OFFICE OF BOB BARR
Member of Congress, 1995-2003

TESTIMONY BY FORMER REP. BOB BARR BEFORE THE JUDICIARY COMMITTEE OF THE U.S. HOUSE OF REPRESENTATIVES CONCERNING OPPOSITION TO S. 1927, "THE PROTECT AMERICA ACT"

SEPTEMBER 5, 2007

OFFICE OF BOB BARR
Member of Congress, 1995-2003

TESTIMONY BY FORMER REP. BOB BARR BEFORE THE JUDICIARY COMMITTEE OF THE U.S. HOUSE OF REPRESENTATIVES CONCERNING OPPOSITION TO S. 1927, "THE PROTECT AMERICA ACT"

SEPTEMBER 5, 2007

Mr. Chairman, and Members of this distinguished Committee on the Judiciary of the U.S. House of Representatives, on which I was privileged to serve throughout my eight years as a Member of this body, it is an honor to appear today to speak to the vitally important topic at hand, "Warrantless Surveillance and the Foreign Intelligence Surveillance Act: The Role of Checks and Balances in Protecting Americans' Privacy Rights." The very title of this hearing is a tribute to your understanding – apparently lost on many in the administration – that electronic surveillance even in this post-911 world, is about much more than technology, and that consideration of the mechanisms and parameters of FISA cannot be considered in the sterile vacuum of technical amendments alone. Surveillance, whether for law-enforcement or foreign-intelligence purposes, does affect the fundamental privacy rights of American citizens, and this recognition must be the underpinning of any consideration of this inherently intrusive technique.

Thank you, Mr. Chairman, for inviting me here today to appear with this distinguished panel of Americans, to discuss this crucially important topic. I appear today as a private citizen, but also as a former Member of this Committee and as a once-again practicing attorney. I am also privileged to inform the Committee that I continue to serve as chairman of Patriots to Restore Checks and Balances, and as the holder of the 21st Century Liberties Chair for Freedom and Privacy at the American Conservative Union.

For several months leading to the passage and subsequent signing by the President of S. 1927, "The Protect America Act," on August 5, 2007 as

P.L. 110-55, the administration had been beating the PR drums clamoring for amendments to the Foreign Intelligence Surveillance Act (FISA), ostensibly in order to bring the 1978 law into accord with 21st Century technology. Then, shortly prior to its passage, the administration and its supporters in the Congress raised the decibel level of their arguments; claiming that a recent federal court decision finding that an electronic communication between two non-U.S. persons both outside the United States was nonetheless subject to the FISA warrant requirements because the communication was routed through the United States, made it absolutely urgent that the Congress "fix" FISA. The administration said it was crucial that such communications be monitored without being subject to the delays and uncertainties that the administration said would hamper its foreign intelligence-gathering efforts in light of the secret court decision.

The administration's gambit worked. A majority of members in both houses of the Congress, apparently receptive to the administration's dire warnings and its thinly-veiled warnings that failure to pass the remedial FISA legislation would likely result in a terrorist incident that -- for failure of the Congress to give the administration the tools it needed to gather electronic intelligence to help thwart such incidents – would be laid at the doorstep of the Congress.

Unfortunately, the legislation that passed in this atmosphere did not simply "fix" the problem identified by the administration – which arguably is meritorious – but went far, far beyond what could reasonably be deemed necessary to address a technological problem with the 1970s-era FISA law that manifested itself because of 21st-Century technology. Now, thanks to the poorly-considered "Protect America Act" the administration is able to order the surreptitious interception and surveillance of virtually any electronic communication (including phone calls and e-mails) from or to any person in the United States, so long as the government reasonably believes one of the parties is "located outside of the United States." Insofar as one party to a communication being outside the United States is the very definition of an "international communication," the universe of calls and e-mail transmissions subject now to warrantless monitoring by agencies of the federal government encompasses all such communications. This result is fully breathtaking in the practical scope of its reach, and in its potential damage to the very foundation of the Fourth Amendment to our Constitution.

Despite continued efforts by the Administration to characterize these changes as merely "technical" and only "corrective" of technological problems arising in and as a result of the "internet age" – problems compounded by the [still-secret] court decision – the changes wrought by "The Protect America Act" are neither "technical" nor "corrective." Especially those provisions found in Section 2 of the Act (which amends FISA by adding new Sections 105A and 105B), represent a profound alteration in the scope and reach of FISA, and a dramatic "brave new world" of electronic surveillance.

Essentially, thanks to this law, the government has potentially carved out from Fourth-Amendment protection an entire class of communication – electronic communications going to a person outside the United States, or coming to a person inside the United States. There is -- and here again contrary to the public missives by the Administration and its supporters -- no requirement whatsoever, implied or express, that even one of the parties to such category of communications subject to warrantless surveillance would first have to have any known or even suspect connection with any terrorist or other targeted group or activity.

As a result of the broad manner in which the Administration was able to effect this change to FISA – removing from the definition of "electronic surveillance" and therefore from the entire reach and mechanism of FISA entirely, any communication of a person "reasonably believed to be located outside of the United States" – it has effectively neutered any oversight role the Congress or the Foreign Intelligence Surveillance Court (FISC) might play in overseeing or limiting the government's surveillance. The only oversight role either the Congress or the FISC would be able to exert would be superficial at best.

Even a Reagan-appointed federal judge, who has served with distinction on the FISC – the Honorable Royce Lamberth – understands the gravamen of the danger posed by unfettered electronic surveillance in the name of "fighting the war on terrorism":

> "We have to understand you can fight the war [on terrorism] and lose everything if you have no civil liberties left when you get through fighting the war…[b]ut what we have found in the history of our country is that you can't trust the executive…[w]e still have to preserve our civil liberties. Judges are the kinds of people you want to entrust that kind of judgment to more than

the executive," U.S. District Court Judge Royce Lamberth, June 23, 2007.

Judge Lamberth's relevant and timely admonition follows the prescient warning by the well-known jurist, Justice Louis Brandeis, who, in the 1928 *Olmstead* decision issued this ominous warning:

> "Subtler and more far-reaching means of invading privacy have become available to the government… Ways may someday be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home… It is not the breaking of his doors, and the rummaging of his drawers that constitutes the essence of the offense; but it is the invasion of his indefeasible right of personal security, personal liberty, and private property."

These jurists are hardly alone in sounding the alarm against unfettered government invasion of citizens' privacy through the use of electronic surveillance powers and equipment, regardless of whether done in the name of fighting organized crime, communist infiltrators, or terrorists. I am gratified this Committee, or at least you, Mr. Chairman, and some of your colleagues, have heard this call and heeded the warnings of these wise jurists and many others in government, academia and the private sector who understand the bedrock principles embodied in our Constitution and its Bill of Rights and who understand also that no threat, no matter how serious, should ever provide the excuse for decimating the carefully constructed set of checks and balances woven into the fabric of our system of government.

I know this Committee understands as do few citizens that the quest – legitimate as it is – for actionable foreign intelligence, should never be allowed to serve as a subterfuge for circumventing the requirements of the Fourth Amendment, which functions in essence as the fundamental privacy right for each and every citizen of this great land. This understanding was the basis for creation of the FISA mechanism in the first instance; yet with the stroke of the presidential pen in signing P.L. 110-55, that rationale and that principle has been swept aside. What is left is a structure with no foundation. The sole limitation on which communications involving American citizens the government could

surreptitiously monitor without any intervention of the courts, is that the government "reasonably believe[s]" at least one of the parties to be "located outside of the United States." That's it; that's all; end of argument.

The silver lining in this dark cloud of unfettered and unsupervised surveillance of virtually all or any international electronic communications, is the fact that the leadership of this 110th Congress granted the administration only a six-month expansion of FISA. All freedom-loving Americans should applaud the Congress for having taken this step and at least provided a hedge against perpetual government warrantless surveillance. In addition to repealing the changes to FISA resulting from Section 2 of P.L. 110-55, and reining in the unnecessary and constitutionally-destructive expansion of FISA, the Congress should take the opportunity provided by this six-month sunset period, to address in a narrow and focused manner the specific change sought by the administration. This could include addressing the anomaly of requiring a court order to intercept a communication between two persons both outside the United States if the communication is simply routed through our country. The administration should not be permitted to take a mile when they ask for – and are entitled to only – an inch.

Additionally, the Congress should avail itself of this opportunity, and of your leadership, Mr. Chairman, to replace the fig-leaf court and congressional oversight provided for in P.L. 110-55, with meaningful oversight such as contained in the original FISA; a mechanism, I might add, that, despite cries to the contrary by the administration, has worked well and expeditiously these many years. If in fact the administration can point to a specific area in which the judicial or congressional oversight needs to be tweaked to strengthen or streamline it – consistent with and not adverse to the original intent of both FISA and the Fourth Amendment – then I would respectfully recommend this Committee afford the administration a willing but skeptical ear, force it to justify the changes sought, and then provide only the clearest and most narrow remedy to address the problem.

In closing, Mr. Chairman, let me refer back to April 12, 2000, on which date I testified on FISA before your sister committee, the Permanent Select Committee on Intelligence. That same day, before that same committee, on that same subject, Gen. Michael Hayden, in his then-

capacity as Director of the National Security Agency (NSA), testified. He correctly noted that before the NSA could lawfully initiate any surreptitious collection of intelligence by electronic surveillance on any American in the United States, the government first "must have a court order." Until the President signed P.L. 110-55 last month, this remained the law.

General Hayden had it right then, and this committee has it right now in insisting that the privacy rights of American continue to be thus protected; and that necessary exceptions to the general principle that when an American citizen picks up a phone or types an e-mail into their Blackberry to someone or some entity that happens to be outside the geographic boundaries of the United States, he or she can rest assured their communication will *not* be intercepted absent a good, sufficient and constitutionally-based reason. In this expectation, we are all children of of our Founding Fathers. I thank this Committee for working to reestablish this foundational principle by reining in the power shift from citizen to government represented by "The Protect America Act."