



**Remarks of U.S. Senator Russ Feingold
Opposing H.R. 6304, FISA Amendments Act of 2008**

[Download](#) this video

June 25, 2008

Mr. President, I strongly oppose H.R. 6304, the FISA Amendments Act of 2008.

This legislation has been billed as a compromise between Republicans and Democrats. We are asked to support it because it is a supposedly reasonable accommodation of opposing views. Let me respond as clearly as possible: This bill is not a compromise. It is a capitulation.

This bill will effectively and unjustifiably grant immunity to companies that allegedly participated in an illegal wiretapping program – a program that more than 70 members of this body still know virtually nothing about. And this bill will grant the Bush Administration – the same administration that developed and operated this illegal program for more than five years – expansive new authorities to spy on Americans' international communications.

If you don't believe me, here is what Senator Bond had to say about the bill: "I think the White House got a better deal than even they had hoped to get." And House Minority Whip Roy Blunt said this: "The lawsuits will be dismissed."

There is simply no question that Democrats who had previously stood strong against immunity and in support of civil liberties were on the losing end of this backroom deal.

Mr. President, the railroading of Congress began last summer, when the Administration rammed through the so-called "Protect America Act," or PAA, vastly expanding the government's ability to eavesdrop without a court-approved warrant. That legislation was rushed through this chamber in a climate of fear – fear of terrorist attacks, and fear of not appearing sufficiently strong on national security. There was very little understanding of what the legislation actually did.

But the silver lining was that the law had a six-month sunset. So Congress quickly started working to fix the legislation. The House passed a bill last fall, and the Senate passed its bill – one that I believe was deeply flawed – in February. As the PAA's six-month sunset approached in late February, the House faced enormous political pressure simply to pass the Senate bill before the sunset date. But the reality was that no orders under the PAA were going to expire in February, and the

House stood firm in its resolve not to pass the Senate bill with its unjustified immunity provision. The House deserved great credit for not buckling in the face of the President's attempts to intimidate them. Ultimately the House passed new legislation in March, setting up the negotiations that have led us here today.

I think it's safe to say that even many who voted for the Protect America Act last year came to believe it was a mistake to pass that legislation. And while the House deserves credit for refusing to pass the Senate bill in February, and for securing the changes that are in this new bill, this bill is also a serious mistake.

Mr. President, the immunity provision is a key reason for that. It is a key reason for my opposition to this legislation and for that of so many of my colleagues and so many Americans. No one should be fooled about the effect of this bill. Under its terms, the companies that allegedly participated in the illegal wiretapping program will walk away from these lawsuits with immunity. There is simply no question about it, and anyone who says that this bill preserves a meaningful role for the courts to play in deciding these cases is wrong.

But I'm concerned that the focus on immunity has diverted attention away from the other very important issues at stake in this legislation. In the long run, I don't believe this will be remembered as the 'immunity' bill. This legislation is going to be remembered as the legislation in which Congress granted the executive branch the power to sweep up all of our international communications with very few controls or oversight.

Mr. President, I'm talking about Title I of the bill, the title that makes substantive changes to the FISA statute. I'd like to explain why I am so concerned about the new surveillance powers granted in this part of the bill, and why the modest improvements made to this part of the bill don't go far enough.

This part of the bill has been sold to us as necessary to ensure that the government can collect communications between persons overseas without a warrant, and to ensure that the government can collect the communications of terrorists, including their communications with people in the United States. No one disagrees that the government should have this authority. But this bill goes much further, authorizing widespread surveillance involving innocent Americans – at home and abroad.

First, the FISA Amendments Act, like the Protect America Act, would authorize the government to collect all communications between the U.S. and the rest of the world. That could mean millions upon millions of communications between innocent Americans and their friends, families, or business associates overseas could legally be collected. Parents calling their kids studying abroad, emails to friends serving in Iraq – all of these communications could be collected, with absolutely no suspicion of any wrongdoing, under this legislation. In fact, the DNI even testified that this type of 'bulk collection' would be 'desirable.'

The bill's supporters like to say that the government needs additional powers to target terrorists overseas. But under this bill, the government is not limited to targeting foreigners outside the U.S. who are terrorists, or who are suspected of some wrongdoing, or who are members or agents of some foreign government or organization. In fact, the government does not even need a specific purpose for wiretapping anyone overseas. All it needs to have is a general "foreign intelligence" purpose, which is a standard so broad that it covers all international communications. That's not just my opinion -- the DNI has testified that, under the PAA, and presumably this bill, the government could legally collect all communications between the United States and overseas. Let me repeat that: under this bill, the government can legally collect all communications – every last one – between Americans here at home and the rest of the world.

Mr. President, I should note that one of the few bright spots in this bill is the inclusion of a provision from the Senate bill to prohibit the intentional targeting of an American overseas without a warrant. That is an important new protection. But that amendment does not prevent the indiscriminate vacuuming up of all international communications, which would allow the government to collect the communications of

Americans overseas, including with friends and family back home, without a warrant.

I tried to address this issue of “bulk collection” when the bill was on the floor in February by offering an amendment that would have required that there be some foreign intelligence purpose for the collection of communications to or from particular targets. The vast majority of Democrats supported this effort, but unfortunately it was defeated. And the bill we are considering today does not address this problem.

Second, like the earlier Senate version, this bill fails to effectively prohibit the practice of reverse targeting – namely, wiretapping a person overseas when what the government is really interested in is listening to an American here at home with whom the foreigner is communicating. The bill does have a provision that purports to address this issue. The bill prohibits intentionally targeting a person outside the U.S. without an individualized court order if, quote, “the purpose” is to target someone reasonably believed to be in the U.S. But this language would permit intentional and possibly unconstitutional warrantless surveillance of an American so long as the government has any interest in the person overseas with whom the American is communicating. And, if there was any doubt, the DNI has publicly said that the Senate bill – which contained identical language as the current bill – merely “codifies” the administration’s position, which is that the government can wiretap a person overseas indefinitely without a warrant, no matter how interested it may really be in the American with whom that person overseas is communicating.

Supporters of this bill also will argue that it requires the executive branch to establish guidelines for implementing this new reverse targeting requirement. But the guidelines are not subject to judicial review. And requiring guidelines to implement an ineffective limitation is not a particularly comforting safeguard.

When the Senate considered the FISA bill earlier this year, I offered an amendment – one that had been approved by the Senate Judiciary Committee – to make the prohibition on reverse targeting meaningful. My amendment, which again had the support of the vast majority of the Democratic caucus and was included in the bill passed by the House in March, would have required the government to obtain a court order whenever a significant purpose of the surveillance is to acquire the communications of an American in the U.S. This would have done a far better job of protecting the privacy of the international communications of innocent Americans. Unfortunately, it is not in this bill.

Third, the bill before us imposes no meaningful consequences if the government initiates surveillance using procedures that have not been approved by the FISA Court, and the FISA Court later finds that those procedures were unlawful. Say for example, that the FISA Court determines that the procedures were not even reasonably designed to wiretap foreigners rather than Americans. Under the bill, all that illegally obtained information on Americans can be retained and used. Once again, there are no consequences for illegal behavior.

Now, unlike the Senate bill, this new bill does generally provide for FISA Court review of surveillance procedures before surveillance begins. But it also says that if the Attorney General and Director of National Intelligence certify that they don’t have time to get a court order and that intelligence important to national security may be lost or not timely acquired, then they can go forward without judicial approval. This is a far cry from allowing an exception to FISA Court review in a true emergency because arguably all intelligence is important to national security and any delay at all might cause some intelligence to be lost. So I am concerned that this ‘exigency’ exception could very well swallow the rule and undermine any presumption of prior judicial approval.

But whether the exception is applied broadly or narrowly, if the government invokes it and ultimately engages in illegal surveillance, the court should be given some flexibility after the fact to determine whether the government should be allowed to keep the results of that illegal surveillance if it involves Americans. That is what another one of my amendments on the Senate floor would have done, an amendment that garnered 40 votes, yet this issue goes unaddressed in the so-called compromise.

Fourth, this bill doesn't protect the privacy of Americans whose communications will be collected in vast new quantities. The Administration's mantra has been: "don't worry, we have minimization procedures." Mr. President, minimization procedures are nothing more than unchecked executive branch decisions about what information on Americans constitutes "foreign intelligence." As recently declassified documents have again confirmed, the ability of government officials to find out the identity of Americans and use that information is extremely broad. Moreover, even if the Administration were correct that minimization procedures have worked in the past, they are certainly inadequate as a check against the vast amounts of Americans' private information that could be collected under this bill. That is why on the Senate floor, I joined with Senator Webb and Senator Tester to offer an amendment to provide real protections for the privacy of Americans, while also giving the government the flexibility it needs to wiretap terrorists overseas. But this bill, like the Senate bill, relies solely on these inadequate minimization procedures.

Mr. President, the broad surveillance powers involving international communications that are contained in this legislation are particularly troubling because we live in a world in which international communications are increasingly commonplace. Thirty years ago it was very expensive, and not very common, for most Americans to make an overseas call. Now, particularly with email, such communications happen all the time. Millions of ordinary, and innocent, Americans communicate with people overseas for entirely legitimate personal and business reasons. Parents or children call family members overseas. Students email friends they have met while studying abroad. Business people communicate with colleagues or clients overseas. Technological advancements combined with the ever more interconnected world economy have led to an explosion of international contacts.

Supporters of the bill like to say that we just have to bring FISA up to date with new technology. But changes in technology should also cause us to take a close look at the need for greater protections of the privacy of our citizens. If we are going to give the government broad new powers that will lead to the collection of much more information on innocent Americans, we have a duty to protect their privacy as much as we possibly can. And we can do that without sacrificing our ability to collect information that will help protect our national security. This supposed compromise, unfortunately, fails that test.

Mr. President, I don't mean to suggest that this bill does not contain some improvements over the bill that the Senate passed early this year. Clearly it does, and I appreciate that. Certainly, it is a good thing that this bill includes language making clear, once and for all, that Congress considers FISA and the criminal wiretap laws to be the exclusive means by which electronic surveillance can be conducted in this country – a provision that Senator Feinstein fought so hard for. And it is a good thing that Congress is directing the relevant Inspectors General to do a comprehensive report on the President's illegal wiretapping program – a report whose contents I hope will be made public to the greatest degree possible. And it is a good thing that the bill no longer redefines the critical FISA term "electronic surveillance," which could have led to a great deal of confusion and unintended consequences.

All of those provisions are positive developments, and I am glad that the ultimate product seemingly destined to become law contains these improvements.

But I can't pretend that these improvements are enough. They are nowhere close. When I offered my amendments on the Senate floor in February, the vast majority of the Democratic caucus supported me. While I did not have the votes to pass those amendments, I am confident that more and more members of Congress will agree that changes to this legislation need to be made. If we can't make them this year, then Congress must return to this issue – and it must do so as soon as a new President takes office. These issues are far too important to wait until the sunset date, especially now that it is set in this bill for 2012, another presidential election year.

But Mr. President, let me now turn to the grant of retroactive immunity that is contained in this bill because on that issue there is no question that any differences

between this bill and the Senate bill are only cosmetic. Make no mistake: This bill will result in immunity.

Under the terms of this bill, a federal district court would evaluate whether there is substantial evidence that a company received “a written request or directive ... from the Attorney General or the head of an element of the intelligence community ... indicating that the activity was authorized by the President and determined to be lawful.”

But, Mr. President, we already know from Senate Select Committee on Intelligence’s committee report last fall that the companies received exactly these materials. That is already public information. So under the terms of this proposal, the court’s evaluation would essentially be predetermined.

Regardless of how much information the court is permitted to review, what standard of review is employed, how open the proceedings are, and what role the plaintiffs are permitted to play, the court will essentially be required to grant immunity under this bill.

Now, proponents will argue that the plaintiffs in the lawsuits against the companies can participate in briefing to the court. This is true, but they are allowed to participate only to the extent it does not necessitate the disclosure of classified information. Mr. President, the administration has restricted information about this illegal program so much that more than 70 members of this chamber don’t even have access to the basic facts about what happened. So let’s not pretend that the plaintiffs will be able to participate in any meaningful way. And even if they could participate fully, immunity is a foregone conclusion under the bill.

This result is extremely disappointing on many levels, perhaps most of all because granting retroactive immunity is entirely unnecessary and unjustified. Doing this will profoundly undermine the rule of law in this country.

For starters, current law already provides immunity from lawsuits for companies that cooperate with the government’s request for assistance, as long as they receive either a court order or a certification from the Attorney General that no court order is needed and the request meets all statutory requirements. But if requests are not properly documented, FISA instructs the telephone companies to refuse the government’s request, and subjects them to liability if they instead decide to cooperate. This framework, which has been in place for 30 years, protects companies that act at the request of the government while also protecting the privacy of Americans’ communications.

Some supporters of retroactively expanding this already existing immunity provision argue that the telephone companies should not be penalized if they relied on a high-level government assurance that the requested assistance was lawful. Mr. President, as superficially appealing as that argument may sound, it utterly ignores the history of FISA.

Telephone companies have a long history of receiving requests for assistance from the government. That’s because telephone companies have access to a wealth of private information about Americans – information that can be a very useful tool for law enforcement. But that very same access to private communications means that telephone companies are in a unique position of responsibility and public trust. And yet, before FISA, there were basically no rules to help the phone companies resolve the tension between the government’s requests for assistance in foreign intelligence investigations and the companies’ responsibilities to their customers.

This legal vacuum resulted in serious governmental abuse and overreaching. The abuses that took place are well documented and quite shocking. With the willing cooperation of the telephone companies, the FBI conducted surveillance of peaceful anti-war protesters, journalists, steel company executives – and even Martin Luther King Jr.

Congress decided to take action. Based on the history of, and potential for, government abuses, Congress decided that it was not appropriate for telephone

companies to simply assume that any government request for assistance to conduct electronic surveillance was legal. Let me repeat that: a primary purpose of FISA was to make clear, once and for all, that the telephone companies should not blindly cooperate with government requests for assistance.

At the same time, however, Congress did not want to saddle telephone companies with the responsibility of determining whether the government's request for assistance was a lawful one. That approach would leave the companies in a permanent state of legal uncertainty about their obligations.

So Congress devised a system that would take the guesswork out of it completely. Under that system, which was in place in 2001, and is still in place today, the companies' legal obligations and liability depend entirely on whether the government has presented the company with a court order or a certification stating that certain basic requirements have been met. If the proper documentation is submitted, the company must cooperate with the request and will be immune from liability. If the proper documentation has not been submitted, the company must refuse the government's request, or be subject to possible liability in the courts.

The telephone companies and the government have been operating under this simple framework for 30 years. The companies have experienced, highly trained, and highly compensated lawyers who know this law inside and out.

In view of this history, it is inconceivable that any telephone companies that allegedly cooperated with the administration's warrantless wiretapping program did not know what their obligations were. And it is just as implausible that those companies believed they were entitled to simply assume the lawfulness of a government request for assistance. This whole effort to obtain retroactive immunity is based on an assumption that doesn't hold water.

That brings me to another issue, Mr. President. I've been discussing why retroactive immunity is unnecessary and unjustified, but it goes beyond that. Granting companies that allegedly cooperated with an illegal program this new form of automatic, retroactive immunity undermines the law that has been on the books for decades – a law that was designed to prevent exactly the type of actions that allegedly occurred here.

Remember, telephone companies already have absolute immunity if they complied with the applicable law. And they have an affirmative defense if they believed in good faith that they were complying with that law. So the retroactive immunity provision we're debating here is necessary only if we want to extend immunity to companies that did not comply with the applicable law and did not even have a good faith belief that they were complying with it. So much for the rule of law.

Even worse, granting retroactive immunity under these circumstances will undermine any new laws that we pass regarding government surveillance. If we want companies to follow the law in the future, it sends a terrible message, and sets a terrible precedent, to give them a "get out of jail free" card for allegedly ignoring the law in the past.

I find it particularly troubling when some of my colleagues argue that we should grant immunity in order to encourage the telephone companies to cooperate with the government in the future. They want Americans to think that not granting immunity will damage our national security. But if you take a close look at the argument, it doesn't hold up. The telephone companies are already legally obligated to cooperate with a court order, and as I've mentioned, they already have absolute immunity for cooperating with requests that are properly certified. So the only thing we'd be encouraging by granting immunity here is cooperation with requests that violate the law. Mr. President, that's exactly the kind of cooperation that FISA was supposed to prevent.

And let's remember why. These companies have access to our most private conversations, and Americans depend on them to respect and defend the privacy of these communications unless there is clear legal authority for sharing them. They depend on us to make sure the companies are held accountable for betrayals of

that public trust. Instead, this immunity provision would invite the telephone companies to betray that trust by encouraging cooperation with illegal government programs.

But Mr. President, this immunity provision doesn't just allow telephone companies off the hook for breaking the law. It also will make it that much harder to get to the core issue that I've been raising since December 2005, which is that the President ran an illegal program and should be held accountable. When these lawsuits are dismissed, we will be that much further away from an independent judicial review of this program.

Mr. President, since 9-11, I've heard it said many times that what separates us from our enemies is respect for the rule of law. Unfortunately, the rule of law has taken it on the chin from this administration. Over and over, the President and his advisers have claimed the right to ignore the will of Congress and the laws on the books if and when they see fit. And now they are claiming the same right for any entity that assists them in that effort, no matter how unreasonable that assistance might have been.

On top of all this, we are considering granting immunity when more than 70 members of the Senate still – still – have not been briefed on the President's wiretapping program. The majority of this body still does not even know what we are being asked to grant immunity for.

In sum, Mr. President, I cannot support this legislation. I appreciate that changes were made to the Senate bill, but they are not enough. Nowhere near enough.

And Mr. President, we have other alternatives. We have options. We do not have to pass this law in the midst of a presidential election year, while George Bush remains President, in the worst possible political climate for constructive legislating in this area. If the concern is that orders issued under the PAA could expire as early as August, we could extend the PAA for another six months, nine months, even a year. We could put a one-year sunset on this bill, rather than having it sunset in the next presidential election year when partisan politics will once again be at their worst. Or we could extend the effect of any current PAA orders for six months or a year. All of these options would address any immediate national security concerns.

What we do not have to do, Mr. President, and what we should not do, is pass a law that will immunize illegal behavior and fundamentally alter our surveillance laws for years to come.

I have spent a great deal of time over the past year – in the Senate Intelligence Committee, in the Senate Judiciary Committee, and on the Senate floor – discussing my concerns, offering amendments, and debating the possible effects of the fine print of various bills. But this isn't simply about fine print. In the end, my opposition to this bill comes down to this: This bill is a tragic retreat from the principles that have governed government conduct in this sensitive area for 30 years. It needlessly sacrifices the protection of the privacy of innocent Americans. And it is an abdication of this body's duty to stand up for the rule of law. I will vote No.

I yield the floor.

###