meddling in this area at all. However, unlike the Specter bill, these two amendments were offered to replace the broad grant of retroactive immunity in the FISA bill, and they were offered after the Senate had voted not to adopt the Dodd-Feingold amendment. Each of them was an improvement, however slight, to the underlying immunity provision, in that they would have left open the possibility that the lawsuits could continue, thus permitting the courts to rule on the legality of the warrantless wiretapping program. Therefore, I voted in favor of both of these amendments, even though I would have much preferred to see retroactive immunity stricken entirely.

The PRESIDING OFFICER. By unanimous consent, the mandatory quorum call has been waived.

The question is, Is it the sense of the Senate that debate on S. 2248, an original bill to amend the Foreign Intelligence Surveillance Act of 1978, to modernize and streamline the provisions of that act, and for other purposes, shall be brought to a close.

The yeas and nays are required under the rule.

The clerk will call the roll.

The bill clerk called the roll.

Mr. DURBIN. I announce that the Senator from New York (Mrs. CLINTON) is necessarily absent.

Mr. KYL. The following Senator is necessarily absent: the Senator from South Carolina (Mr. GRAHAM).

Further, if present and voting, the Senator from South Carolina (Mr. GRAHAM) would have voted ''yea.''

The PRESIDING OFFICER. Are there any other Senators in the Chamber desiring to vote?

The yeas and nays resulted—yeas 69, nays 29, as follows:

[Rollcall Vote No. 19 Leg.]

YEAS—69

Alexander	Dole	McConnell
Allard	Domenici	Mikulski
Barrasso	Ensign	Murkowski
Baucus	Enzi	Nelson (FL)
Bayh	Feinstein	Nelson (NE)
Bennett	Grassley	Pryor
Bond	Gregg	Roberts
Brownback	Hagel	Rockefeller
Bunning	Hatch	Salazar
Burr	Hutchison	Sessions
Carper	Inhofe	Shelby
Casey	Inouye	Smith
Chambliss	Isakson	Snowe
Coburn	Johnson	Specter
Cochran	Kohl	Stevens
Coleman	Kyl	Sununu
Collins	Landrieu	Thune
Conrad	Lieberman	Vitter
Corker	Lincoln	Voinovich
Cornyn	Lugar	Warner
Craig	Martinez	Webb
Crapo	McCain	Whitehouse
DeMint	McCaskill	Wicker

NAYS—29

Akaka	Durbin	Murray
Biden	Feingold	Obama
Bingaman	Harkin	Reed
Boxer	Kennedy	Reid
Brown	Kerry	Sanders
Byrd	Klobuchar	Schumer
Cantwell	Lautenberg	Stabenow
Cardin	Leahy	Tester
Dodd	Levin	Wyden
Dorgan	Menendez	

NOT VOTING—2

Clinton Graham

The PRESIDING OFFICER. On this vote, the yeas are 69, the nays are 29. Three-fifths of the Senators duly chosen and sworn having voted in the affirmative, the motion is agreed to.

RECESS

The PRESIDING OFFICER. Under the previous order, the Senate stands in recess until 2:15 p.m.

Thereupon, the Senate, at 12:34 p.m., recessed until 2:15 p.m. and reassembled when called to order by the Presiding Officer (Mr. CARPER).

FISA AMENDMENTS ACT OF 2007

The PRESIDING OFFICER. The Senator from California is recognized.

Mrs. BOXER. Mr. President, I ask unanimous consent that immediately following Senator FEINGOLD's 15 minutes on FISA, I be recognized for 10 minutes and that the time be taken from Senator DODD's 4 hours.

The PRESIDING OFFICER. Is there objection?

Without objection, it is so ordered.

The Senator from Wisconsin is recognized.

Mr. FEINGOLD. Mr. President, I strongly oppose S. 2248. This bill is deeply flawed in ways that will have a direct impact on the privacy of Americans. Along with several other Members of this body, I have offered modest amendments that would have permitted the government to obtain the intelligence it needs, while providing the checks and balances required to safeguard our constitutional rights. Unfortunately, under intense administration pressure marked by inaccurate and misleading scare tactics, the Senate has buckled. And we are left with a very dangerous piece of legislation.

The railroading of Congress began last summer, when the administration rammed through the so-called Protect America Act, 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 there was one silver lining: The bill had a 6-month sunset to force Congress to do its homework and reconsider the approach it took. Unfortunately, with far too few exceptions, the damage has not been undone.

This new bill was intended 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.

Proponents of the bill and the administration don't want to talk about what this bill actually authorizes. Instead, they repeatedly and inaccurately assert that efforts to provide checks and balances will impede the government's surveillance of terrorists. They launched these attacks against the more balanced bill that came out of the Judiciary Committee. And they have attacked and mischaracterized amendments offered on the floor of this body. This is fear-mongering, it is wrong, and it has obscured what is really going on.

What does this bill actually authorize? First, it permits the government to come up with its own procedures for determining who is a target of surveillance. It doesn't need advance approval from the FISA Court to ensure that the government's targets are actually foreigners, and not Americans here in the United States. And, if the Court subsequently determines that the government's procedures are not even reasonably designed to wiretap foreigners, rather than Americans, there are no meaningful consequences. All that illegally obtained information on Americans can be retained and used.

Second, even if the government is targeting foreigners outside the U.S., those foreigners need not be terrorists. They need not be suspected of any wrongdoing. They need not even be a member or agent of some foreign power. In fact, the government can just collect international communications indiscriminately, so long as there is a general foreign intelligence purpose, a meaningless qualification that the DNI has testified permits the collection of all communications between the United States and overseas. Under this bill, the government can legally collect all communications—every last one—between Americans here at home and the rest of the world. Even the sponsor of this bill, the chairman of the Intelligence Committee, acknowledges that this kind of bulk collection is probably unconstitutional, but the DNI has said it would be not only authorized but ''desirable'' if technically possible. Technology changes fast in this area. We have been forewarned, yet the Senate failed to act.

One of the few bright spots in this bill is the inclusion of an amendment, offered by Senators WYDEN, WHITEHOUSE and myself in the Intelligence Committee, to prohibit the intentional targeting of an American overseas without a warrant. That is an important new protection. But that amendment does not rule out 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. And those communications can be retained and used. Even the administration's illegal warrantless wiretapping program,

as described when it was publicly confirmed in 2005, at least focused on the communications of particular terrorists. What we are talking about now is potentially a huge dragnet that could sweep up the communications of countless innocent Americans.

Third, the Senate failed to prohibit the practice of reverse targeting; namely, wiretapping a person overseas when what the government is really interested in is an American here at home with whom the foreigner is communicating. The underlying bill simply does not stop this practice and, if there was any doubt, the DNI has publicly said that the bill merely ''codifies'' the administration's view that surveillance of an American is fine, so long as the government is technically wiretapping the foreigner. Even the DNI has said this is unconstitutional, but there is nothing in this bill to stop it.

Fourth, the Senate has failed to 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.'' 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 these new authorities.

This legislation is 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 are commonplace. 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.

We often hear from those who want to give the government new powers 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.

But, the Senate has once again fallen for administration tactics that have become so depressingly familiar. ''Trust us,'' they say. ''We don't need judicial oversight. The courts will just get in our way. You never know when they might tell us that what we're doing is unconstitutional, and we would prefer to make that decision on our own. Checks and balances, judicial and congressional oversight, will impede our ability to fight terrorism.'' And, sadly, these grossly misleading efforts at intimidation have apparently worked.

I have been speaking for some time now about my strong opposition to this bill, and I haven't even addressed one of the most outrageous elements of that bill: the granting of retroactive immunity to companies that allegedly participated in an illegal wiretapping program that lasted for more than 5 years.

This grant of automatic immunity is simply unjustified. There is already an immunity provision in current law that has been there since FISA was negotiated—with the participation of the telecommunications industry—in the late 1970s. The law is clear. Companies have immunity from civil liability when they cooperate with a Government request for assistance—as long as they receive a court order, or the Attorney General certifies that a court order is not required and all statutory requirements have been met.

This is not about whether companies had good intentions. It is about whether they complied with this statutory immunity provision, which has applied to them for 30 years. If the companies followed that law, they should get immunity. If they did not follow that law, they should not get immunity. And a court should make that decision, not Congress. It is that simple.

Congress passed a law laying out when telecom companies get immunity and when they don't for a reason. These companies have access to our most private communications, so Congress has subjected them to very precise rules about when they can provide that information to the government. If the companies did not follow the law Congress passed, they should not be granted a ''get out of jail free'' card after the fact.

Proponents of retroactive immunity have said repeatedly that immunity is necessary if the government is going to have the cooperation of carriers in the future. We do need that cooperation. But we also need to make sure that carriers don't cooperate with illegitimate requests. We already have a law that tells companies when they should and when they shouldn't cooperate, so they are not placed in the position of having to evaluate independently whether the government's request for help is legitimate.

Instead of allowing the courts to apply that law to the facts—instead of allowing judges to decide whether the companies deserve immunity for acting appropriately—this bill sends the message that companies need not worry about complying with questionable government requests in the future because they will be bailed out after the fact.

This is outrageous. Even more outrageous is that fact that if these lawsuits are dismissed, the courts may never rule on the NSA wiretapping program. This is an ideal outcome for an administration that believes it should be able to interpret laws alone, without worrying about how Congress wrote them or what a judge thinks. For those of us who believe in three independent and co-equal branches of government, it is a disaster.

In the 1970s, Congress learned that the executive branch had been using its immense powers and the advance of technology to spy on its citizens. By passing FISA, Congress faced up to the fact that we can't just trust the executive branch, including the President of the United States, to do the right thing, that judicial oversight of the power to spy was needed, that checks and balances are the best way to ensure liberty, and security.

I have spent a great deal of time on the floor over the past several weeks discussing the details of the bill, offering amendments, and debating the possible effects of the fine print of the statute. 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 court oversight and protection of the privacy of innocent Americans. It is an abdication of this body's duty to stand up for the rule of law.

We know what is wrong with this legislation. We know that it authorizes unconstitutional surveillance of Americans. We have been forewarned. I urge my colleagues to vote ''no'' on final passage.

The PRESIDING OFFICER. The Senator from California is recognized.

Mrs. BOXER. Mr. President, I rise to speak about the FISA bill currently being considered by the Senate. I believe it is our duty to provide all the tools necessary to fight terrorism. We also have another duty—I would say a simultaneous duty, a sworn duty—to protect the constitutional rights of our citizens.

So we have two duties. One is to protect the American people and give the Government the tools it needs to do that; two, to protect the constitutional rights of Americans. If we lose those rights, then the basic freedoms of our people are at risk.

I believe we have fallen far short. We have fallen far short of the balance that we always need to look for, ever since the beginning of our Republic—

the balance between security and freedom. I think we missed it here.

It is not the Government's job to scare our people; it is the Government's job to protect our people. It is not the Government's job to endanger the privacy of law-abiding Americans, but to protect the privacy of law-abiding Americans. Sadly, we had a number of amendments to this bill which would have brought that balance I talked about into being, the balance between security and freedom.

Senator FEINGOLD had an amendment limiting the use and dissemination of information unlawfully obtained through foreign surveillance on U.S. citizens. His amendment would have protected the rights of innocent U.S. citizens and provided a necessary balance to the bill. I was proud to support it because the bill, obviously, needed some more checks and balances.

Senator FEINGOLD also had an amendment to provide protection against bulk collection of foreign communications that could include communications of innocent Americans. Again, this measure would have provided additional protection for the rights of American citizens, and I was proud to support it because I believe we need, again, additional checks on enhanced Government surveillance authority.

My colleague and friend from California, Senator FEINSTEIN, had an amendment that stated a very important principle: that FISA, the Foreign Intelligence Surveillance Act, is the exclusive authority for conducting foreign intelligence surveillance.

Why is that important? It is important because this administration argues time and again that ''it has inherent authority'' to conduct warrantless surveillance, or that Congress somehow gave them the authority when it authorized the use of military force in Iraq—a ridiculous claim. The Feinstein amendment was a very important amendment because it would have made it clear that FISA is the exclusive authority, pure and simple.

Why was that important going forward? We don't want to have this administration or another one in the future—I don't care which party they are from—spying on the American people and then saying: It is true, we didn't obey FISA, but we thought it was important to go outside the law. If we had adopted the Feinstein amendment, we would have clearly stated that FISA is the law when it comes to conducting surveillance on our own people.

The Feinstein amendment—which failed, sadly by only 1 or 2 votes short of the 60-vote hurdle—said we are not going to lose our freedoms, we are not going to allow another administration to spy on us; FISA is going to be the one and only law that pertains here.

Finally, there is the issue of immunity for telecommunications companies that cooperated with the administration's warrantless surveillance program. We know that American law did not give these telephone companies the authority to do what they did, but they were somehow persuaded by the administration to go along with them. Not every telephone company, not every communications company did go along. At least one said: Look, we think this is not legal; show us the legality. And they stood, I think, in firm support of their consumers.

Here is the problem with granting immunity. Congress has not been given complete information on this program. We do not know the level of involvement by the telephone companies and the telecom companies. We need complete information; we have incomplete information. How can I be a good Senator, how can I do a good job if I don't have the facts surrounding this whole matter of the warrantless surveillance program? When you put out that immunity, you basically stop the court cases, and if you stop the court cases, we will never get to the bottom of this issue and our citizens will never know who was spied on, why were they spied on, what happened, what went wrong, what went right, and how much power this Government tried to exercise over its people illegally.

Granting immunity without fully understanding whether our people were illegally spied upon and to what extent, I find that irresponsible. Where is our pride? We wrote a law that said phone companies cannot do this, and they went ahead and did it. Not all of them. Now we are saying: Never mind, President Bush and Vice President CHENEY write the law, they make the decision. It is not right. It is not American. It is anti-American. It is not what we do in this great country.

President Bush says we are sending our troops overseas to fight for freedom, fight for democracy, and at home they ask the telecom companies to break the law. They spied on Americans, and we cannot find out what they did, how they did it, the details of the program, and now we are going to now grant immunity. I cannot believe that we didn't do better on that particular amendment. That amendment failed. Again, I was proud to stand with Senator DODD and Senator FEINGOLD on the amendment.

In closing, I don't believe this bill strikes the kind of balance we need between broadening the Government's authority to conduct surveillance and protecting the rights of our citizens. We did have many chances today to increase the oversight of FISA surveillance programs. We had many opportunities to hold this administration accountable and future administrations accountable while giving them what they need to go after the bad actors, those who would harm us. I voted to get bin Laden. I voted to go to war against al-Qaida. I voted no on the Iraq war because that was a diversion. I want to get the terrorists who perpetrated 9/11. I want to give any administration the tools they need, but I do not want to expose my constituents and the people of America who are law-abiding and caring and all they live for is for their families—I don't want to subject them to being spied upon.

Unfortunately, those amendments all went down. It is sad for me to say that we have a bill that steps on the rights of the freedoms of our people, of the law-abiding Americans in our country and, therefore, I cannot support it.

Mr. President, I yield the floor. I suggest the absence of a quorum, and I ask that the time be taken equally off both sides.

The PRESIDING OFFICER. Without objection, it is so ordered.

The clerk will call the roll.

The bill clerk proceeded to call the roll.

Mr. DODD. Mr. President, I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER. Without objection, it is so ordered.

Mr. DODD. Mr. President, it is clear now that this body is going to approve retroactive immunity for the telecom industry, which may have helped the President to illegally spy on millions of Americans.

I have spoken on this issue now for I think in excess of 20 hours, going back 2½ months ago when this issue first came to the floor in December. Just to recall the history of the last couple of months briefly, if I may: Two committees of the Senate, appropriately, had jurisdiction over this matter—the Intelligence Committee and the Judiciary Committee. In fact, the House of Representatives similarly had two committees with jurisdiction over this matter, the matter being the amendments to the Foreign Intelligence Surveillance Act.

I have talked at length about the history of that act and commended our previous colleagues who served in this body for having crafted a rather ingenious piece of legislation that architecturally created the balance between security and liberty in the wake of the Watergate scandal in the mid-1970s. Democrats and Republicans came together and said: How can we guarantee that we can gather information to keep our Nation safe and secure from those who would do us harm and simultaneously protect the more than two centuries of liberties and rights that Americans have come to associate with our Constitution—the rule of law?

This was not an easy matter, striking that balance, that tension which has existed for more than 220 years in our country, and I would be the first to admit that. So I have great admiration for those who struggled with it.

In 1978, the FISA—the Foreign Intelligence Surveillance Act—Court was established, a secret court, the members of which are appointed by the Chief Justice of the U.S. Supreme Court. The members of that court are sitting Federal judges across the land. No one can ever know who these judges are. They are anonymous in that sense, and they are called upon at a moment's

notice to determine whether probable cause exists for a warrant to be issued to allow our Government to require institutions, public or private, to provide information that could affect the safety and security of our country. That has been the history.

Since 1978, time and again the Congress of the United States has amended the Foreign Intelligence Surveillance Act. Usually, it was amended in order to keep pace with the ability of those who would do us harm to utilize new technologies, new sources of information that could prove to be dangerous for our country; but simultaneously, legislation was upgraded so that the new means of gathering information, of determining who would do us harm, were also improving. In almost every instance, the amendments and the changes to the Foreign Intelligence Surveillance Act were adopted unanimously by members of both political parties.

That brings us, of course, to this year, with the amendments being offered to this Foreign Intelligence Surveillance Act.

Events occurred either prior to 9/11 or shortly thereafter which have caused the most significant debate yet on FISA. There are those who have argued that, in fact, the surveillance activity that is the subject of the retroactive immunity actually began prior to the attacks of 9/11. The bulk of the evidence seems to point to the fact that this surveillance began shortly thereafter.

I would not be standing here, as I have said before, had this been a momentary lapse of judgment, considering the emotions of the attacks here on our country. I could understand why a President, why a telecom industry, in the wake of 9/11, would have responded to a request to gather information quickly to determine not only who did us harm but what additional dangers they posed to us. I would not be standing here if this had been an administration that had not engaged in a pattern of behavior over the years that suggested they had less than a high regard for the rule of law. But as we have now learned, this was not a matter of a week or a month or a year. This warrantless invasion of our privacy went on for 5 long years, without any rule of law behind it except the word of an American President and apparently the sanction of the Attorney General of the United States.

FISA specifically said in 1978 that you must have a warrant to do this. We even changed the law, as you know, Mr. President, to say that you could even get the warrant after the fact if the emergency was such that you didn't have the opportunity to get the warrant but went after the fact, immediately thereafter.

I would point out, Mr. President, as I did in some detail last evening for almost 3 hours on this floor, that the President's warrantless wiretapping program was not a selective or focused surveillance merely on those who were outside the country or those who were suspected or might be involved in threatening activities. This decision to gather information included literally every phone call, every fax, every e-mail, every image that went through 16 phone companies of our country, using what they call splitters to literally vacuum up everything that came in. If the allegations are true, it was one of the single largest invasions of privacy in the history of our country, all done without a warrant and without a court order.

We discovered this because of a whistleblower and a report in the media that revealed the program. Otherwise, I suspect it would be going on as I speak, without any interruption whatsoever. In fact, the only interruption that occurred, I might point out—because the argument has been made that these companies were acting out of patriotism—came, according to some reports when the Federal Government stopped paying the phone companies for collecting it.

I would also point out that not every phone company complied. I know the argument has been made: Look, everyone did it. It is a common argument, one we made to our parents, usually: Everyone was doing it. We all remember the answer we received from our parents. Well, the argument here is: Almost everyone was doing it. Quest decided not to. When the request was made of them to gather information without a warrant, they said: Give us a court order, and we will comply. A court order was never forthcoming, of course, and they never participated.

So this December, we arrived at this debate about whether to grant the telecoms retroactive immunity. Three other committees had examined this issue, and all three of the committees, in the House and in this body, had determined that retroactive immunity was not warranted. Only one committee decided it was, but that committee has prevailed in the last several days, weeks, and months in this debate, and as such we are now confronted with cloture being invoked, cutting off debate here about the subject matter. And given the votes today, in all likelihood this body is not going to change its mind on this issue. Our only hope, those of us who feel strongly about this, is that the other body, the House of Representatives, which has taken a very different point of view, will be able to prevail in the conference between these two bills, and deny retroactive immunity.

Let me point out quickly that denying retroactive immunity does not mean the phone companies will necessarily be found guilty of doing something wrong. All it means is that the coequal branch of Government, the judicial branch, will get a chance to look at whether what they did was legal. I have my own opinions about this, but my opinions should not prevail, nor should the opinions of 51 Members of this body. We are not the judicial branch, we are the legislative branch.

The Founders of this great Republic of ours created three coequal branches of Government, and the judicial branch was designed and created to check the actions of the executive and legislative branches and determine whether things we did were constitutional—legal—or not. That is why they exist. So the debate about whether what the companies did or did not do is legal is not a matter for this body to determine, any more than it is for the executive branch. It is the judicial branch that should make that determination. Yet, by the action we took earlier today, we are now going to close the door on determining whether the action taken by the phone companies was legal.

Sweep it under the carpet, close the door, and we will set the precedent for some future Congress, which will point to this debate and its conclusion and decide that the Congress of the United States found that the FISA Court was not needed or, that in fact the President could collect whatever data and information he wanted—maybe medical records, maybe financial records, maybe personal histories of families.

I feel passionately about this issue. This is the first time in my quarter of a century service here that I have engaged in what might be called some ''extended debate''—that is how deeply I care about this issue.

Nothing is more important, in my view, than the rule of law and the Constitution. No threat is so urgent that we should be willing to abandon the rule of law. But that is exactly what we have done. And it is a false and phony argument to claim that failing to do so would jeopardize our security. There is a long history of the judicial branch of Government in this country dealing with sensitive national security matters in camera, without revealing state secrets. The suggestion that we cannot possibly let the courts look at the use of warrantless wiretapping is so false on its face it is hardly worthy of an argument to the contrary.

In fact, Judge Walker, a Republican appointee to the Federal bench, I might point out, has ridiculed the argument that these matters could not go before the judicial branch for review. There is no longer a debate about whether the wiretapping program is in the public—it is. And the means and technology used to do it have publicly been discussed and debated.

This decision deprives us of the opportunity to determine exactly what happened. I would further point out that but for the insistence of the chairman of this committee and the ranking member, and I suspect others, the administration would have succeeded in immunizing everyone involved with this, everyone within the executive branch, the White House, the Justice Department.

The chairman and the ranking member said that was going too far. But that request is instructive. What do we

learn from it? Why did the administration demand of the Intelligence Committee that everyone associated with this matter be immunized against any further legal action? What was the motive behind it? Doesn't that suggest that something else must be going on?

That is where we are in all of this. Again, I apologize to my colleagues and others for taking so much time to talk about this. But as I mentioned last evening, I grew up in a family with a father who was deeply involved in the rule of law. He was a prosecutor at the Nuremberg trials in 1945 and 1946, a rather unique moment in American history, where because of an American President, because of a Secretary of War, because of a Supreme Court Justice and a handful of others, America did not yield to the vengeance, even for those enemies we hated the most: Nazis who had incinerated 6 million Jews and 5 million others targeted for their politics, religion, and otherwise. Why would you possibly give that crowd a trial? A handful of Americans, Republicans and Democrats, got together and said: America is different. We believe in the rule of law in the United States. And we believe the rule of law is something that does not necessarily belong to one Nation or sovereignty; it belongs to all people, reaching back to our own founding documents that tell us that the rule of law, not the rule of man, ought to prevail.

So the United States, along with our very reluctant allies, created the Nuremberg trials, which established the moral high ground for the United States in so many ways. As a result, 21 defendants in the first trial got a lawyer and got to present evidence and defend themselves—because we followed the rule of law.

It was the moral high ground and the basis for so much else that was created in the post World War II period: The international courts, the U.N. system, the NATO system, the Marshall Plan. All these institutions sprang from that what we helped create in the wake of World War II and the Nuremberg trials.

So I grew up around a dining room table where the rule of law was talked about all the time. I was taught that our Constitution did not belong to a political party, it did not belong to politicians or candidates.

And I remember that great scene in the movie ''A Man For All Seasons,'' where Thomas More is asked if he would not be willing to cut down all the laws in England to get his hands on the devil.

And More responds, and I am paraphrasing his quote: When I have cut down every law in England to get to the devil and the devil comes after me, what laws will stand there to protect me?

So while some may feel comfort that they are being protected by this decision we have made, they should remind themselves the worm does turn, and someday they may find themselves on the opposite side of this question.

So this debate should not be framed as the issue of the hour; rather, it is about the principle behind it, and that is the rule of law. The power of courts to decide the legality and illegality of actions is so deeply imbedded in our Constitution, so deeply imbedded in the fabric of how we conduct ourselves, that it ought not to be the subject of a partisan discussion and debate.

That is why I have fought to keep this day from coming with everything I had in me. I have not fought alone. Many average Americans have given me strength for this fight, strength that comes from the passion and eloquence of citizens who do not have to be involved, but choose to be involved. I thank them for it.

But today when I speak in this body against this immunity and for the rule of law, I am speaking for a minority. And respecting the rule of law anywhere means respecting it everywhere, even when it means we do not win. The rule of law says we, the minority, cannot stand forever; and having made our case with all the fire in us, we stand down and wait for a different day and a different set of circumstances.

I will say this, though. I have seen some dark days in this Chamber; in my mind, one of the worst was September 28, 2007. That was the day the Senate voted to strip habeas corpus and tolerate torture.

Today, February 12, 2008, is nearly as dark: the day the Senate voted to ensure secrecy and to exempt corporations from the rule of law. Frankly, I have seen a lot of darkness in recent years, as one by one our dearest traditions of constitutional governance have been attacked.

At each new attack, millions of Americans have stood up in outrage; but millions more have answered with patience. One might fault them for that, but I do not. More than two centuries of democratic tradition have nurtured that patience; it speaks well of our Democratic faith that so many take the rule of law in America as a given.

If millions have not yet noticed the rule of law falling, that is because it has so far to fall. But fall it will, if we remove our support for it. The law in America is not a gift or an inheritance; it is the active work of every generation to preserve and protect it.

As America's patience wears thinner and thinner, and as more and more citizens take up that active work, our minority will—I have faith that it will—make itself a majority.

But today was not that day. And so the Senate has signed its name to this immunity, this silencing of our courts, this officially sanctioned secrecy, without a majority of us evening laying eyes on the secret papers that are supposed to prove the President's case.

Retroactive immunity is a disgrace in itself. And in the last months I believe we have proved that beyond a reasonable doubt. But it is even more disgraceful in all it represents. It is the mindset that the Church Committee summed up so eloquently three decades ago.

> The view that the traditional American principles of justice and fair play have no place in our struggle against the enemies of freedom.

That view created the Nixonian secrecy of the 1970s, and the Church Committee wrote those words, in part, as a rebuke to our predecessors in this Chamber who for years let secrecy and executive abuses slide. But today those words take on a new meaning. Today they rebuke us. They shame us for our lack of faith that we can, at the same time, keep our country safe and our Constitution whole.

When the 21st century version of the Church Committee convenes to investigate the abuse of the past years, how will it judge us? What will it say about us when they look back on our actions? When it reads through the records of our debate—not if, but when—what will it find?

When the President asked us to repudiate the Geneva Conventions and strip away the right of habeas corpus, how did we respond?

When images of American troops tormenting detainees were broadcasted around the world, how did we protest?

When stories of secret prisons and outsourced torture became impossible to deny, how did we resist?

And on February 12, 2008, when we were asked to put corporations explicitly outside the law and accept at face value the argument that some are literally too rich to be sued, how did we vote?

All of those questions are coming for us. All of them and more. And in the quiet of his or her own conscience, each Senator knows what the answers are.

I fought so long against retroactive immunity because, in this huge fabric of lawlessness, it was the closest thread to grab. I believed if we grabbed hold and pulled, it would begin to unravel. That has not happened.

But if we believe that each assault against the rule of law was an accident, that each was isolated, we are deluding ourselves. If the past is any guide, there will be another one. And hope, as they say, springs eternal. I hope we will stand up then.

And perhaps we will have the chance to do so very soon. As I mentioned a few minutes ago, the House of Representatives has passed a version of this bill without retroactive immunity. It will be the job of the conference between the House of Representatives and the Senate to reconcile the two versions of this bill.

And before I stand down, I wish to implore the members of that committee, in the strongest terms I can find, to strip retroactive immunity from this bill once and for all. Remember, this is about more than a few telephone calls, a few companies, a few lawsuits. If the supporters of retroactive immunity keep this small, they win. In truth, the issue we have debated for the last few months, the issue

that will finally come to a head in this conference committee, is so much more. At stake is our latest answer to the defining question: The rule of law or the rule of men?

That question never goes away. As long as there are free societies, generations of leaders will struggle mightily to answer it. Each generation must answer for itself; and just because our Founders answered it correctly does not mean they are bound by their choice. In that, as in all decisions, we are entirely free; the whole burden falls on us.

But we can take counsel. We can listen to those who came before us, who made the right choice, even when our Nation's very survival was at risk. They knew that the rule of law was far more rooted in our character than any one man's lawlessness.

I do not think that has changed at all. Secure in that faith, I will sit down now and end my part in this conversation. But when the question of the rule of law or the rule of men comes again, which it surely will, I will be proud to stand up once more. And if this bill comes back with retroactive immunity, I will speak against that travesty—the denial of the rule of law in favor of the rule of men.

I yield the floor.

The PRESIDING OFFICER (Mr. SALAZAR). The Senator from Washington is recognized.

Ms. CANTWELL. I rise today to express concerns about the FISA Amendments Act S. 2248 before us. This morning, the Senate lost an opportunity to strengthen this bill. And, unfortunately, without those critical provisions, I will have to oppose the bill before us. I thank the Senator from Connecticut for his leadership in fighting against this bill. I know he will be back on this issue at every opportunity.

Mr. President, I rise to join this debate. I have been, over many years, interested and involved in privacy rights issues in a variety of capacities. Certainly, the residents of my state care passionately about their rights to privacy.

This administration has done a lot to blur the line between foreign intelligence gathering and spying on U.S. citizens. Now, the legislation before us today could have been improved to better protect the rights of U.S. citizens by passing amendments proposed by my colleague Senator FEINGOLD, but we turned those down.

Instead what has been a delicate balance in the United States to protect the rights of privacy of U.S. citizens and national security is going to be further eroded.

Congress has limited powers and so does the President. The President does not and should not have unchecked power in this or any other area. It would be contrary to our American values and our system of government, which has endured for more than 231 years.

When strengthening national security, we must also safeguard civil liberties and the privacy rights of American citizens. I cannot support a bill that fails to strike this critical balance, as the original Foreign Intelligence Surveillance Act (FISA) did. We didn't allow the government to have unchecked unlimited authority then, and we shouldn't allow it now. There have been times in the past when both Democratic and Republican administrations lost sight of the need to protect U.S. citizens' privacy rights.

We all want to protect the United States, but how good is this approach if the end result is that everyone thinks that there is a back door to our computer operating systems, a back door to our telecommunication systems? Who will want to do business in the United States if they think there are no secure systems, only systems to which the U.S. government will have access? Communications over the Internet, regardless of country of origin or country of destination, know no national boundaries, and travel by the most efficient route. If the Act as currently drafted goes forward, it may lead to an international reexamination of how the Internet should operate. FISA has been a very important part of our checks and balances.

In our country, a Senator cannot pick or choose what laws they follow and neither should the President nor telecommunication companies. Congress should not be providing blanket immunity for telecommunications companies that cooperated with the Administration's warrantless wiretapping programs. We don't know precisely what those companies did or the full extent of what they did.

I believe the Federal courts should be allowed to rule on the legality of the companies' conduct. Congress should not move to preempt judicial decisions. Special procedures can be put in place that could allow such cases to move ahead without revealing classified information or damaging U.S. national security. Specifically, I want to touch on the lawsuit the Electronic Frontier Foundation (EFF) filed against a large telecom company, accusing it of violating FISA, on behalf of a class of its customers. If retroactive immunity is granted to telecom providers, the lawsuit will be dismissed, and the public will never get an opportunity of getting even a glimpse of what happened.

The issue of the Federal Government and telecoms possibly violating FISA came to light in part as a result of the actions of a brave whistleblower. According to media reports and internal AT&T documents provided by this whistleblower, Mark Klein, the telecom company allegedly splits off a copy of all of the Internet traffic transported over fiber-optic cables running though its San Francisco office and diverts it all—e-mails, IMs, web browsing, everything—to a secure room under the control of the National Security Agency that contains sophisticated data-mining equipment capable of monitoring all the communications' content in real-time. What appears to have happened is a major change in how electronic surveillance is conducted in this country. Surveillance used to be particularized—investigators would pick a target and then intercept the communications of that target. But now, it appears the Administration is using advances in technology to move to a wholesale surveillance regime, where everything is intercepted and then investigators sift through the hay to pick their targets. In other words, the Administration is seizing millions of Americans' communications—billions of phone calls and e-mails and more—in a 21st century high-tech equivalent of the King's general warrants that our Founders fought a revolution to avoid.

The Electronic Frontier Foundation wants a court to be able to decide whether this new mode of surveillance is or can ever be legal, under FISA or the fourth amendment. Letting the courts decide that question is critical to checks and balances, critical to ensuring that Congress' privacy laws are followed and the fourth amendment respected, and critical to preventing abuses of power. Therefore, I urge my colleagues to allow this case to move forward. I urge them to allow the Federal courts to rule on the legality of the companies' conduct. These are the issues, I believe, that must be reviewed by the courts. I think passing this legislation really preempts what is critical judicial review and undermines the fundamental principle of checks and balances in our system.

I know these are challenging times. But we have to remember our Constitution and to remember what is effective policy. Everybody in America wants to be safer and we want to use technology to protect our national security. But, technology can be used in a way that protects privacy rights. This all goes back to checks and balances. Instead of rushing to dismantle them, Congress needs to maintain and strengthen these checks and balances in order to prevent abuses of power. This model has worked for our country.

I encourage my colleagues to make sure we remember the fourth amendment and we remember our citizens' rights to privacy as well in considering this legislation, which I hope the Senate will turn down this afternoon.

Mr. ROCKEFELLER. Mr. President, under a unanimous Consent agreement, the Senate has accepted three amendments to the FISA Amendments Act of 2008. I would like to say a word about each.

The senior Senator from Massachusetts has authored a helpful amendment to ensure that the Government will not intentionally acquire communications where the sender and all intended recipients are known at the time of the acquisition to be located in the United States.

Our bill, S. 2248, is not intended to authorize the intelligence community to acquire purely domestic communications.

Electronic surveillance of purely domestic communications requires a court order under title I of FISA. In addition, S. 2248 explicitly prohibits the targeting of persons known at the time of acquisition to be located inside the United States.

The importance of the Kennedy amendment is that it reinforces our intent. It should put to rest any doubts about what the Senate intends with respect to protecting the communications of persons within the United States. I am grateful for the willingness of the Senator KENNEDY to work with the committee on this amendment.

I would also like to acknowledge his leading role in the history of FISA as the sponsor of the original FISA legislation, first in 1976, and then when FISA was enacted in 1978. Senator KENNEDY helped the Congress then to enact legislation that protects both our national security and the rights of Americans. We are grateful that he has stepped forward again to help us achieve those goals.

Under the unanimous consent agreement, the Senate has accepted an amendment by Senator WHITEHOUSE that resolves an important question about the status, pending appeal, of an order by the Foreign Intelligence Surveillance Court requiring correction of deficiencies in intelligence collection procedures under the new title VII of FISA.

The amendment requires the FISA Court of Review to determine, within 60 days of the Government's appeal, whether all or part of a FISA Court order requiring correction will be implemented during the appeal. The Government may continue collection until the appellate court makes that determination, and longer if the Court so determines. The 60-day requirement ensures that the matter will receive appellate attention without undue delay.

We appreciate Senator WHITEHOUSE's successful effort to resolve this matter.

Finally, under the unanimous consent agreement, the Senate has accepted an amendment by Vice Chairman BOND to delete a statutory requirement that appeals in cases either challenging or seeking to enforce directives to companies be filed within 7 days. The amendment leaves it to the FISA Court or the Court of Review to establish that deadline as they do for all other appeals under FISA.

The amendment recognizes the responsibility of those courts to establish rules. And it recognizes that both the Government and carriers may require additional time to evaluate whether an appeal should be filed.

I appreciate the vice chairman's effort to resolve this matter.

Mr. OBAMA. Mr. President, I am disappointed that the Senate has rejected several commonsense improvements to the Intelligence Committee's FISA proposal. I commend my colleagues, Senators DODD, FEINGOLD, TESTER, WEBB, WHITEHOUSE, LEAHY, SPECTER and others, for proposing these solutions, and I welcome the outpouring of interest on this issue from informed and concerned citizens around the country.

News last week from the Intelligence Committee hearing underscored the importance of ensuring that our surveillance laws protect our security, just as we must vigilantly safeguard our civil liberties. Director of National Intelligence McConnell warned that al-Qaida continues to train and recruit new adherents to attack within the United States, and such reports should serve to unite us in common purpose against the terrorists that threaten our homeland. Instead, President Bush is using this debate once again to divide us through a politics of fear.

I was disappointed to learn of the President's threat to veto any FISA bill that does not include an unprecedented grant of immunity for telephone companies that cooperated with the President's warrantless wiretapping program. Why the President continues to try to hold this important legislation captive to that special interest provision defies explanation.

I was proud to cosponsor the Dodd-Feingold amendment to strike the immunity provision from the bill. However, with the defeat of this amendment, telephone companies will not be held accountable even if it could be proven that they clearly and knowingly broke the law and nullified the privacy rights of Americans. This is a matter for the courts to decide, not for preemptive action by the Senate.

We can give our intelligence and law enforcement community the powers they need to track down and take out terrorists without undermining our commitment to the rule of law or our basic rights and liberties. That is why I cosponsored the Feingold amendment, which would have prevented the Government from using these extraordinary warrantless powers to conduct ''bulk collection'' of American information. I also supported the Feingold-Webb-Tester amendment to protect the privacy of Americans' communications by requiring court orders to monitor American communications on American soil, unless there is reason to believe that the communications involve terrorist activities directed at the United States or the monitoring is necessary to prevent death or serious bodily harm. Unfortunately, these amendments were defeated as well. These are the types of narrowly tailored, commonsense fixes that would have allowed the Government to conduct surveillance without sacrificing our precious civil liberties.

For over 6 years since the attacks of 9/11, this administration has approached issues related to terrorism as opportunities to use fear to advance ideological policies and political agendas. It is time for this politics of fear to end.

We need durable tools in this fight against terrorism—tools that protect the liberties we cherish and the security we demand. We are trying to protect the American people, not special interests like the telecommunications industry. We are trying to ensure that we don't sacrifice our liberty in pursuit of security, and it is past time for the administration to join us in that effort.

There is no need for the goals of security and liberty to be contradictory.

Mr. LEVIN. Mr. President, last year Congress passed a temporary bill with a 6-month time limit that would give us the opportunity to carry out a thorough, thoughtful examination of how to utilize complicated new technologies in the surveillance of suspected terrorists without invading the privacy of innocent Americans. In the months since we passed that temporary act, we have worked in a bipartisan manner to consider the best course forward for permanent changes to the Foreign Intelligence Surveillance Act. Despite the enormous complexity of these issues, we reached a bipartisan consensus on the key provisions contained in title I of the bill we are considering today.

I believe that title I of the bill before us appropriately provides the intelligence community the authority it needs to collect intelligence information on suspected terrorists. The collection of that intelligence is important to our national security and merits congressional support. That is why I helped write the Rockefeller-Levin substitute amendment that we voted on last summer, why I voted in favor of the Leahy substitute amendment that we considered in January, and why I support title I of the bill before us today. In my view, the Rockefeller-Levin substitute, the Leahy substitute, and title I of this bill all provide for the appropriate collection of intelligence information on suspected terrorists.

Title I of this bill would provide the needed authority for collection of that information in a responsible manner.

Title I of this bill, unlike the temporary act which we passed last summer, would not authorize the targeting of U.S. persons for electronic surveillance without probable cause.

Title I of this bill, unlike the temporary act, would not authorize the administration to collect communications—including communications to and from U.S. persons—for months without even submitting the collection program for court approval.

Title I of this bill, unlike the temporary act, would not authorize the administration to continue to collect such communications for an extended period even after the FISA Court has specifically rejected an application for approval.

Title I of this bill, unlike the temporary act, would expressly authorize judicial review of the targeting and so-called minimization procedures in order to protect the privacy rights of U.S. persons.

Title I of this bill, unlike the temporary act, would require regular inspector general reviews and regular reports to Congress on any authorized collection program.

I congratulate Senator ROCKEFELLER and other colleagues on their success in achieving the administration's support for these well-crafted title I provisions, which are significant improvements over the temporary bill hastily adopted last year.

Title II of the bill is a different story. Title II would eliminate accountability by granting retroactive immunity for telecommunications providers that disclosed communications and other confidential information of their customers at the behest of Government officials. They did this despite a law specifically making it illegal to do so. Unlike title I, there is no bipartisan agreement on title II.

Title II would require dismissal of lawsuits brought by persons claiming injury from interception and disclosure of their communications, even if the activity resulting in the injury was illegal. It would require dismissal of lawsuits, even if the disclosure violated the constitutional rights of individuals whose personal information was illegally disclosed. It would require dismissal of lawsuits, even if innocent U.S. citizens were damaged by the disclosure or compromise of confidential personal information.

Retroactive immunity is not fair. It is not wise. And it is not necessary.

Retroactive immunity is not fair because it leaves American citizens who may have been harmed by the alleged unlawful conduct of these providers without any legal remedy.

Retroactive immunity is not wise because it precludes any judicial review of that conduct. I am deeply concerned that if we act here to immunize private parties who participated in a program that appears to have been clearly illegal, we may encourage others to engage in such illegal activities in the future. In a free society, illegal activity cannot be excused on the grounds that Government officials asked you to carry it out. There must be accountability for illegal acts. As written, title II eliminates some critically required accountability.

Nor is retroactive immunity necessary. Congress has already ensured the future cooperation of the telecommunications providers with the intelligence community in the Protect America Act adopted last August. That act authorizes the Attorney General or the Director of National Intelligence to direct telecommunications providers to disclose certain information and provides prospective immunity to telecommunications providers that cooperate with such directives.

Title I of the bill before us appropriately continues to provide prospective immunity to telecommunications providers. Title I states:

Notwithstanding any other law, no cause of action shall lie in any court against any electronic communication service provider for providing any information, facilities, or assistance in accordance with a directive issued by the Attorney General or the Director of National Intelligence pursuant to the act.

In light of the prospective immunity in title I, which is appropriately in this bill, the retroactive immunity of title II is not necessary to ensure the future cooperation of telecommunications providers that receive legitimate requests for information from the intelligence community.

The argument has been made that we must provide retroactive immunity to the telecommunications providers to ensure the cases against them are immediately dismissed because if the cases are permitted to proceed, vital national security information will be disclosed. But the courts have numerous tools at their disposal to protect such information and have successfully used these tools throughout our history. They can review evidence in a classified setting; they can redact documents; they can even dismiss a case for national security reasons if they deem it necessary to do so.

Some have even taken the position that the mere existence of this litigation, even without the disclosure of any information, will somehow help the terrorists. But the President has already disclosed the existence of the collection program at issue. It has been discussed in Congress and in the press. The Director of National Intelligence has publicly discussed the program.

There is a way to properly immunize from legal liability telecommunications providers that acted in good faith based on the assurances of appropriate administration officials. The way to do that is by substituting the United States for the telecommunications providers as the defendant in lawsuits based on the actions of those providers. That substitution would safeguard telecommunications providers from liability just as effectively as the retroactive immunity language in title II of the bill. But unlike the retroactive immunity language of title II, it would not leave persons who can prove they were victims of unlawful actions without a remedy.

We can ensure that any such innocent victims retain whatever legal rights they have under applicable law, except that the U.S. Government would be substituted for the telecommunications providers as the defendant in such lawsuits. And it is appropriate that the Government be liable rather than the telecommunications providers, since the disclosures were allegedly made by the providers in these cases at the request of senior executive branch officials based on appeals to help safeguard U.S. security and assurances that the providers would be protected from liability regardless of the requirements of law.

We had a number of opportunities to provide equity both to the telecommunications providers and to any injured citizens.

We had the opportunity to adopt the Dodd-Feingold amendment, which would have struck title II from the bill, allowing us to adopt a new approach that protects both the equities of telecommunications providers that acted in good faith and those of people who were allegedly injured by their illegal actions.

We had the opportunity to adopt the Specter-Whitehouse substitution amendment, which would have fully protected telecommunications providers, without depriving American citizens who were harmed by unlawful collection of their personal information of a legal remedy. It did so by substituting the United States for the telecommunications providers as the defendant in lawsuits based on the actions of those providers. That substitution would safeguard telecommunications providers from liability just as effectively as the retroactive immunity language in title II of the bill.

And we had the opportunity to adopt the Feinstein amendment, which would have limited immunity to those telecommunications providers that are found by a court to have acted in reasonable, good-faith reliance on assurances from executive branch officials.

The adoption of these amendments would have made a significant improvement to the bill. With their rejection, I cannot support this bill despite my support for title I, which again, appropriately, authorizes the collection of intelligence. But it is my hope that a bill comes from conference with the House of Representatives that includes appropriate changes to eliminate unfair, unwise, and unnecessary retroactive immunity provisions.

I yield the floor and suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The legislative clerk proceeded to call the roll.

Mr. LEAHY. Madam President, I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER (Mrs. MCCASKILL). Without objection, it is so ordered.

Mr. LEAHY. Madam President, what is the parliamentary situation?

The PRESIDING OFFICER. The Senator from Vermont has 20 minutes.

Mr. LEAHY. Madam President, the Foreign Intelligence Surveillance Act FISA is intended to protect our national security. It is also intended to protect the privacy and civil liberties of Americans. The law was passed to protect the rights of Americans after the excesses of an earlier time.

We are debating amendments to this important law. I had hoped the Senate would act to improve the bill reported by the Select Committee on Intelligence. It has not. I had hoped the Senate would incorporate improvements included in the House-passed RESTORE Act and the bill reported by the Senate Judiciary Committee. It has not.

I had hoped the administration would work with us. It has not. Instead, having gotten exactly the bill they want, in the way they want, from the Intelligence Committee, they have threatened a Presidential veto if we improve this bill in any way or fix its flaws.

I had hoped that Republican Senators would work with us as we have worked together to amend FISA dozens of times over the last 30 years and to update it in more than a dozen ways even since September 11, 2001. But instead of working in a bipartisan fashion, as I have seen before in my 34 years in the Senate, in an unprecedented way, Republicans voted lockstep to table the Judiciary Committee improvements and virtually lockstep against every individual amendment and improvement.

Worse, the Republican leadership has stalled action on the measure for weeks. They continue to insist it is their way or no way. Sadly, with the acquiescence of even some on this side of the aisle, they have controlled the debate, the bill, and the final result in the Senate.

Working together we could have done so much better. I look forward to working with the House to make improvements that are needed to this measure before I can support it.

The process has been, in large part, a repeat of that which led to the so-called Protect America Act last summer. That ill-conceived measure was rushed through the Senate in an atmosphere of fear and intimidation just before the August recess, and after the administration had broken their word and reneged on agreements reached with congressional leaders. The bill was hurriedly passed under intense partisan pressure from the administration. It provided sweeping new powers to the Government to engage in surveillance, without a warrant, of calls to and from the United States involving Americans, and it provided no meaningful protection for the privacy and civil liberties of Americans who were on those calls.

I was here when we first passed FISA because we knew what happened when we had an out-of-control administration. We saw it during the Watergate years. We saw it with J. Edgar Hoover. We saw those who wiretapped people because they didn't like what they said, they disagreed with the administration; they actually raised questions about the Vietnam war. Sometimes it would help if everybody read a history book every now and then around here. Some seem too willing to give up the liberties for which we fought.

The Senate should have considered and incorporated more meaningful corrections to the so-called Protect America Act. Before that flawed bill passed, Senator ROCKEFELLER and I and several others in the House and Senate had worked hard and in good faith with the administration to craft legislation that solved an identified problem but also protected Americans' privacy and liberties.

We all want to protect our security. We all want the ability to go after those who would do this country harm. And we drafted legislation that would have taken care of the problem they told us about.

But just before the August recess, we got a call. Basically, the Director of National Intelligence told us they could not keep their word, they could not keep the administration's word, and the administration decided to ram through its version of the so-called Protect America Act, with excessive grants of Government authority and without accountability or checks and balances. They refused to consider any other way.

After almost 6 years of breaking the law and violating FISA through secret warrantless wiretapping programs, that was wrong. A number of us supported a better balanced alternative, and we voted against the Protect America Act as drafted by the administration and passed by the Senate.

Ironically, the reason we were even voting on it is that the press found out how the administration was breaking the law. Even though the administration was required by statute to tell leaders in Congress what they were doing, which was a clear violation of the law, they had failed to do that. Fortunately, we still have some remnant of a free press in this country and they found it out.

Because of a sunset provision, we had a chance to revisit that matter and correct it. The Judiciary Committees and the Intelligence Committees of the Senate and the House spent the past months considering changes to FISA. In the Senate Judiciary Committee, we held open hearings and countless briefings and meetings to consider new surveillance legislation, including classified meetings. We considered legislative language in a number of open business meetings of the committee, and we reported a good bill to the Senate. This was before last Thanksgiving.

Instead of that bill, a good bill, the Senate is poised to pass a bill that will permit the Government to review more Americans' communications with little in the way of meaningful court supervision.

I support surveillance targeting foreign threats, but I wanted to make sure we protect those American liberties that, after all, we fought a Revolutionary War to protect and a civil war and two World Wars and not just give it away because some people around here get cold feet when threatened by the administration.

Attorney General Mukasey said at his nomination hearing that ''protecting civil liberties, and people's confidence that those liberties are protected, is a part of protecting national security.'' I agree with him about that. That is what the Senate judiciary bill would have done.

The administration insists on avoiding accountability by including blanket retroactive immunity in their bill. It would grant blanket retroactive immunity to telecommunications carriers for their warrantless surveillance activities from 2001 through earlier this year contrary to FISA and in violation of the privacy rights of Americans.

The administration violated FISA by conducting warrantless surveillance for more than 5 years. They got caught. Frankly, if they had not gotten caught, they would probably still be doing it. When the public found out about the President's illegal surveillance of Americans, the administration and telephone companies were sued by citizens who believed their privacy and their rights were violated.

So now the administration is trying to get this Congress to terminate those lawsuits. But don't believe the crocodile tears of this administration, saying they are doing it to protect these telephone companies. This is, after all, the same administration that owed the telephone companies millions of dollars in unpaid bills for wiretapping. They will not even pay their bills.

No, the reason they want this provision is to protect those in the administration who broke the law. They don't want anybody to find out which members of the Department of Justice so thwarted the law in writing cockamamie legal opinions that a first-year law student would see through. They want to insulate themselves from accountability. I am not going to support such an end run around accountability.

The administration knows these lawsuits may be the only way that it is ever going to be called to account for its flagrant disrespect of the law. In running its illegal program of warrantless surveillance, the administration relied on legal opinions prepared in secret and shown to only a tiny cabal of like-minded officials.

This ensured that the administration received the advice they wanted. Don't tell us what the law is; tell us what we want the law to be. I used to read my children ''Alice in Wonderland.'' Now I read my grandchildren ''Alice in Wonderland.'' This sounds like ''Alice in Wonderland.''

Jack Goldsmith, a conservative Republican who came in briefly to head the Justice Department's Office of Legal Counsel, described the program as a ''legal mess.'' This administration does not want a court to have a chance to look at this legal mess, and retroactive immunity will assure not that they are protecting telephone companies, but that they will cover their own backsides. They want to protect themselves.

The rule of law is fundamentally important in our system, and so is protecting the rights of Americans from unlawful surveillance. I do not believe Congress can or should seek to take those rights and those claims from those already harmed. As I said, I worked with Senator SPECTER and both Senators FEINSTEIN and WHITEHOUSE to try to craft more effective alternatives

to retroactive immunity. We worked with the legal concept of substitution, replacing Government in the shoes of private defendants that acted at its behest. Let it assume full responsibility for the illegal conduct.

Substitution would have protected the telephone companies. It would have placed the administration in their shoes in the lawsuits. But the truth is that the administration doesn't really care about the telephone companies. They are worried only about the American public finding out what they did illegally, how they violated the laws and the Constitution of this country.

I also supported Senator FEINSTEIN's proposal to strengthen the role of the FISA Court in this regard. The administration and its allies in the Senate defeated both of these viable alternatives to retroactive immunity. The administration, by trying to frighten people, warded off all efforts of compromise and accommodation. They don't want to be held accountable, and they have enough Senators who will protect them so they will not be held accountable—not to the Congress or, more importantly, to the American people.

The Senate was forced to vote on retroactive immunity even though not all Senators had access to the information they needed to make an informed judgment about the Government's and the phone companies' conduct. The majority leader wrote to the administration last year urging such access, and I supported it. Of course, we got had no response. The administration ignored the request. After all, if we knew what we were doing around here, we might actually make them stand up and be responsible for their actions, which is the last thing in the world they want. It is clear they do not want to allow Senators or anyone else to evaluate their lawlessness. Their rule is no accountability. Whether it is Scooter Libby or anyone else, no accountability. We will protect those who break the law on our behalf.

I have drawn very different conclusions from Senator ROCKEFELLER about retroactive immunity. I agree with Senator SPECTER and many others that blanket retroactive immunity, which would end ongoing lawsuits by legislative fiat, undermines accountability.

Senator SPECTER has been working diligently, first as chairman of the Judiciary Committee and now as ranking member, to obtain judicial review of the legality of warrantless wiretapping of Americans from 2001 until last year. The checks and balances the judiciary provides in our constitutional democracy has an important role to play. Every one of us, if we follow our oath of office, should want to protect that. Judicial review can and should provide a measure of accountability.

I believe protecting the rule of law is important, and I believe in protecting the rights of Americans from unlawful surveillance. I do not believe the Congress can or should seek to take those rights and those claims from those already harmed. Moreover, ending ongoing litigation eliminates the only viable avenue of accountability for the Government's illegal actions.

Therefore, I say again, I oppose retroactive immunity. There should be a measure of accountability for the administration's actions in the years following 9/11. If it is simply a case of protecting the telephone companies, then why don't we vote for something that would put the Government in their shoes? Why don't we? Because that is the last thing in the world this administration wants because then they would have to answer to how many different people in the Bush administration broke the law.

I don't believe anybody is above the law. I don't believe the President is; I don't believe a Senator is; I don't believe anybody is. Keep in mind, as I said earlier, why we have FISA. Congress passed that law only after we discovered the shameful abuses of J. Edgar Hoover's FBI. Through the COINTEL Program—sometimes called COINTELPRO—Director Hoover spied on Americans who objected and spoke out against the war in Vietnam. I objected and spoke out against the war in Vietnam. Many Vermonters opposed that war. I wonder how many Vermonters were spied on for daring to speak out against it.

Ironically, Madam President, in April of 1975, the United States Senate voted by a one-vote margin in the Armed Services Committee to stop the war in Vietnam. A year later, it was hard to find anybody in this body who had supported it, although obviously an awful lot of Senators had.

Well, I wonder if we are going to look back that same way someday and ask: were we so frightened by 9/11 that we were willing to throw away everything this country fought for, everything that has made this country great through our history?

We can protect Americans' rights. We can protect those things our forefathers fought a revolution to obtain, that we fought a civil war to protect, that we fought two world wars to cement. We can protect ourselves. But we cannot protect ourselves if we do not protect our rights. Are we going to throw our rights away because of a group of terrorists? This Senator is not going to.

Let us show the American people and the world what America stands for. We can and will do all we can to secure the future for ourselves, our children, and our grandchildren. At the same time, we can protect the cherished rights and freedoms that define America and make this country different from all others. Those are the rights and freedoms that protected past generations and allow us to have an American future. If we do not protect them, what will we leave to our children and grandchildren?

Let us stand up for American values. Let us not be afraid to preserve our freedom while protecting our national security.

Madam President, I retain the remainder of my time, and I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The bill clerk proceeded to call the roll.

Mr. LEAHY. Madam President, I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER. Without objection, it is so ordered.

Mr. LEAHY. Madam President, I ask unanimous consent that the vote on passage of S. 2248, as amended, occur at 5:30 p.m. today, notwithstanding rule XII, paragraph 4, and that the time specified in the previous order remain in effect, with the time from 5:10 to 5:30 equally divided and controlled between the leaders, with the majority leader controlling the final 10 minutes.

The PRESIDING OFFICER. Without objection, it is so ordered.

Mr. LEAHY. Madam President, I yield back the remainder of my time, and I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The bill clerk proceeded to call the roll.

Mr. ROCKEFELLER. Madam President, I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER. Without objection, it is so ordered.

AMENDMENT NO. 4018 TO AMENDMENT NO. 3911

Mr. ROCKEFELLER. Madam President, I ask unanimous consent that the amendment at the desk making technical and conforming changes to the bill be in order, notwithstanding the adoption of the substitute amendment, and that the amendment be adopted. This consent request has been approved by both leaders.

The PRESIDING OFFICER. Is there objection?

Without objection, it is so ordered.

The amendment (No. 4018) was agreed to, as follows:

(Purpose: To make technical corrections)

On page 7, beginning on line 14, strike '', consistent with the requirements of section 101(h) or section 301(4), minimization procedures'' and insert ''minimization procedures that meet the definition of minimization procedures under section 101(h) or section 301(4)''.

On page 8, line 13, strike ''168 hours'' and insert ''7 days''.

On page 26, beginning on line 22, strike ''consistent with the requirements of section 101(h) or section 301(4)'' and insert ''that meet the definition of minimization procedures under section 101(h) or section 301(4)''.

On page 32, line 3, strike ''subsection (2)'' and insert ''subsection (b)''.

On page 35, line 6, strike ''obtained;'' and insert ''obtained,''.

On page 35, line 18, strike ''168 hours'' and insert ''7 days''.

On page 35, line 24, strike ''subsection'' and insert ''section''.

On page 36, line 6, strike ''168 hours'' and insert ''7 days''.

On page 36, line 16, strike ''168-hour'' and insert ''7-day''.

On page 40, beginning on line 16, strike ''consistent with the requirements of section 101(h) or section 301(4)'' and insert ''that meet the definition of minimization procedures under section 101(h) or section 301(4)''.

On page 44, line 15, strike ''clause'' and insert ''subparagraph''.

On page 45, line 15, strike ''obtained;'' and insert ''obtained,''.

On page 46, line 2, strike ''168 hours'' and insert ''7 days''.

On page 46, line 8, strike ''subsection'' and insert ''section''.

On page 46, lines 14 and 15, strike ''168 hours'' and insert ''7 days''.

On page 46, line 24, strike ''168-hour'' and insert ''7-day''.

On page 48, beginning on line 13, strike ''orders under section 704(b) or section 705(b)'' and insert ''orders under section 704(c) or section 705(c)''.

On page 54, beginning on line 22, strike ''during the period such directive was in effect'' and insert ''for information, facilities, or assistance provided during the period such directive was or is in effect''.

On page 60, line 4, strike ''reasonably''.

On page 60, line 5, strike ''determines'' and insert ''reasonably determines''.

On page 60, line 10, strike ''determines'' and insert ''reasonably determines''.

On page 60, lines 20 and 21, strike ''168 hours'' and insert ''7 days''.

On page 61, line 7, strike ''168 hours'' and insert ''7 days''.

On page 65, line 6, strike ''168 hours'' and insert ''7 days''.

On page 65, lines 16 and 17, strike ''168 hours'' and insert ''7 days''.

On page 67, line 2, strike ''168 hours'' and insert ''7 days''.

On page 67, line 4, strike ''168 hours'' and insert ''7 days''.

Mr. ROCKEFELLER. Madam President, after a long debate, we are, in fact, ready to, hopefully, pass the FISA bill. This has been an extremely important debate over important issues critical to the Nation's security.

As I discussed at the beginning of the debate, the guiding principle in bringing this bill to the Senate floor was to modernize our ability to collect communications intelligence against foreign targets without compromising the constitutional and statutory privacy protections afforded to all Americans. In my mind, we have achieved this goal.

Vice Chairman BOND and I worked very hard in the Intelligence Committee to produce a balanced and bipartisan bill. One can say whatever one wants, but 13 to 2 is 13 to 2. I think we can be proud of the improvements we have made to the bill each step of the way since last September. But, in fact, it goes all the way back almost a year. In the end, the bill we are about to pass, I hope, strengthens our national security and represents a very significant improvement over the Protect America Act that passed last summer.

Let me mention a few of the provisions we have included in the bill for protecting the rights of Americans here in the United States and overseas.

We require an individual FISA order for the targeting of U.S. persons believed to be located outside the United States any time the collection is conducted inside the United States.

We have also put in place for the first time a procedure requiring FISA Court approval for collection on United States persons outside of the United States in circumstances that would require a warrant if undertaken within the United States. This has never before existed. It now exists in the FISA law, if we do, in fact, pass it.

We have increased the role of the FISA Court in other significant ways, starting with the new requirement that the FISA Court approve the minimization procedures that are essential to the treatment of information concerning Americans authorized under this act. And thanks to Senator WHITEHOUSE's amendment adopted this morning, we have clarified that the FISA Court has inherent authority to enforce compliance with the procedures that it, and it alone, can approve.

We also adopted new requirements to give Congress visibility into how the new collection authority is being implemented, from the Feingold amendment on FISA Court documents, to the new requirements for reporting by the Attorney General and the Director of National Intelligence.

Just as we have worked on a bipartisan basis here in the Senate in order to achieve the strongest possible bill, I believe now is the time to work with our colleagues in the House of Representatives to achieve a true bipartisan, bicameral bill. I look forward to that dialog with our House colleagues.

I would note there are additional measures I support which may make this legislation even stronger. Among these would be the exclusivity amendment of Senator FEINSTEIN that received a strong bipartisan majority vote this morning. I think it was 57 votes. I commend her for all of her work she has done on this critical issue and on other parts of the bill, and I will fight like heck for her in the conference committee, if we are to have one. We will continue to work with her and with Vice Chairman BOND to see if there is any way to bridge the differences in the bipartisan manner that has dominated our negotiations throughout this procedure.

In closing, it would not have been possible to have reached this point without the hard work of the staff of the Intelligence and Judiciary Committees, as well as the leadership staff. From the Intelligence Committee, I thank Andy Johnson; Louis Tucker; Melvin Dubee; Michael Davidson; Jack Livingston; Christine Healey; Alissa Starzak; and Kathleen Rice. I also thank Mary DeRosa, Nick Rossi, Zulima Espinel, and Matt Solomon of the Judiciary Committee; and Ron Weich, Serena Hoy, and Marcel Lettre of the majority leader's staff.

Finally, I must recognize the steadfast support and work of the committee's vice chairman, Senator BOND. The work of the Intelligence Committee is not easy. When it comes on the floor, it is more difficult because there is a certain kind of exclusivity which is not appreciated by some Members but is the way it works.

Vice Chairman BOND has been dogged in his efforts to move this whole thing forward. He is formidable in his pursuit of intelligence and his insistence it be made available to the committee and to the appropriate committees; and he is flexible in his willingness to find compromises to keep our bipartisan coalition together.

I hope this bill does pass. I think it is landmark legislation. I don't think all will see it that way at the very beginning, and that is OK because what we do is not so much of the moment but for the longer term. So there may be disagreements on immunity. But, on the other hand, there can be no disagreements on the national security of the United States. Immunity has been narrowly tailored. A lot of people don't know that, or maybe made up their minds at the beginning, but, whatever, we did what we thought was the right thing to do.

One of the great things about being in this body is no matter what people say and what people think, if you do what you think is right, you are serving your country.

I thank the Presiding Officer and yield the floor.

I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The bill clerk proceeded to call the roll.

Mr. MCCONNELL. Madam President, I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER. Without objection, it is so ordered.

Mr. MCCONNELL. Madam President, are we now in my designated time?

The PRESIDING OFFICER. We are.

Mr. MCCONNELL. Madam President, earlier today the Senate voted to invoke cloture on the bipartisan Rockefeller-Bond bill. It was not a close vote. Rather, it was a strong bipartisan show of support for this important piece of legislation.

The Protect America Act expires at the end of this week. That is Saturday, February 16.

Twenty-one House Democrats have written to Speaker PELOSI saying they ''fully support'' the Rockefeller-Bond bill if it is not changed substantially—and it was not changed—and they urge her, the Speaker, to ''quickly consider'' the bill in order ''to get a bill signed into law before the Protect America Act expires in February.''

I have a copy of the letter signed by 21 Democrats, so-called Blue Dog Democrats, in the House. I ask unanimous consent that it be printed in the RECORD.

There being no objection, the material was ordered to be printed in the RECORD, as follows:

CONGRESS OF THE UNITED STATES,
Washington, DC, January 28, 2008.

DEAR MADAM SPEAKER: Legislation reforming the Foreign Intelligence Surveillance Act (FISA) is currently being considered by the Senate. Following the Senate's passage of a FISA bill, it will be necessary for the House to quickly consider FISA legislation

to get a bill to the President before the Protect America Act expires in February.

It is our belief that such legislation should include the following provisions: Require individualized warrants for surveillance of U.S. citizens living or traveling abroad; Clarify that no court order is required to conduct surveillance of foreign-to-foreign communications that are routed through the United States; Provide enhanced oversight by Congress of surveillance laws and procedures; Compel compliance by private sector partners; Review by FISA Court of minimization procedures; Targeted immunity for carriers that participated in anti-terrorism surveillance programs.

The Rockefeller-Bond FISA legislation contains satisfactory language addressing all these issues and we would fully support that measure should it reach the House floor without substantial change. We believe these components will ensure a strong national security apparatus that can thwart terrorism across the globe and save American lives here in our country.

It is also critical that we update the FISA laws in a timely manner. To pass a long-term extension of the Protect America Act, as some may suggest, would leave in place a limited, stopgap measure that does not fully address critical surveillance issues. We have it within our ability to replace the expiring Protect America Act by passing strong, bipartisan FISA modernization legislation that can be signed into law and we should do so—the consequences of not passing such a measure could place our national security at undue risk.

Sincerely,

Leonard L. Boswell, ———, Mike Ross, Bud Cramer, Heath Shuler, Allen Boyd, Dan Boren, Jim Matheson, Lincoln Davis, Tim Holden, Dennis Moore, Earl Pomeroy, Melissa L. Bean, John Barrow, Joe Baca, John Tanner, Jim Cooper, Zachary T. Space, Brad Ellsworth, Charlie Melancon, Christopher P. Carney.

Mr. MCCONNELL. Madam President, it is clear that not only does the Rockefeller-Bond bill enjoy bipartisan majority support in the Senate, it also enjoys bipartisan majority support in the House. It is a tribute to the fine work of the Senator from West Virginia, Mr. ROCKEFELLER, and the Senator from Missouri, Mr. BOND, in pulling this complex piece of legislation together and getting extraordinary support across the aisle.

This bill protects the country. It is a bill that will be signed by the President of the United States, so we are making a law here. We need to focus on completing action on this legislation and get it to the President before the Protect America Act expires.

As to further delays: Back in August, our Democratic colleagues said an additional 6 months was needed to get this right. In the fall, they said: We need a little more time. Last month, they said: Give us another 15 days and we can wrap it up. At this point, no Member of this body can reasonably state this piece of legislation was hastily or unfairly considered. It has been the product of 6 months' work, intense work on behalf of Senator ROCKEFELLER and Senator BOND.

We do not need yet another extension, yet another delay. We need to focus on getting our work done. I am confident that with the help of our friends on the other side of the aisle, we can get a second bipartisan accomplishment to the President in as many weeks. Tomorrow, he will sign the stimulus package—an important bipartisan accomplishment. Later in the week, he could conceivably be in a position to sign this important piece of bipartisan legislation.

I encourage my colleagues in the House and the Senate to redouble their efforts toward this end. That would show the American people that Congress can indeed function on a bipartisan basis on important issues before the country.

I am among those proud of the fine work done by Senator ROCKEFELLER and Senator BOND. This is a terrific, important piece of legislation. I know it will pass the Senate shortly, overwhelmingly.

I yield the floor.

I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The legislative clerk proceeded to call the roll.

Mr. BOND. Madam President, I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER. Without objection, it is so ordered.

Mr. BOND. Madam President, is there time remaining on this side prior to the vote?

The PRESIDING OFFICER. Four and a half minutes remain.

Mr. BOND. Madam President, with the sufferance of the minority leader, I thank my colleagues, especially Senator ROCKEFELLER, and all those who worked with us. We have had to make a number of very tough votes. We made some good changes in the bill. I thank, particularly, Senators WYDEN, FEINSTEIN, and WHITEHOUSE for working with us to achieve their objectives in a way that would allow the program to continue.

Approximately 10 months ago, the DNI, Admiral McConnell, came to Congress and asked that we update FISA. Changes in technology had resulted in the FISA Court rulings or interpretations that impeded the effective use of electronic surveillance against terrorists overseas.

This problem came to a head in May 2007, when there was a FISA Court ruling causing significant gaps in our intelligence collection against foreign terrorists. Throughout the summer of 2007 and amid growing concern of increased threats to our security in light of these gaps, Congress was asked by the DNI to act. And Congress, in August, passed the Protect America Act, a short-term fix that did what it was supposed to do. It was lacking in one important aspect; it did not provide civil liability protection to those private partners who assisted the intelligence community.

Following passage of the PAA, Chairman ROCKEFELLER and I immediately set to work to come up with a bipartisan permanent solution. We worked closely with the intelligence community.

In the end, after many hearings, briefings, debate, and visits to the facility, we did pass it on a 13-to-2 vote. We concluded that those electronic communication service providers that assisted with the President's TSP acted in good faith and deserve civil liability protection from frivolous lawsuits. As indicated by the chairman, this bill goes further than any legislation in history in protecting the privacy of U.S. persons, mostly Americans, whose communications may be acquired incidentally to this foreign targeting. For the first time in history, it requires the FISA Court to approve targeting of U.S. persons, American citizens, overseas to obtain foreign intelligence information.

This bill was a series of delicate compromises. Both sides had to give. Many of us would have preferred to have all litigation related to the TSP terminated as the DNI originally requested. Again, we agreed, for reasons set forth on the floor, that cases against Government officials—and all criminal cases—could go forward.

Others believed the FISA Court should not approve targeting of Americans abroad, particularly when these same protections are not afforded in ordinary criminal cases. In the spirit of compromise, we created a process that allows sufficient flexibility while addressing privacy concerns.

In the end, I am proud to say we have accomplished our collective goals of making sure we have a bill with clear authorities for foreign targeting, with strong protections for Americans, and with civil liability protection for those providers who may have assisted with the President's terrorist surveillance program.

We have heard debate over the past several weeks on a number of amendments that I believe would have proved harmful to our intelligence collection efforts. Some would have shut down, or severely impeded, intelligence collection against foreign terrorists. That is one of the reasons we worked so closely with the intelligence community to ascertain what could be done to increase protections without harming their ability to collect.

We now have a solid bill. The DNI will support it and the President can sign it into law. I urge my colleagues to send this bill to the House with a strong bipartisan vote. It gives our intelligence operators and law enforcement officials the tools they need to conduct surveillance of foreign terrorists in foreign countries who are planning to conduct attacks against the U.S., our troops, and our allies. It is a balance we need to protect our civil liberties, without handcuffing our intelligence professionals.

I hope we can do the right thing and pass the bill. I thank all our colleagues who helped.

I yield the floor.

The PRESIDING OFFICER. The majority leader is recognized.

Mr. REID. Madam President, I want the RECORD to reflect that any of my remarks where I disagree with the bill before the Senate in no way reflects upon the chairman of the committee. I have known JAY ROCKEFELLER for several decades, and I have not known a better public servant than JAY. JAY ROCKEFELLER got into Government for the right reasons. We know that the Rockefeller name is magic, that he could have led a life of leisure, doing many different things. But he chose public service. He went to West Virginia doing work as a VISTA volunteer. He fell in love with the people—the poor people—of West Virginia and has worked since then to improve the lives of the people of West Virginia. He has done a wonderful job there, serving as the secretary of state, Governor, and now as a long-time Senator.

There are certain things in this legislation that I disagree with. But I repeat, as a public servant, there is not one better—or I doubt that there ever has been anyone better than JAY ROCKEFELLER. He has devoted his Senate life in service to the Intelligence Committee. He devotes night and day not only working in the Committee room where there is no exposure to the public—he gets no publicity for doing this. He does it because he believes it is the right thing for the country. Of course, I receive calls from him well after hours on concerns he has in dealing with foreign intelligence generally.

I already voted against it on the FISA legislation, and I will vote ''no'' on final passage of the bill.

The Senate's debate on FISA has made the Intelligence Committee's bill better—no question about that—by adding a number of protections from the Judiciary Committee's version.

The Senate adopted amendments offered by Senators KENNEDY, WHITEHOUSE, and FEINGOLD to improve title I of the bill. This concerns the procedures we use to conduct this kind of surveillance in the future. That is an improvement. But the Senate rejected amendments to strike and modify various parts of title I, to improve title I, and rejected all amendments to strike or modify title II concerning immunity for telecommunications companies that may have broken the law by abiding the White House's requests for warrantless wiretaps on American citizens.

I believe the White House and any companies that broke the law must be held accountable.

In their unyielding effort to expand Presidential powers, President Bush and Vice President CHENEY created a system to conduct wiretapping—including on American citizens—outside the bounds of longstanding Federal law.

As I have said before—and books have been written on it—the President, as soon as we passed the first PATRIOT Act, after he joined with us in celebrating it, he basically ignored it and did whatever he wanted to do because he was told by the White House staff he was above the law, he didn't have to follow the law we passed.

The President could have taken the simple step at any time of requesting new authority from Congress. All he would have had to do was come talk to us. We would have been willing to listen to him and, very likely, would have done anything he wanted to do. After all, Congress has repeatedly amended FISA because of new technology and legitimate needs in the intelligence community.

But whether out of convenience, incompetence, or outright disdain for the rule of law, the Bush-Cheney administration chose to ignore Congress and ignore the Constitution.

The White House should bear responsibility for this reckless disdain for the rule of law.

It also appears that many companies followed the administration's orders without regard to the law or privacy, or even basic common sense. I always will support giving our intelligence community the tools it needs to collect intelligence on terrorists and other foreign targets. We have to do that.

We always have and always will need to help in the private sector to protect our country. That is clear. When companies comply with legal and constitutional directives to support intelligence and law enforcement activities, they have no reason to fear. But the requirement and obligation they have for protecting the rights of American citizens and the Constitution and FISA are perfectly clear, very clear.

According to the press reports, at least one company—Qwest Communications Company—refused the White House request to participate in this program. The others had an opportunity to do the same. As far as we know, they chose not to. They didn't follow the example of Qwest.

If the Senate had voted today to reject amnesty, we would have sent a message that no one is above accountability and no one is above the law. If we had rejected amnesty, we would have sent a message that fighting terrorism doesn't require the sacrifice of basic fundamental rights.

I was disappointed that the Senate rejected amendments opposing immunity. Even though their efforts were unsuccessful, all Americans owe a debt of gratitude to two outstanding and principled Senators, Senators FEINGOLD and DODD. I don't mean in any way to suggest that people who disagree with them are not outstanding or are unprincipled. That isn't the case. There is a basic disagreement. I felt I needed to applaud and commend these two men for how hard they worked in making their point. I believe they stood up to the administration, which certainly needs standing up to. They stood up for accountability.

Despite today's votes, there is no doubt in my mind that history will prove they were right. Millions of Americans joined this effort. Win or lose, their voices were heard and their efforts made a difference.

If the Senate votes for final passage of FISA today, which I suspect will be the case, we must decide what comes next. The mere fact that we pass something today, and the House passed something previously, doesn't mean we have anything to send to the President.

Two weeks ago, in the runup to the State of the Union Address—and we have heard it time and again—the President and Vice President and Senate Republicans believed it was urgent to pass the FISA bill, that it is critical to our national security. But then, Senate Republicans spent most of the time since then refusing to allow any votes on FISA amendments, slow-walking the bill as part of a strategy to jam the House. That is what happened. I have to suggest that they deserve a pin on their lapel because they set out and did what they wanted to do—stall this as long as they could.

A week and a half ago, as the February 1 sunset to the Protect America Act approached, we passed a 15-day extension. This would have allowed 2 weeks to negotiate with the House, which would have been rushed, but we could have at least had meaningful meetings. Those will not take place.

Unfortunately, the White House has been convinced that if they dragged this process out long enough, there would not be enough time to negotiate a bill with the House. The White House is convinced they can force the House to pass exactly the bill they want. I believe it is wrong for the White House to do this, and I believe it is unfair to the House of Representatives.

Due to months of White House foot-dragging, the relevant House committees have only just gotten the documents relating to immunity. They need some time to review and analyze that.

We must not let this critical issue be resolved by the White House trying to force the House to do something they didn't want to do, such as happened last August.

I plan to ask, after this legislation passes today, unanimous consent for an extension in order to allow sufficient time for negotiation with the House. My friend, the distinguished Republican leader, has already said there will be no extensions given. I hope that is not the case, and with this extra time, the conference committee can make further improvements to this critical bill.

Why do we need to improve the bill?

Richard Clarke, a national security adviser to Presidents Reagan, Bush Sr., and President Clinton, said it well in an op-ed:

> FISA has and still works as the most valuable mechanism for monitoring our enemies.
>
> In order to defeat the violent Islamic extremists who do not believe in human rights, we need not give up the civil liberties, constitutional rights and protections that generations of Americans fought to achieve.

The Bush-Cheney White House continues to sell us a false choice between

security and liberty. I reject that choice.

This is America and we are Americans. We can and must have both liberty and security.

It is my understanding we are ready to vote on final passage.

The PRESIDING OFFICER. The question is on passage of S. 2248, as amended.

Mr. BOND. I ask for the yeas and nays.

The PRESIDING OFFICER. Is there a second?

There appears to be a sufficient second.

The clerk will call the roll.

The legislative clerk called the roll.

Mr. DURBIN. I announce that the Senator from New York (Mrs. CLINTON) and the Senator from Illinois (Mr. OBAMA) are necessarily absent.

Mr. KYL. The following Senator is necessarily absent: the Senator from South Carolina (Mr. GRAHAM).

Further, if present and voting, the Senator from South Carolina (Mr. GRAHAM) would have voted ''yea.''

The result was announced—yeas 68, nays 29, as follows:

[Rollcall Vote No. 20 Leg.]

YEAS—68

Alexander	Dole	Mikulski
Allard	Domenici	Murkowski
Barrasso	Ensign	Nelson (FL)
Baucus	Enzi	Nelson (NE)
Bayh	Grassley	Pryor
Bennett	Gregg	Roberts
Bond	Hagel	Rockefeller
Brownback	Hatch	Salazar
Bunning	Hutchison	Sessions
Burr	Inhofe	Shelby
Carper	Inouye	Smith
Casey	Isakson	Snowe
Chambliss	Johnson	Specter
Coburn	Kohl	Stevens
Cochran	Kyl	Sununu
Coleman	Landrieu	Thune
Collins	Lieberman	Vitter
Conrad	Lincoln	Voinovich
Corker	Lugar	Warner
Cornyn	Martinez	Webb
Craig	McCain	Whitehouse
Crapo	McCaskill	Wicker
DeMint	McConnell	

NAYS—29

Akaka	Durbin	Menendez
Biden	Feingold	Murray
Bingaman	Feinstein	Reed
Boxer	Harkin	Reid
Brown	Kennedy	Sanders
Byrd	Kerry	Schumer
Cantwell	Klobuchar	Stabenow
Cardin	Lautenberg	Tester
Dodd	Leahy	Wyden
Dorgan	Levin	

NOT VOTING—3

Clinton	Graham	Obama

The bill (S. 2248), as amended, was passed.

The PRESIDING OFFICER. Under the previous order, the Senate will proceed to the consideration of H.R. 3773, which the clerk will report.

The legislative clerk read as follows:

A bill (H.R. 3773) to amend the Foreign Intelligence Surveillance Act of 1978 to establish a procedure for authorizing certain acquisitions of foreign intelligence, and for other purposes.

The PRESIDING OFFICER. Under the previous order, all after the enacting clause is stricken and the text of S. 2248, as amended, is inserted in lieu thereof; the bill, as amended, is considered read the third time and passed, the motion to reconsider made and laid upon the table, and passage of S. 2248 vitiated and that bill be returned to the calendar.

The bill (H.R. 3773), as amended, was passed, as follows:

H.R. 3773

Resolved, That the bill from the House of Representatives (H.R. 3773) entitled ''An Act to amend the Foreign Intelligence Surveillance Act of 1978 to establish a procedure for authorizing certain acquisitions of foreign intelligence, and for other purposes.'', do pass with the following amendment:

Strike out all after the enacting clause and insert:

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the ''Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008'' or the ''FISA Amendments Act of 2008''.

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

Sec. 1. Short title; table of contents.

TITLE I—FOREIGN INTELLIGENCE SURVEILLANCE

Sec. 101. Additional procedures regarding certain persons outside the United States.
Sec. 102. Statement of exclusive means by which electronic surveillance and interception of domestic communications may be conducted.
Sec. 103. Submittal to Congress of certain court orders under the Foreign Intelligence Surveillance Act of 1978.
Sec. 104. Applications for court orders.
Sec. 105. Issuance of an order.
Sec. 106. Use of information.
Sec. 107. Amendments for physical searches.
Sec. 108. Amendments for emergency pen registers and trap and trace devices.
Sec. 109. Foreign Intelligence Surveillance Court.
Sec. 110. Weapons of mass destruction.
Sec. 111. Technical and conforming amendments.

TITLE II—PROTECTIONS FOR ELECTRONIC COMMUNICATION SERVICE PROVIDERS

Sec. 201. Definitions.
Sec. 202. Limitations on civil actions for electronic communication service providers.
Sec. 203. Procedures for implementing statutory defenses under the Foreign Intelligence Surveillance Act of 1978.
Sec. 204. Preemption of State investigations.
Sec. 205. Technical amendments.

TITLE III—OTHER PROVISIONS

Sec. 301. Severability.
Sec. 302. Effective date; repeal; transition procedures.

TITLE I—FOREIGN INTELLIGENCE SURVEILLANCE

SEC. 101. ADDITIONAL PROCEDURES REGARDING CERTAIN PERSONS OUTSIDE THE UNITED STATES.

(a) IN GENERAL.—The Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is amended—

(1) by striking title VII; and

(2) by adding after title VI the following new title:

''TITLE VII—ADDITIONAL PROCEDURES REGARDING CERTAIN PERSONS OUTSIDE THE UNITED STATES

''SEC. 701. LIMITATION ON DEFINITION OF ELECTRONIC SURVEILLANCE.

''Nothing in the definition of electronic surveillance under section 101(f) shall be construed to encompass surveillance that is targeted in accordance with this title at a person reasonably believed to be located outside the United States.

''SEC. 702. DEFINITIONS.

''(a) IN GENERAL.—The terms 'agent of a foreign power', 'Attorney General', 'contents', 'electronic surveillance', 'foreign intelligence information', 'foreign power', 'minimization procedures', 'person', 'United States', and 'United States person' shall have the meanings given such terms in section 101, except as specifically provided in this title.

''(b) ADDITIONAL DEFINITIONS.—

''(1) CONGRESSIONAL INTELLIGENCE COMMITTEES.—The term 'congressional intelligence committees' means—

''(A) the Select Committee on Intelligence of the Senate; and

''(B) the Permanent Select Committee on Intelligence of the House of Representatives.

''(2) FOREIGN INTELLIGENCE SURVEILLANCE COURT; COURT.—The terms 'Foreign Intelligence Surveillance Court' and 'Court' mean the court established by section 103(a).

''(3) FOREIGN INTELLIGENCE SURVEILLANCE COURT OF REVIEW; COURT OF REVIEW.—The terms 'Foreign Intelligence Surveillance Court of Review' and 'Court of Review' mean the court established by section 103(b).

''(4) ELECTRONIC COMMUNICATION SERVICE PROVIDER.—The term 'electronic communication service provider' means—

''(A) a telecommunications carrier, as that term is defined in section 3 of the Communications Act of 1934 (47 U.S.C. 153);

''(B) a provider of electronic communication service, as that term is defined in section 2510 of title 18, United States Code;

''(C) a provider of a remote computing service, as that term is defined in section 2711 of title 18, United States Code;

''(D) any other communication service provider who has access to wire or electronic communications either as such communications are transmitted or as such communications are stored; or

''(E) an officer, employee, or agent of an entity described in subparagraph (A), (B), (C), or (D).

''(5) ELEMENT OF THE INTELLIGENCE COMMUNITY.—The term 'element of the intelligence community' means an element of the intelligence community specified in or designated under section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4)).

''SEC. 703. PROCEDURES FOR TARGETING CERTAIN PERSONS OUTSIDE THE UNITED STATES OTHER THAN UNITED STATES PERSONS.

''(a) AUTHORIZATION.—Notwithstanding any other law, the Attorney General and the Director of National Intelligence may authorize jointly, for periods of up to 1 year, the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information.

''(b) LIMITATIONS.—An acquisition authorized under subsection (a)—

''(1) may not intentionally target any person known at the time of acquisition to be located in the United States;

''(2) may not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States, except in accordance with title I or title III;

''(3) may not intentionally target a United States person reasonably believed to be located outside the United States, except in accordance with sections 704, 705, or 706;

''(4) shall not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States; and

''(5) shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States.

''(c) CONDUCT OF ACQUISITION.—An acquisition authorized under subsection (a) may be conducted only in accordance with—

''(1) a certification made by the Attorney General and the Director of National Intelligence pursuant to subsection (f); and

''(2) the targeting and minimization procedures required pursuant to subsections (d) and (e).

''(d) TARGETING PROCEDURES.—

''(1) REQUIREMENT TO ADOPT.—The Attorney General, in consultation with the Director of National Intelligence, shall adopt targeting procedures that are reasonably designed to ensure that any acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be located outside the United States and does not result in the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States.

''(2) JUDICIAL REVIEW.—The procedures referred to in paragraph (1) shall be subject to judicial review pursuant to subsection (h).

''(e) MINIMIZATION PROCEDURES.—

''(1) REQUIREMENT TO ADOPT.—The Attorney General, in consultation with the Director of National Intelligence, shall adopt minimization procedures that meet the definition of minimization procedures under section 101(h) or section 301(4) for acquisitions authorized under subsection (a).

''(2) JUDICIAL REVIEW.—The minimization procedures required by this subsection shall be subject to judicial review pursuant to subsection (h).

''(f) CERTIFICATION.—

''(1) IN GENERAL.—

''(A) REQUIREMENT.—Subject to subparagraph (B), prior to the initiation of an acquisition authorized under subsection (a), the Attorney General and the Director of National Intelligence shall provide, under oath, a written certification, as described in this subsection.

''(B) EXCEPTION.—If the Attorney General and the Director of National Intelligence determine that immediate action by the Government is required and time does not permit the preparation of a certification under this subsection prior to the initiation of an acquisition, the Attorney General and the Director of National Intelligence shall prepare such certification, including such determination, as soon as possible but in no event more than 7 days after such determination is made.

''(2) REQUIREMENTS.—A certification made under this subsection shall—

''(A) attest that—

''(i) there are reasonable procedures in place for determining that the acquisition authorized under subsection (a) is targeted at persons reasonably believed to be located outside the United States and that such procedures have been approved by, or will be submitted in not more than 5 days for approval by, the Foreign Intelligence Surveillance Court pursuant to subsection (h);

''(ii) there are reasonable procedures in place for determining that the acquisition authorized under subsection (a) does not result in the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States, and that such procedures have been approved by, or will be submitted in not more than 5 days for approval by, the Foreign Intelligence Surveillance Court pursuant to subsection (h);

''(iii) the procedures referred to in clauses (i) and (ii) are consistent with the requirements of the fourth amendment to the Constitution of the United States and do not permit the intentional targeting of any person who is known at the time of acquisition to be located in the United States or the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States;

''(iv) a significant purpose of the acquisition is to obtain foreign intelligence information;

''(v) the minimization procedures to be used with respect to such acquisition—

''(I) meet the definition of minimization procedures under section 101(h) or section 301(4); and

''(II) have been approved by, or will be submitted in not more than 5 days for approval by, the Foreign Intelligence Surveillance Court pursuant to subsection (h);

''(vi) the acquisition involves obtaining the foreign intelligence information from or with the assistance of an electronic communication service provider; and

''(vii) the acquisition does not constitute electronic surveillance, as limited by section 701; and

''(B) be supported, as appropriate, by the affidavit of any appropriate official in the area of national security who is—

''(i) appointed by the President, by and with the consent of the Senate; or

''(ii) the head of any element of the intelligence community.

''(3) LIMITATION.—A certification made under this subsection is not required to identify the specific facilities, places, premises, or property at which the acquisition authorized under subsection (a) will be directed or conducted.

''(4) SUBMISSION TO THE COURT.—The Attorney General shall transmit a copy of a certification made under this subsection, and any supporting affidavit, under seal to the Foreign Intelligence Surveillance Court as soon as possible, but in no event more than 5 days after such certification is made. Such certification shall be maintained under security measures adopted by the Chief Justice of the United States and the Attorney General, in consultation with the Director of National Intelligence.

''(5) REVIEW.—The certification required by this subsection shall be subject to judicial review pursuant to subsection (h).

''(g) DIRECTIVES AND JUDICIAL REVIEW OF DIRECTIVES.—

''(1) AUTHORITY.—With respect to an acquisition authorized under subsection (a), the Attorney General and the Director of National Intelligence may direct, in writing, an electronic communication service provider to—

''(A) immediately provide the Government with all information, facilities, or assistance necessary to accomplish the acquisition in a manner that will protect the secrecy of the acquisition and produce a minimum of interference with the services that such electronic communication service provider is providing to the target; and

''(B) maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning the acquisition or the aid furnished that such electronic communication service provider wishes to maintain.

''(2) COMPENSATION.—The Government shall compensate, at the prevailing rate, an electronic communication service provider for providing information, facilities, or assistance pursuant to paragraph (1).

''(3) RELEASE FROM LIABILITY.—Notwithstanding any other law, no cause of action shall lie in any court against any electronic communication service provider for providing any information, facilities, or assistance in accordance with a directive issued pursuant to paragraph (1).

''(4) CHALLENGING OF DIRECTIVES.—

''(A) AUTHORITY TO CHALLENGE.—An electronic communication service provider receiving a directive issued pursuant to paragraph (1) may challenge the directive by filing a petition with the Foreign Intelligence Surveillance Court, which shall have jurisdiction to review such a petition.

''(B) ASSIGNMENT.—The presiding judge of the Court shall assign the petition filed under subparagraph (A) to 1 of the judges serving in the pool established by section 103(e)(1) not later than 24 hours after the filing of the petition.

''(C) STANDARDS FOR REVIEW.—A judge considering a petition to modify or set aside a directive may grant such petition only if the judge finds that the directive does not meet the requirements of this section, or is otherwise unlawful.

''(D) PROCEDURES FOR INITIAL REVIEW.—A judge shall conduct an initial review not later than 5 days after being assigned a petition described in subparagraph (C). If the judge determines that the petition consists of claims, defenses, or other legal contentions that are not warranted by existing law or by a nonfrivolous argument for extending, modifying, or reversing existing law or for establishing new law, the judge shall immediately deny the petition and affirm the directive or any part of the directive that is the subject of the petition and order the recipient to comply with the directive or any part of it. Upon making such a determination or promptly thereafter, the judge shall provide a written statement for the record of the reasons for a determination under this subparagraph.

''(E) PROCEDURES FOR PLENARY REVIEW.—If a judge determines that a petition described in subparagraph (C) requires plenary review, the judge shall affirm, modify, or set aside the directive that is the subject of that petition not later than 30 days after being assigned the petition, unless the judge, by order for reasons stated, extends that time as necessary to comport with the due process clause of the fifth amendment to the Constitution of the United States. Unless the judge sets aside the directive, the judge shall immediately affirm or affirm with modifications the directive, and order the recipient to comply with the directive in its entirety or as modified. The judge shall provide a written statement for the records of the reasons for a determination under this subparagraph.

''(F) CONTINUED EFFECT.—Any directive not explicitly modified or set aside under this paragraph shall remain in full effect.

''(G) CONTEMPT OF COURT.—Failure to obey an order of the Court issued under this paragraph may be punished by the Court as contempt of court.

''(5) ENFORCEMENT OF DIRECTIVES.—

''(A) ORDER TO COMPEL.—In the case of a failure to comply with a directive issued pursuant to paragraph (1), the Attorney General may file a petition for an order to compel compliance with the directive with the Foreign Intelligence Surveillance Court, which shall have jurisdiction to review such a petition.

''(B) ASSIGNMENT.—The presiding judge of the Court shall assign a petition filed under subparagraph (A) to 1 of the judges serving in the pool established by section 103(e)(1) not later than 24 hours after the filing of the petition.

''(C) STANDARDS FOR REVIEW.—A judge considering a petition filed under subparagraph (A) shall issue an order requiring the electronic communication service provider to comply with the directive or any part of it, as issued or as modified, if the judge finds that the directive meets the requirements of this section, and is otherwise lawful.

''(D) PROCEDURES FOR REVIEW.—The judge shall render a determination not later than 30 days after being assigned a petition filed under subparagraph (A), unless the judge, by order for reasons stated, extends that time if necessary to comport with the due process clause of the fifth amendment to the Constitution of the United States. The judge shall provide a written statement for the record of the reasons for a determination under this paragraph.

''(E) CONTEMPT OF COURT.—Failure to obey an order of the Court issued under this paragraph may be punished by the Court as contempt of court.

''(F) PROCESS.—Any process under this paragraph may be served in any judicial district in which the electronic communication service provider may be found.

''(6) APPEAL.—

''(A) APPEAL TO THE COURT OF REVIEW.—The Government or an electronic communication

service provider receiving a directive issued pursuant to paragraph (1) may file a petition with the Foreign Intelligence Surveillance Court of Review for review of the decision issued pursuant to paragraph (4) or (5). The Court of Review shall have jurisdiction to consider such a petition and shall provide a written statement for the record of the reasons for a decision under this paragraph.

''(B) CERTIORARI TO THE SUPREME COURT.—The Government or an electronic communication service provider receiving a directive issued pursuant to paragraph (1) may file a petition for a writ of certiorari for review of the decision of the Court of Review issued under subparagraph (A). The record for such review shall be transmitted under seal to the Supreme Court of the United States, which shall have jurisdiction to review such decision.

''(h) JUDICIAL REVIEW OF CERTIFICATIONS AND PROCEDURES.—

''(1) IN GENERAL.—

''(A) REVIEW BY THE FOREIGN INTELLIGENCE SURVEILLANCE COURT.—The Foreign Intelligence Surveillance Court shall have jurisdiction to review any certification required by subsection (c) and the targeting and minimization procedures adopted pursuant to subsections (d) and (e).

''(B) SUBMISSION TO THE COURT.—The Attorney General shall submit to the Court any such certification or procedure, or amendment thereto, not later than 5 days after making or amending the certification or adopting or amending the procedures.

''(2) CERTIFICATIONS.—The Court shall review a certification provided under subsection (f) to determine whether the certification contains all the required elements.

''(3) TARGETING PROCEDURES.—The Court shall review the targeting procedures required by subsection (d) to assess whether the procedures are reasonably designed to ensure that the acquisition authorized under subsection (a) is limited to the targeting of persons reasonably believed to be located outside the United States and does not result in the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States.

''(4) MINIMIZATION PROCEDURES.—The Court shall review the minimization procedures required by subsection (e) to assess whether such procedures meet the definition of minimization procedures under section 101(h) or section 301(4).

''(5) ORDERS.—

''(A) APPROVAL.—If the Court finds that a certification required by subsection (f) contains all of the required elements and that the targeting and minimization procedures required by subsections (d) and (e) are consistent with the requirements of those subsections and with the fourth amendment to the Constitution of the United States, the Court shall enter an order approving the continued use of the procedures for the acquisition authorized under subsection (a).

''(B) CORRECTION OF DEFICIENCIES.—If the Court finds that a certification required by subsection (f) does not contain all of the required elements, or that the procedures required by subsections (d) and (e) are not consistent with the requirements of those subsections or the fourth amendment to the Constitution of the United States, the Court shall issue an order directing the Government to, at the Government's election and to the extent required by the Court's order—

''(i) correct any deficiency identified by the Court's order not later than 30 days after the date the Court issues the order; or

''(ii) cease the acquisition authorized under subsection (a).

''(C) REQUIREMENT FOR WRITTEN STATEMENT.—In support of its orders under this subsection, the Court shall provide, simultaneously with the orders, for the record a written statement of its reasons.

''(6) APPEAL.—

''(A) APPEAL TO THE COURT OF REVIEW.—The Government may appeal any order under this section to the Foreign Intelligence Surveillance Court of Review, which shall have jurisdiction to review such order. For any decision affirming, reversing, or modifying an order of the Foreign Intelligence Surveillance Court, the Court of Review shall provide for the record a written statement of its reasons.

''(B) CONTINUATION OF ACQUISITION PENDING REHEARING OR APPEAL.—Any acquisitions affected by an order under paragraph (5)(B) may continue—

''(i) during the pendency of any rehearing of the order by the Court en banc; and

''(ii) if the Government appeals an order under this section, until the Court of Review enters an order under subparagraph (C).

''(C) IMPLEMENTATION PENDING APPEAL.—Not later than 60 days after the filing of an appeal of an order under paragraph (5)(B) directing the correction of a deficiency, the Court of Review shall determine, and enter a corresponding order regarding, whether all or any part of the correction order, as issued or modified, shall be implemented during the pendency of the appeal.

''(D) CERTIORARI TO THE SUPREME COURT.—The Government may file a petition for a writ of certiorari for review of a decision of the Court of Review issued under subparagraph (A). The record for such review shall be transmitted under seal to the Supreme Court of the United States, which shall have jurisdiction to review such decision.

''(i) EXPEDITED JUDICIAL PROCEEDINGS.—Judicial proceedings under this section shall be conducted as expeditiously as possible.

''(j) MAINTENANCE AND SECURITY OF RECORDS AND PROCEEDINGS.—

''(1) STANDARDS.—A record of a proceeding under this section, including petitions filed, orders granted, and statements of reasons for decision, shall be maintained under security measures adopted by the Chief Justice of the United States, in consultation with the Attorney General and the Director of National Intelligence.

''(2) FILING AND REVIEW.—All petitions under this section shall be filed under seal. In any proceedings under this section, the court shall, upon request of the Government, review ex parte and in camera any Government submission, or portions of a submission, which may include classified information.

''(3) RETENTION OF RECORDS.—A directive made or an order granted under this section shall be retained for a period of not less than 10 years from the date on which such directive or such order is made.

''(k) ASSESSMENTS AND REVIEWS.—

''(1) SEMIANNUAL ASSESSMENT.—Not less frequently than once every 6 months, the Attorney General and Director of National Intelligence shall assess compliance with the targeting and minimization procedures required by subsections (e) and (f) and shall submit each such assessment to—

''(A) the Foreign Intelligence Surveillance Court; and

''(B) the congressional intelligence committees.

''(2) AGENCY ASSESSMENT.—The Inspectors General of the Department of Justice and of any element of the intelligence community authorized to acquire foreign intelligence information under subsection (a) with respect to their department, agency, or element—

''(A) are authorized to review the compliance with the targeting and minimization procedures required by subsections (d) and (e);

''(B) with respect to acquisitions authorized under subsection (a), shall review the number of disseminated intelligence reports containing a reference to a United States person identity and the number of United States person identities subsequently disseminated by the element concerned in response to requests for identities that were not referred to by name or title in the original reporting;

''(C) with respect to acquisitions authorized under subsection (a), shall review the number of targets that were later determined to be located in the United States and, to the extent possible, whether their communications were reviewed; and

''(D) shall provide each such review to—

''(i) the Attorney General;

''(ii) the Director of National Intelligence; and

''(iii) the congressional intelligence committees.

''(3) ANNUAL REVIEW.—

''(A) REQUIREMENT TO CONDUCT.—The head of an element of the intelligence community conducting an acquisition authorized under subsection (a) shall direct the element to conduct an annual review to determine whether there is reason to believe that foreign intelligence information has been or will be obtained from the acquisition. The annual review shall provide, with respect to such acquisitions authorized under subsection (a)—

''(i) an accounting of the number of disseminated intelligence reports containing a reference to a United States person identity;

''(ii) an accounting of the number of United States person identities subsequently disseminated by that element in response to requests for identities that were not referred to by name or title in the original reporting;

''(iii) the number of targets that were later determined to be located in the United States and, to the extent possible, whether their communications were reviewed; and

''(iv) a description of any procedures developed by the head of an element of the intelligence community and approved by the Director of National Intelligence to assess, in a manner consistent with national security, operational requirements and the privacy interests of United States persons, the extent to which the acquisitions authorized under subsection (a) acquire the communications of United States persons, as well as the results of any such assessment.

''(B) USE OF REVIEW.—The head of each element of the intelligence community that conducts an annual review under subparagraph (A) shall use each such review to evaluate the adequacy of the minimization procedures utilized by such element or the application of the minimization procedures to a particular acquisition authorized under subsection (a).

''(C) PROVISION OF REVIEW.—The head of each element of the intelligence community that conducts an annual review under subparagraph (A) shall provide such review to—

''(i) the Foreign Intelligence Surveillance Court;

''(ii) the Attorney General;

''(iii) the Director of National Intelligence; and

''(iv) the congressional intelligence committees.

"SEC. 704. CERTAIN ACQUISITIONS INSIDE THE UNITED STATES OF UNITED STATES PERSONS OUTSIDE THE UNITED STATES.

''(a) JURISDICTION OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT.—

''(1) IN GENERAL.—The Foreign Intelligence Surveillance Court shall have jurisdiction to enter an order approving the targeting of a United States person reasonably believed to be located outside the United States to acquire foreign intelligence information, if such acquisition constitutes electronic surveillance (as defined in section 101(f), regardless of the limitation of section 701) or the acquisition of stored electronic communications or stored electronic data that requires an order under this Act, and such acquisition is conducted within the United States.

''(2) LIMITATION.—In the event that a United States person targeted under this subsection is reasonably believed to be located in the United States during the pendency of an order issued pursuant to subsection (c), such acquisition shall cease until authority, other than under this section, is obtained pursuant to this Act or

the targeted United States person is again reasonably believed to be located outside the United States during the pendency of an order issued pursuant to subsection (c).

''(b) APPLICATION.—

''(1) IN GENERAL.—Each application for an order under this section shall be made by a Federal officer in writing upon oath or affirmation to a judge having jurisdiction under subsection (a)(1). Each application shall require the approval of the Attorney General based upon the Attorney General's finding that it satisfies the criteria and requirements of such application, as set forth in this section, and shall include—

''(A) the identity of the Federal officer making the application;

''(B) the identity, if known, or a description of the United States person who is the target of the acquisition;

''(C) a statement of the facts and circumstances relied upon to justify the applicant's belief that the United States person who is the target of the acquisition is—

''(i) a person reasonably believed to be located outside the United States; and

''(ii) a foreign power, an agent of a foreign power, or an officer or employee of a foreign power;

''(D) a statement of the proposed minimization procedures that meet the definition of minimization procedures under section 101(h) or section 301(4);

''(E) a description of the nature of the information sought and the type of communications or activities to be subjected to acquisition;

''(F) a certification made by the Attorney General or an official specified in section 104(a)(6) that—

''(i) the certifying official deems the information sought to be foreign intelligence information;

''(ii) a significant purpose of the acquisition is to obtain foreign intelligence information;

''(iii) such information cannot reasonably be obtained by normal investigative techniques;

''(iv) designates the type of foreign intelligence information being sought according to the categories described in section 101(e); and

''(v) includes a statement of the basis for the certification that—

''(I) the information sought is the type of foreign intelligence information designated; and

''(II) such information cannot reasonably be obtained by normal investigative techniques;

''(G) a summary statement of the means by which the acquisition will be conducted and whether physical entry is required to effect the acquisition;

''(H) the identity of any electronic communication service provider necessary to effect the acquisition, provided, however, that the application is not required to identify the specific facilities, places, premises, or property at which the acquisition authorized under this section will be directed or conducted;

''(I) a statement of the facts concerning any previous applications that have been made to any judge of the Foreign Intelligence Surveillance Court involving the United States person specified in the application and the action taken on each previous application; and

''(J) a statement of the period of time for which the acquisition is required to be maintained, provided that such period of time shall not exceed 90 days per application.

''(2) OTHER REQUIREMENTS OF THE ATTORNEY GENERAL.—The Attorney General may require any other affidavit or certification from any other officer in connection with the application.

''(3) OTHER REQUIREMENTS OF THE JUDGE.—The judge may require the applicant to furnish such other information as may be necessary to make the findings required by subsection (c)(1).

''(c) ORDER.—

''(1) FINDINGS.—Upon an application made pursuant to subsection (b), the Foreign Intelligence Surveillance Court shall enter an ex parte order as requested or as modified approving the acquisition if the Court finds that—

''(A) the application has been made by a Federal officer and approved by the Attorney General;

''(B) on the basis of the facts submitted by the applicant, for the United States person who is the target of the acquisition, there is probable cause to believe that the target is—

''(i) a person reasonably believed to be located outside the United States; and

''(ii) a foreign power, an agent of a foreign power, or an officer or employee of a foreign power;

''(C) the proposed minimization procedures meet the definition of minimization procedures under section 101(h) or section 301(4); and

''(D) the application which has been filed contains all statements and certifications required by subsection (b) and the certification or certifications are not clearly erroneous on the basis of the statement made under subsection (b)(1)(F)(v) and any other information furnished under subsection (b)(3).

''(2) PROBABLE CAUSE.—In determining whether or not probable cause exists for purposes of an order under paragraph (1), a judge having jurisdiction under subsection (a)(1) may consider past activities of the target, as well as facts and circumstances relating to current or future activities of the target. However, no United States person may be considered a foreign power, agent of a foreign power, or officer or employee of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

''(3) REVIEW.—

''(A) LIMITATION ON REVIEW.—Review by a judge having jurisdiction under subsection (a)(1) shall be limited to that required to make the findings described in paragraph (1).

''(B) REVIEW OF PROBABLE CAUSE.—If the judge determines that the facts submitted under subsection (b) are insufficient to establish probable cause to issue an order under paragraph (1), the judge shall enter an order so stating and provide a written statement for the record of the reasons for such determination. The Government may appeal an order under this clause pursuant to subsection (f).

''(C) REVIEW OF MINIMIZATION PROCEDURES.—If the judge determines that the proposed minimization procedures required under paragraph (1)(C) do not meet the definition of minimization procedures under section 101(h) or section 301(4), the judge shall enter an order so stating and provide a written statement for the record of the reasons for such determination. The Government may appeal an order under this clause pursuant to subsection (f).

''(D) REVIEW OF CERTIFICATION.—If the judge determines that an application required by subsection (b) does not contain all of the required elements, or that the certification or certifications are clearly erroneous on the basis of the statement made under subsection (b)(1)(F)(v) and any other information furnished under subsection (b)(3), the judge shall enter an order so stating and provide a written statement for the record of the reasons for such determination. The Government may appeal an order under this clause pursuant to subsection (f).

''(4) SPECIFICATIONS.—An order approving an acquisition under this subsection shall specify—

''(A) the identity, if known, or a description of the United States person who is the target of the acquisition identified or described in the application pursuant to subsection (b)(1)(B);

''(B) if provided in the application pursuant to subsection (b)(1)(H), the nature and location of each of the facilities or places at which the acquisition will be directed;

''(C) the nature of the information sought to be acquired and the type of communications or activities to be subjected to acquisition;

''(D) the means by which the acquisition will be conducted and whether physical entry is required to effect the acquisition; and

''(E) the period of time during which the acquisition is approved.

''(5) DIRECTIONS.—An order approving acquisitions under this subsection shall direct—

''(A) that the minimization procedures be followed;

''(B) an electronic communication service provider to provide to the Government forthwith all information, facilities, or assistance necessary to accomplish the acquisition authorized under this subsection in a manner that will protect the secrecy of the acquisition and produce a minimum of interference with the services that such electronic communication service provider is providing to the target;

''(C) an electronic communication service provider to maintain under security procedures approved by the Attorney General any records concerning the acquisition or the aid furnished that such electronic communication service provider wishes to maintain; and

''(D) that the Government compensate, at the prevailing rate, such electronic communication service provider for providing such information, facilities, or assistance.

''(6) DURATION.—An order approved under this paragraph shall be effective for a period not to exceed 90 days and such order may be renewed for additional 90-day periods upon submission of renewal applications meeting the requirements of subsection (b).

''(7) COMPLIANCE.—At or prior to the end of the period of time for which an acquisition is approved by an order or extension under this section, the judge may assess compliance with the minimization procedures by reviewing the circumstances under which information concerning United States persons was acquired, retained, or disseminated.

''(d) EMERGENCY AUTHORIZATION.—

''(1) AUTHORITY FOR EMERGENCY AUTHORIZATION.—Notwithstanding any other provision of this Act, if the Attorney General reasonably determines that—

''(A) an emergency situation exists with respect to the acquisition of foreign intelligence information for which an order may be obtained under subsection (c) before an order authorizing such acquisition can with due diligence be obtained, and

''(B) the factual basis for issuance of an order under this subsection to approve such acquisition exists,

the Attorney General may authorize the emergency acquisition if a judge having jurisdiction under subsection (a)(1) is informed by the Attorney General, or a designee of the Attorney General, at the time of such authorization that the decision has been made to conduct such acquisition and if an application in accordance with this subsection is made to a judge of the Foreign Intelligence Surveillance Court as soon as practicable, but not more than 7 days after the Attorney General authorizes such acquisition.

''(2) MINIMIZATION PROCEDURES.—If the Attorney General authorizes such emergency acquisition, the Attorney General shall require that the minimization procedures required by this section for the issuance of a judicial order be followed.

''(3) TERMINATION OF EMERGENCY AUTHORIZATION.—In the absence of a judicial order approving such acquisition, the acquisition shall terminate when the information sought is obtained, when the application for the order is denied, or after the expiration of 7 days from the time of authorization by the Attorney General, whichever is earliest.

''(4) USE OF INFORMATION.—In the event that such application for approval is denied, or in any other case where the acquisition is terminated and no order is issued approving the acquisition, no information obtained or evidence derived from such acquisition, except under circumstances in which the target of the acquisition is determined not to be a United States person during the pendency of the 7-day emergency acquisition period, shall be received in evidence or otherwise disclosed in any trial, hearing, or

other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired from such acquisition shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.

''(e) RELEASE FROM LIABILITY.—Notwithstanding any other law, no cause of action shall lie in any court against any electronic communication service provider for providing any information, facilities, or assistance in accordance with an order or request for emergency assistance issued pursuant to subsections (c) or (d).

''(f) APPEAL.—

''(1) APPEAL TO THE FOREIGN INTELLIGENCE SURVEILLANCE COURT OF REVIEW.—The Government may file an appeal with the Foreign Intelligence Surveillance Court of Review for review of an order issued pursuant to subsection (c). The Court of Review shall have jurisdiction to consider such appeal and shall provide a written statement for the record of the reasons for a decision under this paragraph.

''(2) CERTIORARI TO THE SUPREME COURT.—The Government may file a petition for a writ of certiorari for review of the decision of the Court of Review issued under paragraph (1). The record for such review shall be transmitted under seal to the Supreme Court of the United States, which shall have jurisdiction to review such decision.

''SEC. 705. OTHER ACQUISITIONS TARGETING UNITED STATES PERSONS OUTSIDE THE UNITED STATES.

''(a) JURISDICTION AND SCOPE.—

''(1) JURISDICTION.—The Foreign Intelligence Surveillance Court shall have jurisdiction to enter an order pursuant to subsection (c).

''(2) SCOPE.—No element of the intelligence community may intentionally target, for the purpose of acquiring foreign intelligence information, a United States person reasonably believed to be located outside the United States under circumstances in which the targeted United States person has a reasonable expectation of privacy and a warrant would be required if the acquisition were conducted inside the United States for law enforcement purposes, unless a judge of the Foreign Intelligence Surveillance Court has entered an order or the Attorney General has authorized an emergency acquisition pursuant to subsections (c) or (d) or any other provision of this Act.

''(3) LIMITATIONS.—

''(A) MOVING OR MISIDENTIFIED TARGETS.—In the event that the targeted United States person is reasonably believed to be in the United States during the pendency of an order issued pursuant to subsection (c), such acquisition shall cease until authority is obtained pursuant to this Act or the targeted United States person is again reasonably believed to be located outside the United States during the pendency of an order issued pursuant to subsection (c).

''(B) APPLICABILITY.—If the acquisition is to be conducted inside the United States and could be authorized under section 704, the procedures of section 704 shall apply, unless an order or emergency acquisition authority has been obtained under a provision of this Act other than under this section.

''(b) APPLICATION.—Each application for an order under this section shall be made by a Federal officer in writing upon oath or affirmation to a judge having jurisdiction under subsection (a)(1). Each application shall require the approval of the Attorney General based upon the Attorney General's finding that it satisfies the criteria and requirements of such application as set forth in this section and shall include—

''(1) the identity, if known, or a description of the specific United States person who is the target of the acquisition;

''(2) a statement of the facts and circumstances relied upon to justify the applicant's belief that the United States person who is the target of the acquisition is—

''(A) a person reasonably believed to be located outside the United States; and

''(B) a foreign power, an agent of a foreign power, or an officer or employee of a foreign power;

''(3) a statement of the proposed minimization procedures that meet the definition of minimization procedures under section 101(h) or section 301(4);

''(4) a certification made by the Attorney General, an official specified in section 104(a)(6), or the head of an element of the intelligence community that—

''(A) the certifying official deems the information sought to be foreign intelligence information; and

''(B) a significant purpose of the acquisition is to obtain foreign intelligence information;

''(5) a statement of the facts concerning any previous applications that have been made to any judge of the Foreign Intelligence Surveillance Court involving the United States person specified in the application and the action taken on each previous application; and

''(6) a statement of the period of time for which the acquisition is required to be maintained, provided that such period of time shall not exceed 90 days per application.

''(c) ORDER.—

''(1) FINDINGS.—If, upon an application made pursuant to subsection (b), a judge having jurisdiction under subsection (a) finds that—

''(A) on the basis of the facts submitted by the applicant, for the United States person who is the target of the acquisition, there is probable cause to believe that the target is—

''(i) a person reasonably believed to be located outside the United States; and

''(ii) a foreign power, an agent of a foreign power, or an officer or employee of a foreign power;

''(B) the proposed minimization procedures, with respect to their dissemination provisions, meet the definition of minimization procedures under section 101(h) or section 301(4); and

''(C) the application which has been filed contains all statements and certifications required by subsection (b) and the certification provided under subsection (b)(4) is not clearly erroneous on the basis of the information furnished under subsection (b),

the Court shall issue an ex parte order so stating.

''(2) PROBABLE CAUSE.—In determining whether or not probable cause exists for purposes of an order under paragraph (1)(A), a judge having jurisdiction under subsection (a)(1) may consider past activities of the target, as well as facts and circumstances relating to current or future activities of the target. However, no United States person may be considered a foreign power, agent of a foreign power, or officer or employee of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

''(3) REVIEW.—

''(A) LIMITATIONS ON REVIEW.—Review by a judge having jurisdiction under subsection (a)(1) shall be limited to that required to make the findings described in paragraph (1). The judge shall not have jurisdiction to review the means by which an acquisition under this section may be conducted.

''(B) REVIEW OF PROBABLE CAUSE.—If the judge determines that the facts submitted under subsection (b) are insufficient to establish probable cause to issue an order under this subsection, the judge shall enter an order so stating and provide a written statement for the record of the reasons for such determination. The Government may appeal an order under this clause pursuant to subsection (e).

''(C) REVIEW OF MINIMIZATION PROCEDURES.—If the judge determines that the minimization procedures applicable to dissemination of information obtained through an acquisition under this subsection do not meet the definition of minimization procedures under section 101(h) or section 301(4), the judge shall enter an order so stating and provide a written statement for the record of the reasons for such determination. The Government may appeal an order under this clause pursuant to subsection (e).

''(D) SCOPE OF REVIEW OF CERTIFICATION.—If the judge determines that the certification provided under subsection (b)(4) is clearly erroneous on the basis of the information furnished under subsection (b), the judge shall enter an order so stating and provide a written statement for the record of the reasons for such determination. The Government may appeal an order under this subparagraph pursuant to subsection (e).

''(4) DURATION.—An order under this paragraph shall be effective for a period not to exceed 90 days and such order may be renewed for additional 90-day periods upon submission of renewal applications meeting the requirements of subsection (b).

''(5) COMPLIANCE.—At or prior to the end of the period of time for which an order or extension is granted under this section, the judge may assess compliance with the minimization procedures by reviewing the circumstances under which information concerning United States persons was disseminated, provided that the judge may not inquire into the circumstances relating to the conduct of the acquisition.

''(d) EMERGENCY AUTHORIZATION.—

''(1) AUTHORITY FOR EMERGENCY AUTHORIZATION.—Notwithstanding any other provision in this subsection, if the Attorney General reasonably determines that—

''(A) an emergency situation exists with respect to the acquisition of foreign intelligence information for which an order may be obtained under subsection (c) before an order under that subsection may, with due diligence, be obtained, and

''(B) the factual basis for issuance of an order under this section exists,

the Attorney General may authorize the emergency acquisition if a judge having jurisdiction under subsection (a)(1) is informed by the Attorney General or a designee of the Attorney General at the time of such authorization that the decision has been made to conduct such acquisition and if an application in accordance with this subsection is made to a judge of the Foreign Intelligence Surveillance Court as soon as practicable, but not more than 7 days after the Attorney General authorizes such acquisition.

''(2) MINIMIZATION PROCEDURES.—If the Attorney General authorizes such emergency acquisition, the Attorney General shall require that the minimization procedures required by this section be followed.

''(3) TERMINATION OF EMERGENCY AUTHORIZATION.—In the absence of an order under subsection (c), the acquisition shall terminate when the information sought is obtained, if the application for the order is denied, or after the expiration of 7 days from the time of authorization by the Attorney General, whichever is earliest.

''(4) USE OF INFORMATION.—In the event that such application is denied, or in any other case where the acquisition is terminated and no order is issued approving the acquisition, no information obtained or evidence derived from such acquisition, except under circumstances in which the target of the acquisition is determined not to be a United States person during the pendency of the 7-day emergency acquisition period, shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision

thereof, and no information concerning any United States person acquired from such acquisition shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.

''(e) APPEAL.—

''(1) APPEAL TO THE COURT OF REVIEW.—The Government may file an appeal with the Foreign Intelligence Surveillance Court of Review for review of an order issued pursuant to subsection (c). The Court of Review shall have jurisdiction to consider such appeal and shall provide a written statement for the record of the reasons for a decision under this paragraph.

''(2) CERTIORARI TO THE SUPREME COURT.—The Government may file a petition for a writ of certiorari for review of the decision of the Court of Review issued under paragraph (1). The record for such review shall be transmitted under seal to the Supreme Court of the United States, which shall have jurisdiction to review such decision.

''SEC. 706. JOINT APPLICATIONS AND CONCURRENT AUTHORIZATIONS.

''(a) JOINT APPLICATIONS AND ORDERS.—If an acquisition targeting a United States person under section 704 or section 705 is proposed to be conducted both inside and outside the United States, a judge having jurisdiction under section 704(a)(1) or section 705(a)(1) may issue simultaneously, upon the request of the Government in a joint application complying with the requirements of section 704(b) or section 705(b), orders under section 704(c) or section 705(c), as applicable.

''(b) CONCURRENT AUTHORIZATION.—If an order authorizing electronic surveillance or physical search has been obtained under section 105 or section 304 and that order is still in effect, the Attorney General may authorize, without an order under section 704 or section 705, an acquisition of foreign intelligence information targeting that United States person while such person is reasonably believed to be located outside the United States.

''SEC. 707. USE OF INFORMATION ACQUIRED UNDER TITLE VII.

''(a) INFORMATION ACQUIRED UNDER SECTION 703.—Information acquired from an acquisition conducted under section 703 shall be deemed to be information acquired from an electronic surveillance pursuant to title I for purposes of section 106, except for the purposes of subsection (j) of such section.

''(b) INFORMATION ACQUIRED UNDER SECTION 704.—Information acquired from an acquisition conducted under section 704 shall be deemed to be information acquired from an electronic surveillance pursuant to title I for purposes of section 106.

''SEC. 708. CONGRESSIONAL OVERSIGHT.

''(a) SEMIANNUAL REPORT.—Not less frequently than once every 6 months, the Attorney General shall fully inform, in a manner consistent with national security, the congressional intelligence committees, the Committee on the Judiciary of the Senate, and the Committee on the Judiciary of the House of Representatives, concerning the implementation of this title.

''(b) CONTENT.—Each report made under subparagraph (a) shall include—

''(1) with respect to section 703—

''(A) any certifications made under subsection 703(f) during the reporting period;

''(B) any directives issued under subsection 703(g) during the reporting period;

''(C) a description of the judicial review during the reporting period of any such certifications and targeting and minimization procedures utilized with respect to such acquisition, including a copy of any order or pleading in connection with such review that contains a significant legal interpretation of the provisions of this section;

''(D) any actions taken to challenge or enforce a directive under paragraphs (4) or (5) of section 703(g);

''(E) any compliance reviews conducted by the Department of Justice or the Office of the Director of National Intelligence of acquisitions authorized under subsection 703(a);

''(F) a description of any incidents of noncompliance with a directive issued by the Attorney General and the Director of National Intelligence under subsection 703(g), including—

''(i) incidents of noncompliance by an element of the intelligence community with procedures adopted pursuant to subsections (d) and (e) of section 703; and

''(ii) incidents of noncompliance by a specified person to whom the Attorney General and Director of National Intelligence issued a directive under subsection 703(g); and

''(G) any procedures implementing this section;

''(2) with respect to section 704—

''(A) the total number of applications made for orders under section 704(b);

''(B) the total number of such orders either granted, modified, or denied; and

''(C) the total number of emergency acquisitions authorized by the Attorney General under section 704(d) and the total number of subsequent orders approving or denying such acquisitions; and

''(3) with respect to section 705—

''(A) the total number of applications made for orders under 705(b);

''(B) the total number of such orders either granted, modified, or denied; and

''(C) the total number of emergency acquisitions authorized by the Attorney General under subsection 705(d) and the total number of subsequent orders approving or denying such applications.''.

(b) TABLE OF CONTENTS.—The table of contents in the first section of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et. seq.) is amended—

(1) by striking the item relating to title VII;

(2) by striking the item relating to section 701; and

(3) by adding at the end the following:

''TITLE VII—ADDITIONAL PROCEDURES REGARDING CERTAIN PERSONS OUTSIDE THE UNITED STATES

''Sec. 701. Limitation on definition of electronic surveillance.

''Sec. 702. Definitions.

''Sec. 703. Procedures for targeting certain persons outside the United States other than United States persons.

''Sec. 704. Certain acquisitions inside the United States of United States persons outside the United States.

''Sec. 705. Other acquisitions targeting United States persons outside the United States.

''Sec. 706. Joint applications and concurrent authorizations.

''Sec. 707. Use of information acquired under title VII.

''Sec. 708. Congressional oversight.''.

(c) TECHNICAL AND CONFORMING AMENDMENTS.—

(1) TITLE 18, UNITED STATES CODE.—

(A) SECTION 2232.—Section 2232(e) of title 18, United States Code, is amended by inserting ''(as defined in section 101(f) of the Foreign Intelligence Surveillance Act of 1978, regardless of the limitation of section 701 of that Act)'' after ''electronic surveillance''.

(B) SECTION 2511.—Section 2511(2)(a)(ii)(A) of title 18, United States Code, is amended by inserting ''or a court order pursuant to section 705 of the Foreign Intelligence Surveillance Act of 1978'' after ''assistance''.

(2) FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.—

(A) SECTION 109.—Section 109 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1809) is amended by adding at the end the following:

''(e) DEFINITION.—For the purpose of this section, the term 'electronic surveillance' means electronic surveillance as defined in section 101(f) of this Act regardless of the limitation of section 701 of this Act.''.

(B) SECTION 110.—Section 110 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1810) is amended by—

(i) adding an ''(a)'' before ''CIVIL ACTION'',

(ii) redesignating subsections (a) through (c) as paragraphs (1) through (3), respectively; and

(iii) adding at the end the following:

''(b) DEFINITION.—For the purpose of this section, the term 'electronic surveillance' means electronic surveillance as defined in section 101(f) of this Act regardless of the limitation of section 701 of this Act.''.

(C) SECTION 601.—Section 601(a)(1) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1871(a)(1)) is amended by striking subparagraphs (C) and (D) and inserting the following:

''(C) pen registers under section 402;

''(D) access to records under section 501;

''(E) acquisitions under section 704; and

''(F) acquisitions under section 705;''.

(d) TERMINATION OF AUTHORITY.—

(1) IN GENERAL.—Except as provided in paragraph (2), the amendments made by subsections (a)(2), (b), and (c) shall cease to have effect on December 31, 2013.

(2) CONTINUING APPLICABILITY.—Section 703(g)(3) of the Foreign Intelligence Surveillance Act of 1978 (as amended by subsection (a)) shall remain in effect with respect to any directive issued pursuant to section 703(g) of that Act (as so amended) for information, facilities, or assistance provided during the period such directive was or is in effect. Section 704(e) of the Foreign Intelligence Surveillance Act of 1978 (as amended by subsection (a)) shall remain in effect with respect to an order or request for emergency assistance under that section. The use of information acquired by an acquisition conducted under section 703 of that Act (as so amended) shall continue to be governed by the provisions of section 707 of that Act (as so amended).

SEC. 102. STATEMENT OF EXCLUSIVE MEANS BY WHICH ELECTRONIC SURVEILLANCE AND INTERCEPTION OF DOMESTIC COMMUNICATIONS MAY BE CONDUCTED.

(a) STATEMENT OF EXCLUSIVE MEANS.—Title I of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is amended by adding at the end the following new section:

''STATEMENT OF EXCLUSIVE MEANS BY WHICH ELECTRONIC SURVEILLANCE AND INTERCEPTION OF DOMESTIC COMMUNICATIONS MAY BE CONDUCTED

''SEC. 112. The procedures of chapters 119, 121, and 206 of title 18, United States Code, and this Act shall be the exclusive means by which electronic surveillance (as defined in section 101(f), regardless of the limitation of section 701) and the interception of domestic wire, oral, or electronic communications may be conducted.''.

(b) TABLE OF CONTENTS.—The table of contents in the first section of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is amended by adding after the item relating to section 111, the following:

''Sec. 112. Statement of exclusive means by which electronic surveillance and interception of domestic communications may be conducted.''.

(c) CONFORMING AMENDMENTS.—Section 2511(2) of title 18, United States Code, is amended in paragraph (f), by striking '', as defined in section 101 of such Act,'' and inserting ''(as defined in section 101(f) of such Act regardless of the limitation of section 701 of such Act)''.

SEC. 103. SUBMITTAL TO CONGRESS OF CERTAIN COURT ORDERS UNDER THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.

(a) INCLUSION OF CERTAIN ORDERS IN SEMI-ANNUAL REPORTS OF ATTORNEY GENERAL.—Subsection (a)(5) of section 601 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1871) is amended by striking ''(not including orders)'' and inserting '', orders,''.

(b) REPORTS BY ATTORNEY GENERAL ON CERTAIN OTHER ORDERS.—Such section 601 is further amended by adding at the end the following:

''(c) SUBMISSIONS TO CONGRESS.—The Attorney General shall submit to the committees of Congress referred to in subsection (a)—

''(1) a copy of any decision, order, or opinion issued by the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review that includes significant construction or interpretation of any provision of this Act, and any pleadings, applications, or memoranda of law associated with such decision, order, or opinion, not later than 45 days after such decision, order, or opinion is issued; and

''(2) a copy of any such decision, order, or opinion, and any pleadings, applications, or memoranda of law associated with such decision, order, or opinion, that was issued during the 5-year period ending on the date of the enactment of the FISA Amendments Act of 2008 and not previously submitted in a report under subsection (a).

''(d) PROTECTION OF NATIONAL SECURITY.—The Attorney General, in consultation with the Director of National Intelligence, may authorize redactions of materials described in subsection (c) that are provided to the committees of Congress referred to in subsection (a), if such redactions are necessary to protect the national security of the United States and are limited to sensitive sources and methods information or the identities of targets.''.

(c) DEFINITIONS.—Such section 601, as amended by subsections (a) and (b), is further amended by adding at the end the following:

''(e) DEFINITIONS.—In this section:

''(1) FOREIGN INTELLIGENCE SURVEILLANCE COURT; COURT.—The term '''Foreign Intelligence Surveillance Court''' means the court established by section 103(a).

''(2) FOREIGN INTELLIGENCE SURVEILLANCE COURT OF REVIEW; COURT OF REVIEW.—The term 'Foreign Intelligence Surveillance Court of Review' means the court established by section 103(b).''.

SEC. 104. APPLICATIONS FOR COURT ORDERS.

Section 104 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1804) is amended—

(1) in subsection (a)—

(A) by striking paragraphs (2) and (11);

(B) by redesignating paragraphs (3) through (10) as paragraphs (2) through (9), respectively;

(C) in paragraph (5), as redesignated by subparagraph (B) of this paragraph, by striking ''detailed'';

(D) in paragraph (6), as redesignated by subparagraph (B) of this paragraph, in the matter preceding subparagraph (A)—

(i) by striking ''Affairs or'' and inserting ''Affairs,''; and

(ii) by striking ''Senate—'' and inserting ''Senate, or the Deputy Director of the Federal Bureau of Investigation, if designated by the President as a certifying official—'';

(E) in paragraph (7), as redesignated by subparagraph (B) of this paragraph, by striking ''statement of'' and inserting ''summary statement of'';

(F) in paragraph (8), as redesignated by subparagraph (B) of this paragraph, by adding ''and'' at the end; and

(G) in paragraph (9), as redesignated by subparagraph (B) of this paragraph, by striking ''; and'' and inserting a period;

(2) by striking subsection (b);

(3) by redesignating subsections (c) through (e) as subsections (b) through (d), respectively; and

(4) in paragraph (1)(A) of subsection (d), as redesignated by paragraph (3) of this subsection, by striking ''or the Director of National Intelligence'' and inserting ''the Director of National Intelligence, or the Director of the Central Intelligence Agency''.

SEC. 105. ISSUANCE OF AN ORDER.

Section 105 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1805) is amended—

(1) in subsection (a)—

(A) by striking paragraph (1); and

(B) by redesignating paragraphs (2) through (5) as paragraphs (1) through (4), respectively;

(2) in subsection (b), by striking ''(a)(3)'' and inserting ''(a)(2)'';

(3) in subsection (c)(1)—

(A) in subparagraph (D), by adding ''and'' at the end;

(B) in subparagraph (E), by striking ''; and'' and inserting a period; and

(C) by striking subparagraph (F);

(4) by striking subsection (d);

(5) by redesignating subsections (e) through (i) as subsections (d) through (h), respectively;

(6) by amending subsection (e), as redesignated by paragraph (5) of this section, to read as follows:

''(e)(1) Notwithstanding any other provision of this title, the Attorney General may authorize the emergency employment of electronic surveillance if the Attorney General—

''(A) reasonably determines that an emergency situation exists with respect to the employment of electronic surveillance to obtain foreign intelligence information before an order authorizing such surveillance can with due diligence be obtained;

''(B) resonably determines that the factual basis for issuance of an order under this title to approve such electronic surveillance exists;

''(C) informs, either personally or through a designee, a judge having jurisdiction under section 103 at the time of such authorization that the decision has been made to employ emergency electronic surveillance; and

''(D) makes an application in accordance with this title to a judge having jurisdiction under section 103 as soon as practicable, but not later than 7 days after the Attorney General authorizes such surveillance.

''(2) If the Attorney General authorizes the emergency employment of electronic surveillance under paragraph (1), the Attorney General shall require that the minimization procedures required by this title for the issuance of a judicial order be followed.

''(3) In the absence of a judicial order approving such electronic surveillance, the surveillance shall terminate when the information sought is obtained, when the application for the order is denied, or after the expiration of 7 days from the time of authorization by the Attorney General, whichever is earliest.

''(4) A denial of the application made under this subsection may be reviewed as provided in section 103.

''(5) In the event that such application for approval is denied, or in any other case where the electronic surveillance is terminated and no order is issued approving the surveillance, no information obtained or evidence derived from such surveillance shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired from such surveillance shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.

''(6) The Attorney General shall assess compliance with the requirements of paragraph (5).''; and

(7) by adding at the end the following:

''(i) In any case in which the Government makes an application to a judge under this title to conduct electronic surveillance involving communications and the judge grants such application, upon the request of the applicant, the judge shall also authorize the installation and use of pen registers and trap and trace devices, and direct the disclosure of the information set forth in section 402(d)(2).''.

SEC. 106. USE OF INFORMATION.

Subsection (i) of section 106 of the Foreign Intelligence Surveillance Act of 1978 (8 U.S.C. 1806) is amended by striking ''radio communication'' and inserting ''communication''.

SEC. 107. AMENDMENTS FOR PHYSICAL SEARCHES.

(a) APPLICATIONS.—Section 303 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1823) is amended—

(1) in subsection (a)—

(A) by striking paragraph (2);

(B) by redesignating paragraphs (3) through (9) as paragraphs (2) through (8), respectively;

(C) in paragraph (2), as redesignated by subparagraph (B) of this paragraph, by striking ''detailed'';

(D) in paragraph (3)(C), as redesignated by subparagraph (B) of this paragraph, by inserting ''or is about to be'' before ''owned''; and

(E) in paragraph (6), as redesignated by subparagraph (B) of this paragraph, in the matter preceding subparagraph (A)—

(i) by striking ''Affairs or'' and inserting ''Affairs,''; and

(ii) by striking ''Senate—'' and inserting ''Senate, or the Deputy Director of the Federal Bureau of Investigation, if designated by the President as a certifying official—''; and

(2) in subsection (d)(1)(A), by striking ''or the Director of National Intelligence'' and inserting ''the Director of National Intelligence, or the Director of the Central Intelligence Agency''.

(b) ORDERS.—Section 304 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1824) is amended—

(1) in subsection (a)—

(A) by striking paragraph (1); and

(B) by redesignating paragraphs (2) through (5) as paragraphs (1) through (4), respectively; and

(2) by amending subsection (e) to read as follows:

''(e)(1) Notwithstanding any other provision of this title, the Attorney General may authorize the emergency employment of a physical search if the Attorney General reasonably—

''(A) determines that an emergency situation exists with respect to the employment of a physical search to obtain foreign intelligence information before an order authorizing such physical search can with due diligence be obtained;

''(B) determines that the factual basis for issuance of an order under this title to approve such physical search exists;

''(C) informs, either personally or through a designee, a judge of the Foreign Intelligence Surveillance Court at the time of such authorization that the decision has been made to employ an emergency physical search; and

''(D) makes an application in accordance with this title to a judge of the Foreign Intelligence Surveillance Court as soon as practicable, but not more than 7 days after the Attorney General authorizes such physical search.

''(2) If the Attorney General authorizes the emergency employment of a physical search under paragraph (1), the Attorney General shall require that the minimization procedures required by this title for the issuance of a judicial order be followed.

''(3) In the absence of a judicial order approving such physical search, the physical search shall terminate when the information sought is

obtained, when the application for the order is denied, or after the expiration of 7 days from the time of authorization by the Attorney General, whichever is earliest.

''(4) A denial of the application made under this subsection may be reviewed as provided in section 103.

''(5)(A) In the event that such application for approval is denied, or in any other case where the physical search is terminated and no order is issued approving the physical search, no information obtained or evidence derived from such physical search shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired from such physical search shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.

''(B) The Attorney General shall assess compliance with the requirements of subparagraph (A).''.

(c) CONFORMING AMENDMENTS.—The Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is amended—

(1) in section 304(a)(4), as redesignated by subsection (b) of this section, by striking ''303(a)(7)(E)'' and inserting ''303(a)(6)(E)''; and

(2) in section 305(k)(2), by striking ''303(a)(7)'' and inserting ''303(a)(6)''.

SEC. 108. AMENDMENTS FOR EMERGENCY PEN REGISTERS AND TRAP AND TRACE DEVICES.

Section 403 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1843) is amended—

(1) in subsection (a)(2), by striking ''48 hours'' and inserting ''7 days''; and

(2) in subsection (c)(1)(C), by striking ''48 hours'' and inserting ''7 days''.

SEC. 109. FOREIGN INTELLIGENCE SURVEILLANCE COURT.

(a) DESIGNATION OF JUDGES.—Subsection (a) of section 103 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803) is amended by inserting ''at least'' before ''seven of the United States judicial circuits''.

(b) EN BANC AUTHORITY.—

(1) IN GENERAL.—Subsection (a) of section 103 of the Foreign Intelligence Surveillance Act of 1978, as amended by subsection (a) of this section, is further amended—

(A) by inserting ''(1)'' after ''(a)''; and

(B) by adding at the end the following new paragraph:

''(2)(A) The court established under this subsection may, on its own initiative, or upon the request of the Government in any proceeding or a party under section 501(f) or paragraph (4) or (5) of section 703(h), hold a hearing or rehearing, en banc, when ordered by a majority of the judges that constitute such court upon a determination that—

''(i) en banc consideration is necessary to secure or maintain uniformity of the court's decisions; or

''(ii) the proceeding involves a question of exceptional importance.

''(B) Any authority granted by this Act to a judge of the court established under this subsection may be exercised by the court en banc. When exercising such authority, the court en banc shall comply with any requirements of this Act on the exercise of such authority.

''(C) For purposes of this paragraph, the court en banc shall consist of all judges who constitute the court established under this subsection.''.

(2) CONFORMING AMENDMENTS.—The Foreign Intelligence Surveillance Act of 1978 is further amended—

(A) in subsection (a) of section 103, as amended by this subsection, by inserting ''(except when sitting en banc under paragraph (2))'' after ''no judge designated under this subsection''; and

(B) in section 302(c) (50 U.S.C. 1822(c)), by inserting ''(except when sitting en banc)'' after ''except that no judge''.

(c) STAY OR MODIFICATION DURING AN APPEAL.—Section 103 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803) is amended—

(1) by redesignating subsection (f) as subsection (g); and

(2) by inserting after subsection (e) the following new subsection:

''(f)(1) A judge of the court established under subsection (a), the court established under subsection (b) or a judge of that court, or the Supreme Court of the United States or a justice of that court, may, in accordance with the rules of their respective courts, enter a stay of an order or an order modifying an order of the court established under subsection (a) or the court established under subsection (b) entered under any title of this Act, while the court established under subsection (a) conducts a rehearing, while an appeal is pending to the court established under subsection (b), or while a petition of certiorari is pending in the Supreme Court of the United States, or during the pendency of any review by that court.

''(2) The authority described in paragraph (1) shall apply to an order entered under any provision of this Act.''.

(d) AUTHORITY OF FOREIGN INTELLIGENCE SURVEILLANCE COURT.—Section 103 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803), as amended by this Act, is amended by adding at the end the following:

''(h)(1) Nothing in this Act shall be considered to reduce or contravene the inherent authority of the Foreign Intelligence Surveillance Court to determine, or enforce, compliance with an order or a rule of such Court or with a procedure approved by such Court.

''(2) In this subsection, the terms 'Foreign Intelligence Surveillance Court' and 'Court' mean the court established by subsection (a).''.

SEC. 110. WEAPONS OF MASS DESTRUCTION.

(a) DEFINITIONS.—

(1) FOREIGN POWER.—Subsection (a)(4) of section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801(a)(4)) is amended by inserting '', the international proliferation of weapons of mass destruction,'' after ''international terrorism''.

(2) AGENT OF A FOREIGN POWER.—Subsection (b)(1) of such section 101 is amended—

(A) in subparagraph (B), by striking ''or'' at the end

(B) in subparagraph (C), by striking ''or'' at the end; and

(C) by adding at the end the following new subparagraphs:

''(D) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor; or

''(E) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor, for or on behalf of a foreign power; or''.

(3) FOREIGN INTELLIGENCE INFORMATION.—Subsection (e)(1)(B) of such section 101 is amended by striking ''sabotage or international terrorism'' and inserting ''sabotage, international terrorism, or the international proliferation of weapons of mass destruction''.

(4) WEAPON OF MASS DESTRUCTION.—Such section 101 is amended by inserting after subsection (o) the following:

''(p) 'Weapon of mass destruction' means—

''(1) any destructive device described in section 921(a)(4)(A) of title 18, United States Code, that is intended or has the capability to cause death or serious bodily injury to a significant number of people;

''(2) any weapon that is designed or intended to cause death or serious bodily injury through the release, dissemination, or impact of toxic or poisonous chemicals or their precursors;

''(3) any weapon involving a biological agent, toxin, or vector (as such terms are defined in section 178 of title 18, United States Code); or

''(4) any weapon that is designed to release radiation or radioactivity at a level dangerous to human life.''.

(b) USE OF INFORMATION.—

(1) IN GENERAL.—Section 106(k)(1)(B) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1806(k)(1)(B)) is amended by striking ''sabotage or international terrorism'' and inserting ''sabotage, international terrorism, or the international proliferation of weapons of mass destruction''.

(2) PHYSICAL SEARCHES.—Section 305(k)(1)(B) of such Act (50 U.S.C. 1825(k)(1)(B)) is amended by striking ''sabotage or international terrorism'' and inserting ''sabotage, international terrorism, or the international proliferation of weapons of mass destruction''.

(c) TECHNICAL AND CONFORMING AMENDMENT.—Section 301(1) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1821(1)) is amended by inserting ''''weapon of mass destruction','' after ''''person',''.

SEC. 111. TECHNICAL AND CONFORMING AMENDMENTS.

Section 103(e) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803(e)) is amended—

(1) in paragraph (1), by striking ''105B(h) or 501(f)(1)'' and inserting ''501(f)(1) or 703''; and

(2) in paragraph (2), by striking ''105B(h) or 501(f)(1)'' and inserting ''501(f)(1) or 703''.

TITLE II—PROTECTIONS FOR ELECTRONIC COMMUNICATION SERVICE PROVIDERS

SEC. 201. DEFINITIONS.

In this title:

(1) ASSISTANCE.—The term ''assistance'' means the provision of, or the provision of access to, information (including communication contents, communications records, or other information relating to a customer or communication), facilities, or another form of assistance.

(2) CONTENTS.—The term ''contents'' has the meaning given that term in section 101(n) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801(n)).

(3) COVERED CIVIL ACTION.—The term ''covered civil action'' means a civil action filed in a Federal or State court that—

(A) alleges that an electronic communication service provider furnished assistance to an element of the intelligence community; and

(B) seeks monetary or other relief from the electronic communication service provider related to the provision of such assistance.

(4) ELECTRONIC COMMUNICATION SERVICE PROVIDER.—The term ''electronic communication service provider'' means—

(A) a telecommunications carrier, as that term is defined in section 3 of the Communications Act of 1934 (47 U.S.C. 153);

(B) a provider of an electronic communication service, as that term is defined in section 2510 of title 18, United States Code;

(C) a provider of a remote computing service, as that term is defined in section 2711 of title 18, United States Code;

(D) any other communication service provider who has access to wire or electronic communications either as such communications are transmitted or as such communications are stored;

(E) a parent, subsidiary, affiliate, successor, or assignee of an entity described in subparagraph (A), (B), (C), or (D); or

(F) an officer, employee, or agent of an entity described in subparagraph (A), (B), (C), (D), or (E).

(5) ELEMENT OF THE INTELLIGENCE COMMUNITY.—The term ''element of the intelligence community'' means an element of the intelligence community specified in or designated under section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4)).

SEC. 202. LIMITATIONS ON CIVIL ACTIONS FOR ELECTRONIC COMMUNICATION SERVICE PROVIDERS.

(a) LIMITATIONS.—

(1) IN GENERAL.—Notwithstanding any other provision of law, a covered civil action shall not lie or be maintained in a Federal or State court, and shall be promptly dismissed, if the Attorney General certifies to the court that—

(A) the assistance alleged to have been provided by the electronic communication service provider was—

(i) in connection with an intelligence activity involving communications that was—

(I) authorized by the President during the period beginning on September 11, 2001, and ending on January 17, 2007; and

(II) designed to detect or prevent a terrorist attack, or activities in preparation for a terrorist attack, against the United States; and

(ii) described in a written request or directive from the Attorney General or the head of an element of the intelligence community (or the deputy of such person) to the electronic communication service provider indicating that the activity was—

(I) authorized by the President; and

(II) determined to be lawful; or

(B) the electronic communication service provider did not provide the alleged assistance.

(2) REVIEW.—A certification made pursuant to paragraph (1) shall be subject to review by a court for abuse of discretion.

(b) REVIEW OF CERTIFICATIONS.—If the Attorney General files a declaration under section 1746 of title 28, United States Code, that disclosure of a certification made pursuant to subsection (a) would harm the national security of the United States, the court shall—

(1) review such certification in camera and ex parte; and

(2) limit any public disclosure concerning such certification, including any public order following such an ex parte review, to a statement that the conditions of subsection (a) have been met, without disclosing the subparagraph of subsection (a)(1) that is the basis for the certification.

(c) NONDELEGATION.—The authority and duties of the Attorney General under this section shall be performed by the Attorney General (or Acting Attorney General) or a designee in a position not lower than the Deputy Attorney General.

(d) CIVIL ACTIONS IN STATE COURT.—A covered civil action that is brought in a State court shall be deemed to arise under the Constitution and laws of the United States and shall be removable under section 1441 of title 28, United States Code.

(e) RULE OF CONSTRUCTION.—Nothing in this section may be construed to limit any otherwise available immunity, privilege, or defense under any other provision of law.

(f) EFFECTIVE DATE AND APPLICATION.—This section shall apply to any covered civil action that is pending on or filed after the date of enactment of this Act.

SEC. 203. PROCEDURES FOR IMPLEMENTING STATUTORY DEFENSES UNDER THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.

The Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), as amended by section 101, is further amended by adding after title VII the following new title:

"TITLE VIII—PROTECTION OF PERSONS ASSISTING THE GOVERNMENT

"SEC. 801. DEFINITIONS.

''In this title:

''(1) ASSISTANCE.—The term 'assistance' means the provision of, or the provision of access to, information (including communication contents, communications records, or other information relating to a customer or communication), facilities, or another form of assistance.

''(2) ATTORNEY GENERAL.—The term 'Attorney General' has the meaning give that term in section 101(g).

''(3) CONTENTS.—The term 'contents' has the meaning given that term in section 101(n).

''(4) ELECTRONIC COMMUNICATION SERVICE PROVIDER.—The term 'electronic communication service provider' means—

''(A) a telecommunications carrier, as that term is defined in section 3 of the Communications Act of 1934 (47 U.S.C. 153);

''(B) a provider of electronic communication service, as that term is defined in section 2510 of title 18, United States Code;

''(C) a provider of a remote computing service, as that term is defined in section 2711 of title 18, United States Code;

''(D) any other communication service provider who has access to wire or electronic communications either as such communications are transmitted or as such communications are stored;

''(E) a parent, subsidiary, affiliate, successor, or assignee of an entity described in subparagraph (A), (B), (C), or (D); or

''(F) an officer, employee, or agent of an entity described in subparagraph (A), (B), (C), (D), or (E).

''(5) ELEMENT OF THE INTELLIGENCE COMMUNITY.—The term 'element of the intelligence community' means an element of the intelligence community as specified or designated under section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4)).

''(6) PERSON.—The term 'person' means—

''(A) an electronic communication service provider; or

''(B) a landlord, custodian, or other person who may be authorized or required to furnish assistance pursuant to—

''(i) an order of the court established under section 103(a) directing such assistance;

''(ii) a certification in writing under section 2511(2)(a)(ii)(B) or 2709(b) of title 18, United States Code; or

''(iii) a directive under section 102(a)(4), 105B(e), as in effect on the day before the date of the enactment of the FISA Amendments Act of 2008 or 703(h).

''(7) STATE.—The term 'State' means any State, political subdivision of a State, the Commonwealth of Puerto Rico, the District of Columbia, and any territory or possession of the United States, and includes any officer, public utility commission, or other body authorized to regulate an electronic communication service provider.

"SEC. 802. PROCEDURES FOR IMPLEMENTING STATUTORY DEFENSES.

''(a) REQUIREMENT FOR CERTIFICATION.—

''(1) IN GENERAL.—Notwithstanding any other provision of law, no civil action may lie or be maintained in a Federal or State court against any person for providing assistance to an element of the intelligence community, and shall be promptly dismissed, if the Attorney General certifies to the court that—

''(A) any assistance by that person was provided pursuant to an order of the court established under section 103(a) directing such assistance;

''(B) any assistance by that person was provided pursuant to a certification in writing under section 2511(2)(a)(ii)(B) or 2709(b) of title 18, United States Code;

''(C) any assistance by that person was provided pursuant to a directive under sections 102(a)(4), 105B(e), as in effect on the day before the date of the enactment of the FISA Amendments Act of 2008, or 703(h) directing such assistance; or

''(D) the person did not provide the alleged assistance.

''(2) REVIEW.—A certification made pursuant to paragraph (1) shall be subject to review by a court for abuse of discretion.

''(b) LIMITATIONS ON DISCLOSURE.—If the Attorney General files a declaration under section 1746 of title 28, United States Code, that disclosure of a certification made pursuant to subsection (a) would harm the national security of the United States, the court shall—

''(1) review such certification in camera and ex parte; and

''(2) limit any public disclosure concerning such certification, including any public order following such an ex parte review, to a statement that the conditions of subsection (a) have been met, without disclosing the subparagraph of subsection (a)(1) that is the basis for the certification.

''(c) REMOVAL.—A civil action against a person for providing assistance to an element of the intelligence community that is brought in a State court shall be deemed to arise under the Constitution and laws of the United States and shall be removable under section 1441 of title 28, United States Code.

''(d) RELATIONSHIP TO OTHER LAWS.—Nothing in this section may be construed to limit any otherwise available immunity, privilege, or defense under any other provision of law.

''(e) APPLICABILITY.—This section shall apply to a civil action pending on or filed after the date of enactment of the FISA Amendments Act of 2008.''.

SEC. 204. PREEMPTION OF STATE INVESTIGATIONS.

Title VIII of the Foreign Intelligence Surveillance Act (50 U.S.C. 1801 et seq.), as added by section 203 of this Act, is amended by adding at the end the following new section:

"SEC. 803. PREEMPTION.

''(a) IN GENERAL.—No State shall have authority to—

''(1) conduct an investigation into an electronic communication service provider's alleged assistance to an element of the intelligence community;

''(2) require through regulation or any other means the disclosure of information about an electronic communication service provider's alleged assistance to an element of the intelligence community;

''(3) impose any administrative sanction on an electronic communication service provider for assistance to an element of the intelligence community; or

''(4) commence or maintain a civil action or other proceeding to enforce a requirement that an electronic communication service provider disclose information concerning alleged assistance to an element of the intelligence community.

''(b) SUITS BY THE UNITED STATES.—The United States may bring suit to enforce the provisions of this section.

''(c) JURISDICTION.—The district courts of the United States shall have jurisdiction over any civil action brought by the United States to enforce the provisions of this section.

''(d) APPLICATION.—This section shall apply to any investigation, action, or proceeding that is pending on or filed after the date of enactment of the FISA Amendments Act of 2008.''.

SEC. 205. TECHNICAL AMENDMENTS.

The table of contents in the first section of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), as amended by section 101(b), is further amended by adding at the end the following:

''TITLE VIII—PROTECTION OF PERSONS ASSISTING THE GOVERNMENT

''Sec. 801. Definitions.

''Sec. 802. Procedures for implementing statutory defenses.

''Sec. 803. Preemption.''.

TITLE III—OTHER PROVISIONS

SEC. 301. SEVERABILITY.

If any provision of this Act, any amendment made by this Act, or the application thereof to any person or circumstances is held invalid, the validity of the remainder of the Act, any such amendments, and of the application of such provisions to other persons and circumstances shall not be affected thereby.

SEC. 302. EFFECTIVE DATE; REPEAL; TRANSITION PROCEDURES.

(a) IN GENERAL.—Except as provided in subsection (c), the amendments made by this Act

shall take effect on the date of the enactment of this Act.

(b) REPEAL.—

(1) IN GENERAL.—Except as provided in subsection (c), sections 105A, 105B, and 105C of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1805a, 1805b, and 1805c) are repealed.

(2) TABLE OF CONTENTS.—The table of contents in the first section of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is amended by striking the items relating to sections 105A, 105B, and 105C.

(c) TRANSITIONS PROCEDURES.—

(1) PROTECTION FROM LIABILITY.—Notwithstanding subsection (b)(1), subsection (l) of section 105B of the Foreign Intelligence Surveillance Act of 1978 shall remain in effect with respect to any directives issued pursuant to such section 105B for information, facilities, or assistance provided during the period such directive was or is in effect.

(2) ORDERS IN EFFECT.—

(A) ORDERS IN EFFECT ON DATE OF ENACTMENT.—Notwithstanding any other provision of this Act or of the Foreign Intelligence Surveillance Act of 1978—

(i) any order in effect on the date of enactment of this Act issued pursuant to the Foreign Intelligence Surveillance Act of 1978 or section 6(b) of the Protect America Act of 2007 (Public Law 110–55; 121 Stat. 556) shall remain in effect until the date of expiration of such order; and

(ii) at the request of the applicant, the court established under section 103(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803(a)) shall reauthorize such order if the facts and circumstances continue to justify issuance of such order under the provisions of such Act, as in effect on the day before the date of the enactment of the Protect America Act of 2007, except as amended by sections 102, 103, 104, 105, 106, 107, 108, 109, and 110 of this Act.

(B) ORDERS IN EFFECT ON DECEMBER 31, 2013.—Any order issued under title VII of the Foreign Intelligence Surveillance Act of 1978, as amended by section 101 of this Act, in effect on December 31, 2013, shall continue in effect until the date of the expiration of such order. Any such order shall be governed by the applicable provisions of the Foreign Intelligence Surveillance Act of 1978, as so amended.

(3) AUTHORIZATIONS AND DIRECTIVES IN EFFECT.—

(A) AUTHORIZATIONS AND DIRECTIVES IN EFFECT ON DATE OF ENACTMENT.—Notwithstanding any other provision of this Act or of the Foreign Intelligence Surveillance Act of 1978, any authorization or directive in effect on the date of the enactment of this Act issued pursuant to the Protect America Act of 2007, or any amendment made by that Act, shall remain in effect until the date of expiration of such authorization or directive. Any such authorization or directive shall be governed by the applicable provisions of the Protect America Act of 2007 (121 Stat. 552), and the amendment made by that Act, and, except as provided in paragraph (4) of this subsection, any acquisition pursuant to such authorization or directive shall be deemed not to constitute electronic surveillance (as that term is defined in section 101(f) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801(f)), as construed in accordance with section 105A of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1805a)).

(B) AUTHORIZATIONS AND DIRECTIVES IN EFFECT ON DECEMBER 31, 2013.—Any authorization or directive issued under title VII of the Foreign Intelligence Surveillance Act of 1978, as amended by section 101 of this Act, in effect on December 31, 2013, shall continue in effect until the date of the expiration of such authorization or directive. Any such authorization or directive shall be governed by the applicable provisions of the Foreign Intelligence Surveillance Act of 1978, as so amended, and, except as provided in section 707 of the Foreign Intelligence Surveillance Act of 1978, as so amended, any acquisition pursuant to such authorization or directive shall be deemed not to constitute electronic surveillance (as that term is defined in section 101(f) of the Foreign Intelligence Surveillance Act of 1978, to the extent that such section 101(f) is limited by section 701 of the Foreign Intelligence Surveillance Act of 1978, as so amended).

(4) USE OF INFORMATION ACQUIRED UNDER PROTECT AMERICA ACT.—Information acquired from an acquisition conducted under the Protect America Act of 2007, and the amendments made by that Act, shall be deemed to be information acquired from an electronic surveillance pursuant to title I of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) for purposes of section 106 of that Act (50 U.S.C. 1806), except for purposes of subsection (j) of such section.

(5) NEW ORDERS.—Notwithstanding any other provision of this Act or of the Foreign Intelligence Surveillance Act of 1978—

(A) the government may file an application for an order under the Foreign Intelligence Surveillance Act of 1978, as in effect on the day before the date of the enactment of the Protect America Act of 2007, except as amended by sections 102, 103, 104, 105, 106, 107, 108, 109, and 110 of this Act; and

(B) the court established under section 103(a) of the Foreign Intelligence Surveillance Act of 1978 shall enter an order granting such an application if the application meets the requirements of such Act, as in effect on the day before the date of the enactment of the Protect America Act of 2007, except as amended by sections 102, 103, 104, 105, 106, 107, 108, 109, and 110 of this Act.

(6) EXTANT AUTHORIZATIONS.—At the request of the applicant, the court established under section 103(a) of the Foreign Intelligence Surveillance Act of 1978 shall extinguish any extant authorization to conduct electronic surveillance or physical search entered pursuant to such Act.

(7) APPLICABLE PROVISIONS.—Any surveillance conducted pursuant to an order entered pursuant to this subsection shall be subject to the provisions of the Foreign Intelligence Surveillance Act of 1978, as in effect on the day before the date of the enactment of the Protect America Act of 2007, except as amended by sections 102, 103, 104, 105, 106, 107, 108, 109, and 110 of this Act.

(8) TRANSITION PROCEDURES CONCERNING THE TARGETING OF UNITED STATES PERSONS OVERSEAS.—Any authorization in effect on the date of enactment of this Act under section 2.5 of Executive Order 12333 to intentionally target a United States person reasonably believed to be located outside the United States shall remain in effect, and shall constitute a sufficient basis for conducting such an acquisition targeting a United States person located outside the United States until the earlier of—

(A) the date that authorization expires; or

(B) the date that is 90 days after the date of the enactment of this Act.

Mr. ROCKEFELLER. Madam President, I suggest the absence of a quorum.

The PRESIDING OFFICER. Without objection, it is so ordered.

Mr. BOND. Madam President, I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER. Without objection, it is so ordered.

Mr. BOND. Madam President, again I rise to thank Chairman ROCKEFELLER, the members of the committee on both sides, and our very able staffs for a lot of hard work, particularly by members of the committee but by many Members who are not on the committee, who took their time to learn what the electronic surveillance capabilities are, to learn what guidelines and protections there are to protect the privacy rights and constitutional rights of American citizens and help us pass this bill.

This is a bill which I hope we will at least, in large part, find the House agreeable to and that we can send it to the President. This has been a very long procedure. The chairman just pointed out that we have been working on this almost a year. We worked very hard after the August recess to come up with a good bill. I know we had some very warmly felt and vigorously argued amendments, but the fact that these would make it difficult for the intelligence community to collect the intelligence necessary to protect our interests, our allies, our troops abroad, and us here at home led a significant bipartisan majority to improve it.

Again, my sincere thanks to the leadership on both sides for allowing us to get to this important measure. We hope we will have a conference report, if necessary, or a measure from the House that we can pass before the end of the week.

So, Madam President, my sincere thanks to Members on both sides and particularly our great staffs on both sides.

I thank the Chair, and I yield the floor.

The PRESIDING OFFICER. The Democratic leader.

UNANIMOUS-CONSENT REQUEST—S. 2615

Mr. REID. Madam President, as I indicated I would earlier today, I will ask unanimous consent to extend the law that is now in effect. I wish to extend that 15 days to see if we can work out something more with the House.

So I ask unanimous consent that the Senate proceed to the immediate consideration of Calendar No. 571, S. 2615; the bill be read a third time and passed; and the motion to reconsider be laid upon the table with no intervening action or debate.

The PRESIDING OFFICER. The Republican leader.

Mr. MCCONNELL. Reserving the right to object, let me just make the point once again that we just passed this bill 68 to 29 in its initial form, which was preserved on the Senate floor. It came out of the Intelligence Committee 13 to 2. This is the Rockefeller-Bond bipartisan, overwhelmingly supported bill coming out of the Senate.

The current law does not expire until Saturday. It is still my hope that the House, and particularly when you consider the fact that 21 House Democrats, so-called Blue Dog Democrats, have indicated to the Speaker in writing that they would like to see the Senate bill passed—the Rockefeller-Bond bill taken up and passed by the House—I think it is just premature for an extension, Madam President. I think there is