worried that a hijacked airplane would be turned into a missile steered by suicidal terrorists to inflict mass civilian casualties on our homeland.

In other words, the nature of the threat we face, and the technological landscape through which that threat manifests itself, has changed a lot in the days since 1978. Last spring, the Administration sent Congress a comprehensive legislative package to amend FISA to meet today's intelligence challenges. Congress recognized the need to close the intelligence gap that had been created by outdated provisions of FISA, and in August, Congress passed the Protect America Act of 2007.

In simplified terms, this Act allows our intelligence professionals to surveil foreign intelligence targets located abroad without prior court approval. Also, contrary to much of the rhetoric that followed the passage of the Protect America Act, that legislation gave the FISA Court a significant role in those collections, authorizing the Court to review the procedures in place for deciding whether targets of surveillance under the authority are in fact overseas.

The new law has made us safer and has closed the intelligence gap.

That measure of safety, unfortunately, was temporary. The Protect America Act contains a "sunset" provision. Absent legislative action by Congress, the Protect America Act will expire on February 1, 2008.

I must say that I have learned quite a lot about the merits of sunset provisions from my role in overseeing the implementation of the Protect America Act. That Act's sunset provision is in many respects understandable; the Act was passed quickly, in response to Congress's concerns about our Nation's security in a heightened threat environment, and it is under circumstances like those that sunsets provisions are most appropriate. But sunset provisions also have significant costs.

The uncertainty about what the rules will be governing critical intelligence collection presents serious challenges to our intelligence professionals. That uncertainty also provides disincentives to third parties to cooperate with us. If the rules are going to be different tomorrow from what they are today, then it's hard to justify investing money and time today.

These are serious costs that should be considered during the current debate, where—although Congress has had extensive hearings and debates on the need to modernize FISA—some continue to urge that any reforms be accompanied by a short and disruptive sunset provision.

As I mentioned in the outset, our goal as a nation should be to develop long-term, institutional changes that improve our capabilities to prevent terrorist attacks—and sunsetting undermines our ability to do that.

Since Congress passed the Protect America Act, as you all are aware, there has been significant debate and discussion about how to offer long-term solutions to modernize FISA. This has been, by and large, a positive, collaborative process between Congress and the Executive Branch, and we will continue to work closely with Congress to put these needed authorities on a permanent footing.

Since the Act passed, officials from the Justice Department and the Intelligence Community have testified many times about the needed authorities; we have held briefings on our implementation of the Act and oversight of our use of these authorities, and we have met with Congressional Members and staff on these issues, as well as on how the permanent legislation should look.

I am hopeful that there is now consensus about the core authorities in the Protect America Act, and that they are the right ones—that our intelligence agencies should not have to get individualized FISA Court orders in order to conduct surveillance of foreign intelligence directed at targets in foreign lands. That is the core of the intelligence act.

I also want to address the issue of protecting telecom companies from lawsuits. It's critical that Congress provide retroactive liability protection for telecommunications companies, as a bipartisan bill from the Senate Intelligence Committee does. Let me explain why this is important.

Over 40 lawsuits have been filed against telecommunication companies simply because these companies are believed to have assisted our intelligence agencies after the attacks of September 11th. The amounts these claims–which run into the hundreds of billions of dollars; that's billions with a B--are enough to send any company into bankruptcy. These companies face lawsuits, they face bankruptcy, they face loss of reputation, they face millions of dollars in legal fees, all because they are alleged to have helped the government in obtaining intelligence information after 9/11.

Even if you believe the lawsuits will ultimately be dismissed, as we do, the prospect of having to defend against these massive claims is an enormous burden for the companies to bear.

Not only is the litigation itself costly, but the companies also may suffer significant business and reputational harm as the result of the allegations against them—allegations which may or may not be true, but to which they cannot publicly respond, because they're not allowed to confirm or deny whether, and to what extent, they provide classified assistance to the Government.

Many of these companies also have a heavy overseas presence, and that aspect of their business may be particularly vulnerable to financial and physical harm as a result of the litigation. As you might imagine, these companies and others may decide that it's too risky to help the Intelligence Community in the future, no matter how great our need for their assistance may be. And after a year studying this issue, that's exactly what the Senate Intelligence Committee found. That committee said in its report—that, "without retroactive immunity, the private sector might be unwilling to cooperate with lawful Government requests in the future," resulting in a "possible reduction in intelligence" that the committee said is "simply unacceptable for the safety of our Nation."

In an age where we need to use every possible advantage to understand an enemy that may seek to exploit and hide within the vast expanses of the internet, we simply cannot afford to discourage the private sector from helping us to detect and prevent the next terrorist attack.

And not only is immunity in the best interest of our Nation's security, it's also a fair and just result. After reviewing the relevant correspondence between the Executive Branch and the companies that did assist with communications intelligence activities after the September 11 attacks, the Senate Intelligence Committee concluded that those companies acted on a good faith belief that their assistance was lawful.

Indeed, as the Committee recognized, the companies were responding during an extraordinary time of national emergency and relied on written assurances that the President himself authorized the activities and that high-level Government officials had determined the activities to be lawful. Given these unique circumstances, such companies deserve our gratitude, not litigation.

Some, however, argue that we should not provide blanket immunity because the private sector will have less incentive in the future

to insist on the Government's compliance with applicable statutes. The liability protection offered in the Intelligence Committee bill, however, is not blanket immunity.

It applies only in a very narrow set of circumstances—if the Attorney General certifies to a court that the company either (1) did not provide the alleged assistance, or (2) did provide assistance between September 2001 and January 2007 with communications intelligence activities designed to detect and prevent a terrorist attack, and only after receiving a written request from a high-level Government official indicating that the activity was authorized by the President and determined to be lawful.

A court must review this certification before an action may be dismissed, and the immunity does not extend to the Government, Government officials, or any criminal conduct. In short, the provision in the Intelligence Committee's bill would provide protection only in circumstances where such protection is appropriate.

Others have raised concerns about dismissing the lawsuits altogether and have therefore proposed continuing the cases with the Government substituted as a defendant in place of the telecommunication companies. Proposals for substitution may reflect a genuine desire to remove the companies from the lawsuits, but that's not an adequate solution. If the cases continue, even solely against the Government, the companies would still be subject to the type of third party discovery requests, litigation costs, and reputational harm that could deter their future cooperation with the Intelligence Community. After all, the point of the lawsuits would still be to expose whether particular companies provided assistance, and, if they did, what that assistance entailed. And if that kind of information is exposed through litigation, it will harm not only the companies, but also the national security. The lawsuits and the information they generate could become a smorgasbord for our enemies.

As the Intelligence Committee concluded in its report, the specific identity of those who assist us with intelligence activities and the nature of their assistance must be protected as vital intelligence sources and methods. The risk of disclosing that kind of information is not a risk worth taking, particularly where the only effect of substituting in the Government as a defendant would be to shift any liability from the telecommunication companies to the American taxpayer.

Because of the risks, and because the proposed liability provision covers telecommunications companies that simply did what the Government asked them to do, it makes no sense to allow this litigation to go forward. The proposed alternative of substitution would force the American taxpayer to bear the cost and risks of litigating the very assistance that their Government asked for in order to help protect our Nation and would be bound to result in disclosures that could harm us.

Providing immunity to these companies will not, by itself, deprive critics of the Government's surveillance activities of their day in court. There are already a number of surveillance cases against the Government itself winding their way through the courts. While we strongly believe those cases must also be dismissed in order to protect highly classified intelligence information, the courts are going to have the final say over that. What protecting companies will do, as the Senate Intelligence Committee concluded on a near unanimous and bipartisan vote of 13 to two, is to encourage private entities to help us in the future, when lawful, by not punishing those who have provided good faith assistance in a time of crisis with the threat of ruinous liability. That's a goal that will serve the security of this Nation for many years to come, well beyond the current Administration.

Recently, within the last couple of days in fact, a proposal has been made as an alternative to the Congress deciding on the issue of immunity. Under that proposal, the litigation would be sent to the FISA Court to decide, under a multi-part test, whether the provider's assistance was appropriate. In contrast to the relevant provision of the Intelligence Committee bill, which would allow for the prompt dismissal of the litigation, this new proposal would likely result in protracted litigation. That is, the companies would continue to be subject to the burdens of litigation to determine how and why they assisted the Government. And the litigation would still risk the disclosure of highly classified information.

These risks are unnecessary and unwise. The Senate Intelligence Committee has concluded that those who assisted received written assurances that the activities were lawful and were being conducted pursuant to a Presidential authorization. Transferring those cases to the FISA Court after this extensive review could be read as sending a signal that Congress doubts the actions of these companies--the same companies the Intelligence Committee recognized that we rely on to help us protect the Nation.

It could cause companies in the future to feel compelled to make an independent finding that before complying with a lawful Government request for assistance, they have to conduct their own investigation. That could cause dangerous delays in critical intelligence operations and put the companies in the impossible position of making the legal determination without access to the highly classified facts that they would need to do so.

Let me put the importance of private sector cooperation to our national security in some historical perspective. In the Second World War, private industry was not on the sidelines. It was engaged, such that the full measure of this Nation's might was brought to bear against our enemies. Some of the assistance of private industry to the United States and its allies came before the bombs dropped at Pearl Harbor.

Of course, after the bombs dropped on Pearl Harbor, American industry turned from peacetime production to wartime production virtually overnight. Our government was a part of some of that effort, but much of it was voluntary. Our armed forces and those of our allies were by any measure an awesome force. But our armies did not win World War II alone. They won with the cooperation of American industry and the assistance of civilians.

We had our Pearl Harbor on September 11th, 2001. We will need the level of cooperation from American industry that was seen in World War II, and we will need to tap into the technological ingenuity of the private sector if we are going to prevail. Our military, our intelligence agencies, and our law enforcement agencies are forces to be reckoned with, as they should be. But we cannot fight this fight alone. We have to be able to enlist and draw upon the lawful cooperation of the private sector.

And of course, our efforts against that threat also must take place with scrupulous respect for civil liberties and within the rule of law. FISA modernization legislation is only one example of how we put in place a tool that we need to fight against terrorists, while protecting the rights of Americans. I recognize that as Attorney General I have to be committed to both of those goals. I am here to tell you that I am Thank you very much for inviting me today.

###