Statement of David B. Rivkin, Jr.

Partner, Baker Hostetler LLP
Former Department of Justice and Office of the White House Counsel Official

Before the

House Permanent Select Committee on Intelligence

Foreign Intelligence Surveillance Act and NSA Activities

Tuesday, September 18, 2007

I would like to thank Chairman Reyes, Ranking Member Hoekstra, and other Committee Members for inviting me to testify at this hearing on the Foreign Intelligence Surveillance Act ("FISA") and the authorities for the National Security Agency's ("NSA") surveillance activities.

Before the August recess, Congress passed a six-month "fix" to FISA. FISA generally requires a judicial order before the Government can intercept "electronic communications" in the United States for foreign intelligence purposes. The fix was urgently needed because the "warrantless" component of the NSA's post-September 11 "terrorist surveillance program" – directed at al Qaeda global communications and brought under FISA earlier this year – had been dramatically narrowed by the special FISA court in a decision that impaired necessary intelligence collection efforts.

In response, Congress amended the law specifically to permit surveillance of international communications of overseas targets without a court order, even if the interception itself occurs in the United States. Unfortunately, vocal privacy advocates oppose this approach, largely because it may entail the incidental interception of communications by American citizens who, while not terrorist themselves, may nevertheless be in contact with al Qaeda operatives. The emotional issue of privacy seems likely to dominate the unfolding FISA debate. Unless properly addressed, the privacy concerns threaten to derail efforts to enact a permanent reformed FISA. Such an outcome would drastically reduce America's intelligence intake and

increase the risk that Jihadist forces may succeed in once again attacking the United States or our allies.

At one level, today's privacy concerns are rooted in lamentable ignorance about the past. Congress' recent action to exclude foreign communications where the target of the surveillance is overseas from FISA's "warrant" requirements simply returned the law to its original intent. When FISA was enacted in 1978, it did not regulate all, or even most, of the federal government's surveillance activities. Rather, Congress opted to deal with only a discrete portion of the government's intelligence gathering, focusing only on surveillance inside the United States or otherwise targeted at Americans. It made this choice largely because the Nixon Administration (and its predecessors) had justified a wide spectrum of domestic wiretapping on the basis of foreign intelligence needs. The U.S. targets of these activities often suffered real consequences, ranging from criminal prosecutions to other adverse governmental actions.

At the time of FISA's enactment, even the strongest congressional proponents of the statutory regulation of surveillance activities recognized that intelligence gathering was a key executive function and that the U.S. needed to collect as much foreign intelligence as possible. This bi-partisan consensus that FISA compliance could not be allowed to impede foreign intelligence collection was all the more notable, as it arose during a period of congressional activism directed at regulating Executive Branch activities and at a time when Cold War threats, while formidable, did not require a constant real time surveillance of a diverse array of non-state groups.

Consequently, the new law required the Executive Branch to obtain judicial orders where the actual surveillance target was physically present in the United States. For targets located overseas, court orders were not required before the President could authorize an overseas wiretap, or an intercept of their radio communications, whether collected overseas or in the United States. At the time, of course, most of this foreign intelligence collection was

accomplished by NSA satellites and "listening posts" located outside of the United States. These allowed NSA to intercept vast quantities of global communications without any warrants or, indeed, any kind of judicial involvement.

Today, primarily because of the revolution in communications technologies, the United States' excellent communications networks attract a large percentage of the world's message traffic. As a result, the same kinds of communications between non-U.S. persons overseas that were once intercepted overseas, now flow along fiber optic networks physically located in the United States. They nevertheless remain foreign communications between non-U.S. persons. These communications are thus properly subject to warrantless interception under FISA. By permitting the interception of these communications without a FISA court order, Congress has simply restored the original balance struck in 1978.

This history aside, the privacy-related arguments made by the Administration's critics are both vastly overblown and simplistic. They usually assume that the privacy interests of Americans and foreigners are equally worthy of protection, that all privacy impairments are equivalent, and that the mere possibility that somebody's conversation may be overheard without a warrant *per se* constitutes an unacceptable invasion of privacy. Even more problematic is the critics' manifest failure to emplace the FISA debate into the broader context of the ongoing debate in American society about how to balance privacy and public safety. For most Americans, indeed, privacy interests do not trump all other policy imperatives. The end result is an intellectually sterile discourse that does an injustice to all of the nuances and complexities of the privacy issue in modern America.

To begin with, despite all of the emotion surrounding the "innocent American bystander" scenario, far from being a unique and unacceptable consequence of a particular FISA regime, it is endemic to all surveillance. Warrants and other judicial surveillance orders result from a process that considers the particular target's rights. They are not designed particularly to protect the myriad of others who may come into contact with the target and, in the process, also

may have their communications intercepted. At least under FISA, and unlike the case with criminal justice-related surveillance, the Government follows "minimization" procedures – governing how the information is handled to prevent its inappropriate use, dissemination or disclosure – that protect the innocent bystander's privacy. The fact that senior U.S. government officials, unlike their counterparts in other countries, do not get access to the unredacted surveillance-generated information about American citizens and that the system is operated largely by career civil servants, provides additional layers of privacy protection.

Significantly, as explained by CIA Director Michael Hayden in 2006, elaborate minimization procedures are also employed as a matter of practice when foreign intelligence was intercepted, outside of FISA's framework, overseas: "if the U.S. person information isn't relevant [without foreign intelligence value], the data is suppressed." Indeed, it is precisely because warrantless surveillance is conducted in secrecy, with the utmost care being taken that the individuals involved never learn about it, that it is arguably the most privacy-protective. Meanwhile, the number of innocent bystanders, whose privacy has been impacted, will not be diminished if NSA has to seek warrants for all or most of its overseas targets. In either case, an innocent bystander would never know whether a warrant had been issued and hence, could not structure his conduct to minimize the chances of being caught up in the surveillance net.

Making all NSA surveillance warrant-driven is also not required as a matter of law. The Constitution's Fourth Amendment prohibits only unreasonable searches and seizures. Although today's privacy advocates routinely claim that a warrantless search is inherently unreasonable, this position is not supported by the Constitution or the case law. Over the years, the Supreme Court has approved numerous warrantless searches, balancing the government's interests against the relevant privacy expectations. Thus, drivers are subject to sobriety checkpoints and international travelers to search at the border because their reasonable privacy expectations in these situations are limited. Moreover, unlike the case with warrantless NSA surveillance, the fruits of these other warrantless searches are routinely used in civil and criminal prosecutions.

It is difficult to see why foreign nationals communicating abroad have any reasonable expectation of privacy vis-à-vis the United States Government simply because their conversations may be electronically transmitted through American switching stations. Similarly, when Americans make or receive international calls that may be incidentally intercepted because of overseas surveillance, they have a reduced expectation of privacy. Dozens of foreign intelligence services, some belonging to global powers such as Russia and China who have counter-terrorism concerns of their own and others working for regional powers, routinely intercept as many international communications as they can. The odds of interception by some intelligence service grows exponentially whenever an American communicates with people in countries, such as Pakistan, Iraq, Afghanistan, where significant terror-planning activities are known to occur. Meanwhile, some multinational companies also engage in industrial espionage, intercepting in the process at least some global communications. In short, the notion that privacy exists in today's globalized world is largely a myth.

The knowledge of these facts is readily available to even a casual newspaper reader, enabling Americans to structure their overseas communications in ways that satisfy the extent and intensity of their privacy concerns. Far from being uniform, privacy concerns vary among Americans. Even for the same person, their intensity depends upon many factors, including who intercepts their communications, whether they are confronted with this fact, and what other foreseeable consequences, if any, could ensue as a result of the intercept. Many Americans do not care much about solitude and routinely tell the pollsters that they are untroubled by the fact that the government may listen in on their calls. Others are more guarded in their expectations, and some treasure their privacy above all else.

In possession of all the facts about the all-too porous nature of overseas communications, an American who seeks to ensure that his private dealings remain private from all comers and who wants to talk to a person in a Pakistani village, would be well-advised to do so in person. By contrast, a less privacy-phobic innocent American bystander may be quite

happy telephoning Pakistan, either because he never knows for sure that his side of a conversation with an overseas target is being listened to, or at most, suspects that this might be the case, or just plain does not care. More fundamentally, irrespective of his precise privacy-related inclinations, because no adverse consequences will ensue if even a half-dozen intelligence services listen in, his privacy is compromised in a comparatively attenuated fashion.

However, expanding FISA's "warrant" requirements to the collection of all or virtually all foreign intelligence is certain to cripple the United States' intelligence gathering capacity. This would create a particularly acute problem in a protracted war against a shadowy and committed enemy, in which defectors are rare, the CIA's chances of penetrating al Qaeda's inner councils are slim to none, and aggressive interrogations of captured Jihadists have become increasingly unpopular. The widest and most proactive surveillance operations, targeted on every segment of the far-flung Jihadi network, have become the most vital aspects of U.S. intelligence gathering. They have proven their worth in stopping numerous terrorist attacks, with the German plot being the most recent example.

The United States' ability to continue with this strategy will be undermined if privacy protection becomes the overarching imperative of U.S. intelligence policy. Because the special FISA court is not a rubberstamp, it would be impossible to obtain orders against many foreign targets about which comparatively little may be known, including their true identities or the precise modalities of their involvement with Jihadist entities. And, of course, if the FISA court became a rubberstamp, obtaining its orders would not enhance privacy protection.

Those who want to subject all government surveillance activities to a warrant requirement should honestly acknowledge that this approach would dramatically shrink the stream of foreign intelligence. They must be prepared to justify their approach on that basis. Moreover, instead of waving the privacy banner in an undifferentiated fashion, the critics should explain what privacy interests of innocent American bystanders are actually threatened by a warrantless surveillance regime, in what way they are actually compromised, and how the

degree of hardship imposed compares with other privacy compromises that Americans have accepted in the recent past.

Unfortunately, the current debate over privacy and FISA reform has been both simplistic and dominated by political correctness. Thus, for example, none other than the Chairman and Vice Chairman of the 9/11 Commission, writing on the sixth anniversary of the 9/11 attacks, proclaimed that "we're not safe enough," yet lamented warrantless surveillance practices. It is possible to worry about the continuing shortfall in U.S. intelligence gathering and want it augmented; it is also possible to condemn all warrantless surveillance as a threat to U.S. civil liberties and want it banned. Holding both of these views simultaneously, however, is hard to justify.

Moreover, unlike many other war on terror-related policies, such as the handling of enemy combatants, which represent significant departures from peacetime norms of balancing liberty and order which have become deeply ingrained in American legal and political cultures, the FISA debate should be an easy one. Individual privacy is, of course, an important interest. It is not, however, the only important interest. Privacy must be balanced against society's legitimate need for security, whether arising in the war on terror context or in the context of protecting college students from harm caused by deranged shooters. Indeed, a rational society would certainly want to balance privacy and public safety in a consistent manner, across the entire range of threat scenarios. In this regard, it is significant that even domestic public safety problems, such as the recent and tragic shootings at Virginia Tech, routinely lead to proposals to liberalize the sharing of sensitive private information and do so without court involvement.

Restoring FISA to its 1978 scope, which did not prevent NSA from obtaining warrantlessly as much intelligence about overseas targets as possible, strikes an appropriate balance between privacy and safety. In a post-September 11 world, American society cannot afford to elevate privacy concerns beyond all other considerations. The notion that the balance struck between privacy and security in 1978 is somehow inherently inappropriate today and

needs to be recast with security taking the back seat is hard to credit, especially since the need to obtain more intelligence information, and to connect the dots, was one of the 9/11 Commission's most important conclusions.

To the extent that Congress is concerned with potential abuses and wants to bolster the political accountability of the program, it should require enhanced minimization procedures and additional intelligence oversight – perhaps by expanding the current "gang of eight" congressional leaders, who are regularly briefed on intelligence operations. It may also be worthwhile to have Congress review the entire range of possible consequences for an innocent American bystander whose conversations with an overseas target have been intercepted; so as to ensure that such people do not automatically find themselves, for example, on a no-fly list.

Expanding the reach of the FISA court, and limiting in the process the United States' ability to acquire foreign intelligence vital to the security of all Americans, is the wrong way to proceed. Instead, Congress should act to make the recent FISA fix permanent by enacting the Administration's sorely-needed FISA Modernization proposals. At the very least, Congress should make permanent the Protect America Act of 2007 and should immunize from lawsuits those business entities which cooperated with the Administration during the earlier phases of the NSA surveillance program.