Testimony of

James A. Baker

September 25, 2007

Testimony of James A. Baker
Before the
Committee on the Judiciary
United States Senate
September 25, 2007

Mr. Chairman and members of the Committee: thank you for the opportunity to appear before you today to discuss foreign intelligence collection in the 21 st Century, including possible changes to the Foreign Intelligence Surveillance Act of 1978 (FISA) and the Protect America Act of 2007. The issues we will discuss today are very complex and very important. The actions you will take based upon what we are talking about today will have a significant impact on the safety and the freedom of the American people.

From 1998 until January of this year, I was responsible for, among other things, intelligence operations for the Department of Justice. Working with many dedicated professionals in my office - the Office of Intelligence Policy and Review (OIPR) - we represented the United States before the Foreign Intelligence Surveillance Court (FISC), which Congress created in 1978 under FISA. I have prepared, reviewed, or supervised the review and preparation of thousands of FISA applications. The Department of Justice has specifically approved my testifying before the Committee today. Let me emphasize, however, that I am appearing here strictly in my personal capacity, and that the views I express do not necessarily reflect those of the Department of Justice or the Administration.

In the brief time that I have available this morning, I would like to focus on three areas that I think are important to understand in order to determine how best to conduct foreign intelligence collection today. I will not discuss the threat that we face today from hostile foreign powers such as international terrorist groups like al Qaeda. Based upon information that the Intelligence Community has made available to the public, it seems to me that we should assume that we face significant threats that will persist for some time. It appears that al Qaeda wishes to cause as much death and destruction as possible with respect to the United States, and is actively seeking to acquire the means to do so.

FISA's Productivity. First, FISA collection has been extremely productive over the years. The version of FISA that was in effect until August of this year enabled the Intelligence Community to obtain timely and accurate foreign intelligence information about the capabilities, plans, intentions, and activities of foreign powers, persons, organizations, and their agents. FISA served us well throughout the Cold War and it continued to serve us well after the fall of the Soviet Union, even post-9/11. Until the Protect America Act passed in August of this year, most of the core definitions and procedures of FISA had not changed since 1978. And yet using FISA we were able to collect a significant amount of actionable foreign intelligence information (meaning that the Intelligence Community could take prompt action on it) to thwart the plans and activities of our adversaries, including terrorist groups. We could also disseminate the information appropriately within the government and to our foreign partners, and use the information acquired as evidence in criminal trials with the approval of the Attorney General. At the same time, everyone in the system had the comfort of knowing that their actions were lawful, and that they would not be subject to lawsuits or criminal prosecution for having performed in conformance with an act of Congress and federal court orders.

Indeed, there is a paradox with respect to the entire discussion that we are having today. The calls for FISA to be amended result ultimately from the success of FISA itself. Because we were able to collect vital intelligence information in a timely manner through FISA - especially including information about the activities of terrorists located overseas - the Intelligence Community came to regard FISA as a critically important collection platform. U.S. intelligence agencies increasingly turned to the FISA process to obtain the information that they needed to execute

their duties. Moreover, I also believe that our success in FISA collection informed elements of the Intelligence Community about the value of certain types of collection, which led to the growth in the targeting of foreign operatives that has resulted in the desire to change the law that we see today.

Before you decide whether to renew or modify the Protect America Act or make other changes to FISA, I believe that you should ask the Intelligence Community for a thorough analysis of the productivity of the FISA program. I have testified previously before this Committee in closed session about those successes, which I am unable to repeat here today in open session. Suffice it to say that I believe that the record will show that the original FISA contributed significantly to our successes against al Qaeda and other terrorist groups post-9/11, and that FISA worked during wartime. That is not to say that it has been easy. The dedicated men and women from the Office of Intelligence Policy and Review who worked long hours under adverse conditions to enforce the law that Congress had enacted deserve the Nation's gratitude. Each of them exemplifies what it means to be a dedicated public servant. And their actions are worthy of the examination of historians in the years to come.

FISA's Scope. Second, let me focus for just a moment on what we can collect under FISA. To begin with, no means of collection are barred by the 1978 statute. We could obtain authorization to collect all forms of modern communication under the original FISA. Let's also clarify another point - FISA has never applied to wire or radio communications that are clearly from one person in a foreign country to another person in a foreign country. As I discuss a bit later, the problem we face today is that it is not always easy or possible to tell where all of the parties to a communication are located when the interception takes place. FISA also covers physical searches in the United States, including searches of residences and stored data, and other collection as well.

Much has been made in the recent past about what types of communications Congress intended to cover in the original FISA and what it sought to exempt. While it is important to understand what Congress intended when it enacted FISA in 1978, I am not sure that it is determinative of what we should do today. In any event, in order to fully understand the role that technical issues played in the legal and policy decisions of the time, one must consider several factors: (1) the historical record to determine what the state of technology was in 1978 and what technological advances were foreseen or reasonably foreseeable at that time; (2) what Congress understood in 1978 about the state of technology; (3) what Congress intended to cover with the law that it enacted; and (4) what the law that Congress enacted actually covers.

With respect to the state of technology at the time, my preliminary review of some public record materials that I have accessed only recently seems to indicate that transoceanic communications were made in relatively large quantities by both satellites (radio) and coaxial cables (wire); that both kinds of systems were expected to continue in service for many years; and that the use of fiber optics was already anticipated for undersea cables. The lengthy and complex legislative history shows that Congress was concerned about, and considered, many factors when enacting FISA, and some parts of the legislative history appear to suggest that it may well have intended to exclude international communications from the scope of the Act (although this conclusion may be undercut by the fact that at least one of the definitions of electronic surveillance on its face includes international communications, a point on which the pertinent legislative history concurs). If you believe today that it is important to analyze the historical record and the full legislative history in order to inform your decision on pending legislation, I strongly recommend that you ask entities such as the Congressional Research Service (CRS) to conduct a thorough review of all available materials and provide you with their conclusions.

In my view, the real questions regarding whether or not (or how) to modernize FISA ultimately are not technological in nature. Instead, the real questions are: (1) who should be the decision-maker (that is, who should approve foreign intelligence collection before it can begin); (2) what level of predication should be required (that is, how much paperwork and explanation is necessary to justify such collection and what standard of review should apply); and (3) how particular should the approvals be (that is, how specific must the authorizations be with respect to the persons or facilities at which the collection is directed). The lower the level of approval and factual predication needed, and the less specific the approvals are, the more quickly and more easily the Intelligence Community can start collection, and the great the volume of collection it can sustain over extended periods. That, I believe, is what is meant when one says we need to achieve greater speed and agility in foreign intelligence collection. All of this leads me to my next point.

Role of the Court in Intelligence Collection. As others have discussed, such as David Kris, co-author of the recently published National Security Investigations and Prosecutions, one of the key questions with respect to foreign intelligence collection that faces us today is when, and under what circumstances and conditions, should the government be allowed to conduct electronic surveillance (and search) for long periods of time without individualized findings of probable cause made in advance by judges. The Constitution does not mandate that judges play any role in foreign intelligence collection, so long as the collection activities are otherwise reasonable. But it seems to me that there is general consensus today that the FISA court should approve electronic surveillance and physical search in advance when those collection activities are targeted at people who are clearly located inside the United States. This includes surveillance of all domestic-to-domestic communications. Similarly, there appears to be consensus that the court should play no role in approving collection when the surveillance is targeted at people who are clearly located outside the United States, even when the collection itself takes place inside the United States. As I mentioned previously, foreign-to-foreign wire or radio communications traditionally have fallen outside the scope of FISA.

There appears to be less agreement in two other areas. The first is where one end of the communication is, or may be, in the United States, and the other end of the communication is outside the United States. This is sometimes referred to as "one end U.S. communications." The second is where you cannot tell in advance (if ever) where one or both of the parties to a communication are located. This is a particular issue with Internet communications, including web-based email, as well as mobile telephone technology.

Contrary to what some have said, the privacy interests of Americans may be implicated in these situations. When the government targets a foreign national who is abroad, the Fourth Amendment may be implicated if the electronic surveillance results in the interception of communications of a United States person. It may be implicated if the government acquires and listens to (or stores and later examines) a communication to which a United States person is a party, and it may be implicated if the government intercepts and scans the content of such a communication in order to determine whether it is to, from, or concerning a foreign national target who is located abroad.

Whenever the Fourth Amendment is implicated, the government's collection activities must be reasonable. The determination of whether particular collection activities are reasonable will likely depend on many factors, including: (1) as noted above, when and under what circumstances and conditions, the government is allowed to conduct electronic surveillance (and search) for long periods of time without individualized findings of probable cause made in advance by judges; and (2) the adequacy of any minimization procedures that are in place to limit the acquisition, retention, and dissemination of irrelevant information concerning United States persons.

Having worked closely with the FISA court for more than 10 years, I would be happy to provide the Committee with the benefit of my experience as it endeavors to determine the appropriate role for federal judges in approving and reviewing foreign intelligence collection in the two scenarios I have discussed.

Thank you.