Department of Justice

Prepared Remarks of Kenneth L. Wainstein, Assistant Attorney General for National Security at the Georgetown University Law Center's National Security Center

SEPTEMBER 10, 2007

Symposium on Foreign Intelligence Surveillance Act (FISA) Modernization

WASHINGTON, D.C.

This conference is a great idea. It gives us an opportunity to share thoughts about where our surveillance authorities should be -- how the powers should be defined and where the lines should be drawn. And the line I'd like to talk about today is the line between domestic surveillance and overseas surveillance – how the law should distinguish between those two areas of surveillance and how much each area should be subject to judicial review.

There is no question that we should have to get court orders when we want to collect domestic communications or target individuals within the U.S. The question for today is whether we should have to do so when we are targeting surveillance against a person who is outside the United States, where constitutional and privacy protections do not apply.

And, this is not a discussion with only legal or theoretical implications. There are very practical, operational implications here -- implications that will dictate whether we have sufficient coverage overseas or only narrow coverage of our foreign adversaries; whether we can move nimbly and quickly among overseas coverages, or whether we have to go through a resource-consuming court approval process before we go up on one of our adversaries.

In considering this issue, it's useful to look back at the history and the evolution of our surveillance laws. And, when you do that you see that this is a recurring theme. There have been a number of major turning points in the law along the way, and at each of these turning points, we've seen the repetition and reinforcement of this fundamental distinction between foreign and domestic surveillance -- a distinction that finds its origins in the Constitutional balancing between executive authority to take efforts to protect the nation against external threats and the judiciary's authority to protect privacy interests.

You can see this consistent theme as you go back through the evolution of the law. The first turning point in the development of our surveillance law came in the 1960s. In 1967, the

Supreme Court held that telephone conversations were protected by the Fourth Amendment. The next year, Congress responded to the Court's decision by passing the wiretap statute that established a procedure by which the government had to secure a court-issued warrant before wiretapping the subject of a criminal investigation.

While both the Supreme Court decision and the ensuing legislation were clear on the need for a warrant requirement when the government was wiretapping a person in the United States for purposes of a criminal investigation, both the Court and Congress were very careful to carve out surveillances for national security purposes. They made it clear that domestic surveillance for evidence in a criminal case was covered by the warrant requirement, but that national security surveillance involving foreign threats was not.

The next turning point came a decade later, when Congress passed the Foreign Intelligence Surveillance Act, which imposed a court review mechanism for electronic surveillance designed to collect foreign intelligence information. We came to this juncture after it was disclosed in the Church and Pike Hearings that the government had abused its flexibility in the area of national security investigations to investigate domestic persons who had no connection to a foreign power. After those disclosures, Congress and the country were understandably looking for a way to ensure that the executive branch could no longer invade their privacy under the guise of protecting against foreign threats. The result was legislation that subjected our foreign intelligence surveillances to court review.

The Foreign Intelligence Surveillance Act (FISA) was passed in 1978, and it created a regime of court approval for national security surveillances. However, once again, Congress reinforced the distinction between domestic and foreign surveillance. Congress designed a judicial review process that would apply primarily to surveillance activities within the United States where privacy interests are the most pronounced and not to overseas surveillance where privacy interests are minimal or non-existent. Congress gave effect to this careful balancing through its definition of the statutory term "electronic surveillance," the term that identifies those government activities that fall within the scope of the statute and, by implication, those that fall outside it. Congress established this dichotomy by defining "electronic surveillance" by reference to the *manner* of the communication under surveillance -- by distinguishing between "wire" communications -- which included most of the local and domestic traffic in 1978 -- and "radio" communications -- which included most of the transoceanic traffic in that era.

Based on the communications reality of that time, that dichotomy more or less accomplished the Congressional purpose, as it distinguished between domestic communications that generally fell within FISA and foreign international communications that generally did not.

But, that finely-balanced distinction has eroded with the dramatic changes in communications technology in the 29 years since FISA was enacted. In that time, we've seen the migration of the majority of international communications from satellite transmission (which qualified as "radio" communications under the statute) over to fiber-optic cable (which is "wire" under the statute); and, as a result, we've seen the tipping of that careful balance in the FISA statute. As the technology evolved further and further away from the paradigm established in the

statute, we had to subject more and more of our overseas collections to review by the FISA Court.

So we had a situation where, on one hand, we have this technological change making it more difficult for us to surveil overseas threats. And on the other, we have the backdrop of an increasing national security threat from international terrorism -- from terrorists who had hit us hard on 9/11; who were bent on inflicting catastrophic damage to us and our allies; who were taking full advantage of modern modes of communication to organize and command their international network of terrorist operatives; and who have continued to show resiliency and a determination about their work -- as reflected quite clearly in the disruption last week of a large-scale terrorist plot in Germany, and also as reflected in the recently-issued National Intelligence Estimate.

And it is the combination of these two historical trends -- the changing technology that handicapped our efforts to surveil our adversaries and the increasing threat posed by those adversaries -- that produced the turning point we came to this year.

And, this is the turning point that Congress addressed last month when they passed the Protect America Act. The legislation was very straight-forward but very effective. In short, it returned FISA to its original focus on domestic surveillance. And it did that by making it clear that -- regardless of the type of communication being surveilled or the location where the surveillance takes place -- FISA does not apply when the surveillance is targeting persons outside the United States. It does apply – and we have to get a court order – when the communications are domestic or when we target someone in the U.S. But, when the target is truly foreign, when we're targeting someone in another country, we don't need to go through the FISA Court.

For my money, it's an exceptionally fine piece of legislation. I know, however, that there might be some of you out there who don't completely agree with me on the Protect America Act.

In fact, I was up in front of Congress last week and found that there were some members who had questions about it as well. And, maybe that's why Congress didn't grant us this authority on a permanent basis, but instead gave it to us with a six-month sunset.

While I'm not usually a fan of legislative sunsets and renewal periods, this is one renewal period I don't have much problem with. And that's because I see it as an opportunity.

I see it as an opportunity to clearly demonstrate to Congress -- and to the American people -- that we can use this authority both effectively and responsibly.

And that's something we're already starting to do. We have set up an oversight regime that goes way beyond what the statute requires. It includes rigorous internal agency audits by the agencies using this authority. And it includes regular, on-site compliance reviews by a team from the Office of the Director of National Intelligence (ODNI) and the National Security Division (NSD) of the Department of Justice. This DNI/NSD team has already completed its

first audit, and it will complete further audits every 30 days during this interim period to ensure full compliance with the implementation procedures.

We have also agreed to provide an unprecedented level of reporting to Congress. We are giving the Intelligence and Judiciary Committees copies of the procedures we are using to implement this authority; we have promised to give them comprehensive briefs about our implementation of this authority every month throughout this renewal period; and we have promised them the results and written reports of our compliance reviews.

We recognize an important truth here -- which is that we'll be allowed to keep this vital authority only if we show that we can use it responsibly. And, that's exactly what we're going to do. Over this six-month period, we're going to establish a track record that will persuade Congress and the American public that the Protect America Act was the right decision and that Congress turned in just the right direction when it reached that turning point back in early August.

I want to thank Neal Katyal, David Kris and Jim Baker for setting up this conference. FISA reform is a critically important issue, and from where I stand, I welcome this discussion. I feel that the more people understand FISA law and practice and how much we do to protect civil liberties, the more comfort people will have and the more likely we'll be given the tools we need to do our job – which is to protect our country and our liberties.

I appreciate you all coming here to be a part of this discussion, and I'll be happy to answer any questions.

# # #