New Year's Day. That is the average. Some would go up more, some less, of course.

Speaker BOEHNER should call Members back to Washington today. He should not have let them go, in fact. They are not here. JOHN BOEHNER seems to care more about keeping his speakership than about keeping the Nation on a firm financial footing. It is obvious what is going on around here. He is waiting until January 3 to get reelected as Speaker before he gets serious with negotiations because he has so many people over there who will not follow what he wants. That is obvious from the debacle that took place last week, and it was a debacle.

He made an offer to the President. The President came back—they are just a little bit apart—and he walked away from that and went to Plan B. All that did is whack people who need help the most—poor people. He could not even pass that. Remember, he is not letting the House of Representatives vote. He is letting the Republicans vote. It was so bad, and he was in such difficult shape there he would not even let a vote take place with his Republicans because he knew he would lose. For months, he has allowed House Republicans to hold middle-class taxpayers hostage to protect the richest 2 percent, and the funny thing about that is the 2 percent do not want to be protected. The majority of people in our great country are willing to pay more. The only people who disagree with that are Republicans who work in this building.

The Speaker just has a few days left to change his mind, but I have to be very honest; I don't know, timewise, how it can happen now. Everyone knows we cannot bring up anything here unless we do it by unanimous consent because the rules have been so worked the last few years that we cannot do anything without 60 votes. There are 53 of us. After the first of the year, there will be 55 of us.

I hope the Speaker and the Republican leader in the Senate would come to us and say here is what we think will work. Let's find out what that could be because the Speaker cannot pass, it seems, much of anything over there. On the Sunday shows they had Republican Senators and they were asked on the FOX network—pretty conservative, and that is probably a gross understatement—would you filibuster the President's bill? They refused to answer. We don't make that decision. We can't answer that. A filibuster is over all our heads.

That is why we have to look seriously next year at changing the rules around here. The bill that has passed the Senate protects 98 percent of families and 97 percent of small businesses. They passed a bill in the House, that we defeated, that extends the tax cuts for everybody. That was voted down over here. The President said he would veto it. So this happy talk—the Republican House leadership said yesterday: Let them take our bill. That bill was brought up and it was defeated.

I repeat, the American people do not agree with the Republicans in the House and Republicans over here. The way to avoid the fiscal cliff has been right in the face of the Republican leaders, both MCCONNELL and BOEHNER, for days and days, going into weeks and months, and it is the only option that is a viable escape route and that is the Senate-passed bill. It would not be hard to pass. I have talked about that at some length. Every Democrat in the House would vote for it, a handful of Republicans would vote for it, and that is all that would be needed. But Grover Norquist is standing in the way of this—not the rich people but Grover Norquist, the man who says what the Republicans can do. I say to the Speaker: Take the escape hatch we have left you. Put the economic fate of the Nation ahead of your own fate as Speaker of the House. Millions of middle-class families are nervously watching and waiting and counting down the moment until their taxes go up. Nothing can move forward in regard to our budget crisis unless Speaker BOEHNER and Leader MCCONNELL are willing to participate in coming up with a bipartisan plan.

Speaker BOEHNER is unwilling to negotiate, we have not heard a word from Leader MCCONNELL, and nothing is happening. Democrats cannot put forward a plan of their own. Without the participation of Leader MCCONNELL and Speaker BOEHNER, nothing can happen on the fiscal cliff and so far they are radio silent.

We are going to work in the next couple of days to get the most important legislation done on FISA. There should be a good debate. We have people who are interested in changing what we have on the floor. There have been a series of amendments on trying to change FISA—the espionage legislation that guides this country. It should be a good debate.

We have to finish the supplemental appropriations bill that is so important for the people in the Northeast. We have a lot to do. There could be as many as 28 votes in the next few days. We are in Washington working while the Members of the House of Representatives are out watching movies, watching their kids play soccer and basketball and doing all kinds of things. They should be here. They should be here urging the Speaker: Let's bring up the $250,000 bill. Let's not have middle-class Americans and small businesses get hurt.

What is the business?

RESERVATION OF LEADER TIME

The ACTING PRESIDENT pro tempore. Under the previous order, the leadership time is reserved.

FISA AMENDMENTS ACT REAUTHORIZATION ACT OF 2012

The ACTING PRESIDENT pro tempore. Under the previous order, the Senate will proceed to consideration of H.R. 5949, which the clerk will report.

The legislative clerk read as follows:

A bill (H.R. 5949) to extend the FISA Amendments Act of 2008 for five years.

The ACTING PRESIDENT pro tempore. Under the previous order, the Senator from Oregon, Mr. WYDEN, is recognized.

Mr. WYDEN. Mr. President, I thank Leader REID for the honor of being able to open this morning's debate. I also wish to particularly identify with a point the leader made. There is an old saying that most of life is just showing up. I think what the American people want—I heard this at checkout lines in our local stores, for example, this week—they want everybody back in Washington and going to work on this issue, just as the leader suggested.

I think Senators know I am a charter member of what I guess you could call the optimist caucus in the Senate. As improbable as some of these talking heads say on TV that it is, I still think we ought to be here, just as the leader said, working on this issue because of the consequences.

Mr. REID. Mr. President, will my friend yield for a question?

Mr. WYDEN. I would be happy to yield to the majority leader.

Mr. REID. The distinguished Senator from Oregon and I served together in the House of Representatives. Does the Senator remember the days when the House voted not as a majority but as a body to come up with how legislation should be given to the American people? Does my friend remember that?

Mr. WYDEN. I do. The leader is being logical, and Heaven forbid that sometimes logic break out on some of these matters. I remember when we started out—and I joked that I had a full head of hair and rugged good looks—the majority leader and I used to work with people on both sides of the aisle. We would try to show up early, go home late, and, as the leader said, focus on getting some results. I thank the leader for his point and again for the honor of being able to start this discussion.

As I indicated, what I heard at home is that we are supposed to be here and try to find some common ground. I know the talking heads on TV say this is impossible and it cannot be done. First of all, as the majority leader said, this has been done in the past. When there are big issues and big challenges, historically the Congress will come together and deal with it.

I am particularly concerned about some of the effects going over the cliff will have on vulnerable senior citizens. As the Presiding Officer knows, that is my background. We have often talked about health care and seniors. My background was serving as codirector of the Oregon Gray Panthers. If the reimbursement system for Medicare, in

effect, goes over this cliff, that is going to reduce access to health care for senior citizens across the country, and I don't believe there are Democrats and Republicans who want that to happen.

As the majority leader indicated, finding some common ground on this issue and backing our country away from the fiscal cliff is hugely important and crucial to the well-being of our country. I just wanted to start with those remarks.

Also crucial to our country is the legislation before the Senate right now. Its name is a real mouthful.

Mr. President, I think you will recall this legislation from your days serving on the Senate Select Committee on Intelligence. The name of this is the Foreign Intelligence Surveillance Act Amendments Act. It also expires in a few days. Our job is to find a way to strike the best possible balance between protecting our country from threats from overseas and safeguarding the individual liberties of the law-abiding Americans we have cherished in this country for literally hundreds of years. This task of balancing security and liberty was one of the most important tasks defined by the Founding Fathers years and years ago, and it is no less important for the Congress today.

As I indicated earlier, the majority leader, Leader REID, has accorded me the honor of beginning this debate. I will open with a very short explanation of what the FISA Amendments Act is all about. Of course, this is an extension of the law that was passed in 2008. It is a major surveillance law, and it is the successor to the warrantless wiretapping program that operated under the Bush administration, which gave the government new authorities to collect the communications of foreigners outside the United States. The bill before the Senate today would extend this law for another 5 years.

There is going to be a discussion of various issues, but all of them go to what I call the constitutional teetertotter, which is basically balancing security, protecting our country at a dangerous time, and the individual liberties that are so important to all of us. I expect there will be amendments to strengthen protections for the privacy of law-abiding Americans.

I want to say to my colleagues and those who are listening that this is likely to be the only floor debate the Senate has on this law encompassing literally a 9-year period—from 2008 to 2017. So if we are talking about surveillance authority that essentially looks to a 9-year period, we ought to have an important discussion about it, and that is why I am grateful to the majority leader for making today's discussion possible.

I have served on the Senate Intelligence Committee for 12 years now, and I can tell every Member of this body that those who work in the intelligence community are hard-working and patriotic men and women. They give up an awful lot of evenings, weekends, and vacations to try to protect the well-being and security of our country. For example, we hear a lot about a well-publicized event, such as their enormously valuable role in apprehending bin Laden. What we don't hear about is the incredible work they do day in and day out. They work hard to gather intelligence, and I commend them for it as we begin this discussion.

The job of those who work in the intelligence community is to follow whatever laws Congress lays down as those hard-working men and women collect intelligence. Our job here in the Congress is to make sure the laws we pass are in line with the vision of the Founding Fathers, which was to protect national security as well as the rights of individual Americans.

We all remember the wonderful comment by Ben Franklin. I will paraphrase it, but essentially Ben Franklin said: If you give up your liberty to have security, you really don't deserve either. We owe it to the hard-working men and women in the intelligence community to work closely with them. We need to find the balance Ben Franklin was talking about, and we can help them by conducting robust oversight over the work that is being done there so members of the public can have confidence in the men and women of the intelligence community. This will give the public the confidence to know that as we protect our security at a dangerous time, we are also protecting the individual liberties of our people.

The story with respect to this debate really begins in early America when the colonists were famously subjected to a lot of taxes by the British Government. The American colonists thought this was unfair because they were not represented in the British Parliament. They argued that if they were not allowed to vote for their own government, then they should not have to pay taxes.

We all remember the renowned rallying cry of the colonists. It was ''no taxation without representation.'' Early revolutionaries engaged in protests against these taxes all over the country. Of course, the most famous of these protests was the Boston Tea Party in which colonists threw shiploads of tea into the Boston Harbor in protest of the tax on tea.

As we recall from our history books, there were a lot of taxes on items such as tea, sugar, paint, and paper. Because so many colonists believed these taxes were unjust, there was a lot of smuggling going on in the American Colonies. People would import things, such as sugar, and simply avoid paying the tax on them.

We all remember that the King of England didn't like this very much. He wanted the colonists to pay taxes whether they were allowed to vote or not. So the English authority began issuing what were essentially general warrants. They were called writs of assistance, and they authorized government officials to enter into any house or building they wanted in order to search for smuggled goods. These officials were not limited to only searching in certain houses, and they were not required to show any evidence that the place they were searching had any smuggled goods in it. Basically, government officials were allowed to say they were looking for smuggled goods and then would search any house they were interested in to see if the house had some of those smuggled goods.

An English authority's goal is to find smuggled goods. Letting constables and customs officers search any house or building is a pretty effective way to go out and find something. If they keep searching enough houses, eventually they will find some smuggled goods in one of them and seize those goods and arrest whoever lives in that house for smuggling. Of course, the problem is that if government officials can search any house they want, they are going to search through the houses of a lot of people who have not broken any laws.

Mr. President, it is almost as if you decided you were going to search everybody in your State of Rhode Island. You could go in and turn them all upside down, shake them, and see if anything fell out. Obviously, you would find some people who had some things in their possession that they should not have, but that is not the way we do it in America. In America, there has to be probable cause in order to do something like that.

The American colonists had a huge problem with the idea that everybody's house was going to be checked for smuggled goods on the prospect that maybe somebody somewhere had engaged in smuggling. The colonists said it is not OK to go around invading people's privacy unless there is some specific evidence that they have done something wrong. That is how people in Rhode Island and Oregon feel today. One cannot just go out and check everybody in sight on the prospect that maybe there is someone who has done something wrong.

Back in the colonists' time, the law said that these writs of assistance were good until the King died. So when King George II died and the authorities had to get new writs, many colonists tried to challenge them in court.

In Boston, James Otis denounced this mass invasion of privacy by reminding the court that—and we remember this wonderful comment—a man's house is his castle. Mr. Otis described the writs of assistance as the power that places the liberty of every man in the hands of every petty officer. Unfortunately, the court ruled that these general orders permitting mass searches without individual suspicion were legal, and English authorities continued to use them. The fact that English officials went around invading people's privacy without any specific evidence against them was one of the fundamental complaints the American colonists had against the British Government. So naturally our Founding Fathers, with

the wisdom they showed on so many matters, made it clear they wanted to address this particular complaint when they wrote the Bill of Rights.

The Bill of Rights ensures that strong protections of individual freedom would be included within our Constitution itself, and the Founding Fathers included strong protections for personal privacy in the fourth amendment. The fourth amendment states:

> The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures shall not be violated and no warrant shall issue but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched and the person or things to be searched.

This was a direct rejection of the authority the British had claimed to have when they ruled the American Colonies.

The Founding Fathers said our government does not have the right to search any house that government officials want to search even if it helps them to do their job. Government officials may only search someone's house if they have evidence that someone is breaking the law and they show the evidence to a judge to get an individual warrant.

For more than 200 years, this fundamental principle has protected Americans' privacy while still allowing our government to enforce the law and to protect public safety.

As time passed and we entered the 20th century, advances in technology—a whole host of technologies—gave government officials the power to invade individual privacy in a whole host of new ways—new ways the Founding Fathers never dreamed of—and all through those days, the Congress and the courts struggled to keep up.

Time and time again Congress and the courts were most successful when they returned to the fundamental principles of the fourth amendment. It is striking. If we look at a lot of the debates we are having today about the Internet—and the Presiding Officer has a great interest in this; we have talked often about it—certainly the Founding Fathers could never have envisioned tweeting and Twitter and the Internet and all of these extraordinary technologies. But what we have seen as technology has continued to bring us this treasure trove of information with all of these spectacular opportunities the Founding Fathers never envisioned is that time and time again the Congress and the courts were most successful when they returned to the fundamental principles of the fourth amendment.

For example, in 1928 the Supreme Court considered a famous case about whether the fourth amendment made it illegal for the government to listen to an individual's phone conversations without a warrant. Once again, dating almost to the precedent about the colonists and smuggling, the 1928 case was about smuggling—specifically, bootlegging. The government argued then that as long as it did the wiretapping remotely without entering an individual's house, the fourth amendment would not apply.

Now, Justice Louis Brandeis wrote what has come to be seen in history as an extraordinary dissent, a brilliant dissent, and he argued that this was all wrong; that the fourth amendment was about preventing the government from invading Americans' privacy regardless of how the government did it.

I am just going to spend a couple of minutes making sure people see how brilliant and farsighted Justice Brandeis was in how his principles—the principles he talked about in 1928—are as valid now as they were then.

Justice Brandeis said:

> When the Fourth and Fifth Amendments were adopted . . . force and violence were then the only means known to man by which a Government could directly effect self-incrimination. . . . Subtler and more far-reaching means of invading privacy have [in effect] now become available to the Government. Discovery and invention have made it possible for the Government . . . to obtain disclosure in court of what is whispered in the closet.

Justice Brandeis goes on to say:

> In the application of a Constitution, our contemplation cannot be only of what has been but of what may be. The progress of science in furnishing the Government with means of espionage is not likely to stop with wiretapping. Ways may someday be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. ''That places the liberty of every man in the hands of every petty officer'' was said by James Otis of much less intrusions than these.

Justice Brandeis goes on to say:

> The principles—

The principles, literally—

> [behind the Fourth Amendment] affect the very essence of constitutional liberty and security. They . . . apply to all invasions on the part of the Government and its employees of the sanctities of a man's home and the privacies of life. It is not the breaking of his doors, and the rummaging of his drawers that constitutes the essence of the offense; but it is the invasion of his indefeasible right of personal security, personal liberty and private property, where the right has never been forfeited by his conviction of some public offense.

Justice Brandeis closes this remarkable dissent saying:

> . . . The evil incident to invasion of the privacy of the telephone is far greater than that involved with tampering with the mails. . . . As a means of espionage, writs of assistance and general warrants are but puny instruments of tyranny and oppression when compared with wiretapping.

The protection guaranteed by the amendments Justice Brandeis was referring to—the fourth and fifth amendments—is broad in scope.

> The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings, and of his intellect. They knew that only a part of the pain, pleasure and satisfaction of life are to be found in material things. They sought to protect Americans and their beliefs, their thoughts, their emotions, and their sensations. They conferred, as against the Government, the right to be let alone—the most comprehensive of rights, and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the Government on the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment.

Because I have outlined Justice Brandeis's dissent on several issues, I want to make sure those last two sentences are clear.

Justice Brandeis said that the right of the people to be left alone by their government is ''the most comprehensive of rights''—the most comprehensive of rights, said Justice Brandeis—and, he said, ''the right most valued by civilized men.'' And the Justice said that intrusions on individual privacy, ''whatever the means employed, must be deemed a violation of the Fourth Amendment.''

The reason I have outlined Justice Brandeis's views on this issue is that Justice Brandeis's views didn't prevail in 1928. Back in 1928 they thought they were dealing with high-tech surveillance. But suffice it to say that his views were eventually adopted by the full Supreme Court. That is why I believe it is so important that as we look to today's debate—really an opportunity to update the way in which that careful balance, the constitutional teeter-totter: security, well-being of all of us on this side and individual liberties on this side—it is so important to recognize what Justice Brandeis said about the value of getting it right when it comes to liberty, when it comes to individual freedom.

One of the reasons there are amendments being offered by Senators to this legislation at a time when we are dealing with these crucial issues about the fiscal cliff, the question of the budget, taxes, and, as I mentioned, senior citizens being able to see a doctor—those are crucial issues, but this legislation, the FISA Amendments Act, is also a crucial piece of legislation, and that is why Senators will be offering amendments in order to strike the best possible balance between security and liberty.

When the Foreign Intelligence Surveillance Act, which is often known as FISA—Senators and those listening will hear that discussion almost interchangeably; the abbreviated name is FISA—when it was written in 1978, Congress applied Justice Brandeis's principles to intelligence gathering. The Congress, when they wrote the original FISA legislation in 1978, really said that Justice Brandeis got it right with respect to how we ought to gather intelligence. So the original FISA statute stated that if the government wants to collect an American's communications for intelligence purposes, the government must go to a court, show evidence that the American is a terrorist or a spy, and get an individual

warrant. This upheld the same principle the Founding Fathers fought for in the revolution, it is the same principle enshrined in the Bill of Rights, and it said that government officials are not allowed to invade Americans' privacy unless they have specific evidence and an individual warrant.

After 9/11, the Bush administration decided it would seek additional surveillance authorities beyond what was in the original Foreign Intelligence Surveillance Act statute. To our great regret, instead of asking the Congress to change the law, the Bush administration developed a warrantless wiretapping program—let me repeat that, a warrantless wiretapping program—that operated in secret for a number of years. When this became public—as I have said on this floor before, these matters always do become public at some point—when it became clear that the Bush administration had developed this warrantless wiretapping program, there was a huge uproar across the land. I remember how angry many of my constituents were when they learned about the warrantless wiretapping program, and I and a lot of other Senators were very angry as well.

As has the Presiding Officer, I have been on the Intelligence Committee, and I have been a member for 12 years, but the first time I heard about the warrantless wiretapping program—the first time I heard about it—was when I read about it in the newspapers. It was in the New York Times before I, as a member of the Senate Select Committee on Intelligence, knew about it.

There was a very heated debate. Congress passed the FISA Amendments Act of 2008, and that was to replace the warrantless wiretapping program with new authorities for the government to collect the phone calls and e-mails of those believed to be foreigners outside the United States.

The centerpiece of the FISA Amendments Act is a provision that is now section 702 of the FISA statute. Section 702 is the provision that gave the government new authorities to collect the communications of people who are believed to be foreigners outside the United States. This was different than the original FISA statute. Unlike the traditional FISA authorities and unlike law enforcement wiretapping authorities, section 702 of the FISA Amendments Act does not involve obtaining individual warrants. Instead, it allows the government to get what is called a programmatic warrant. It lasts for an entire year and authorizes the government to collect a potentially large number of phone calls and e-mails, with no requirement that the senders or recipients be connected to terrorism, espionage—the threats we are concerned about.

If that sounds familiar, it certainly should. General warrants that allowed government officials to decide whose privacy to invade were the exact sort of abuse that the American colonists protested over and led the Founding Fathers to adopt the fourth amendment in the first place. For this reason, section 702 of the FISA law contains language that is specifically intended to limit the government's ability to use these new authorities to spy on Americans.

Let me emphasize that because that is crucial to this discussion and the amendments that will be offered. It is never OK—never OK—for government officials to use a general warrant to deliberately invade the privacy of a law-abiding American. It was not OK for constables and Customs officials to do it in colonial days, and it is not OK for the National Security Agency to do it today. So if the government is going to use general warrants to collect people's phone calls and e-mails, it is extremely important to ensure that this authority is only used against foreigners overseas and not against law-abiding Americans.

Despite what the Acting President pro tempore and the Senate may have heard, this law does not actually prohibit the government from collecting Americans' phone calls and e-mails without a warrant. The FISA Amendments Act states—and I wish to quote because there have been a lot of inaccuracies and misrepresentations on this—the FISA Amendments Act states that acquisitions made under section 702 may not ''intentionally target'' a specific American and may not ''intentionally acquire'' communications that are ''known at the time of acquisition'' to be wholly domestic.

But the problem with that is, it still leaves a lot of room for circumstances under which Americans' phone calls and e-mails—including purely domestic phone calls and e-mails—could be swept up and reviewed without a warrant. This can happen if the government did not know someone is American or if the government made a technical error or if the American was talking to a foreigner, even if that conversation was entirely legitimate.

I am not talking about some hypothetical situation. The FISA Court, in response to a concern I and others have had, has already ruled at least once that collection carried out by the government under the FISA Amendments Act violated the fourth amendment to the Constitution. Senate rules regarding classified information prevent me from discussing the details of that ruling or how many Americans were affected, over what period of time, but this fact alone clearly demonstrates the impact of this law on Americans' privacy has been real and it is not hypothetical.

When the Congress passed the FISA Amendments Act 4 years ago, it included an expiration date. The point of the expiration date was to ensure that Congress could review these authorities closely and the Congress could decide whether protections for Americans' privacy are adequate or whether they need to be modified.

Again, go back to what I have described as the constitutional teetertotter—our job: balance the need of the government to collect information, particularly with respect to what can be threats coming from overseas, with the right of individual Americans to be left alone. It is that balance we are discussing. If the Congress finds it is unbalanced, the Congress has a responsibility to step up and figure out how to make the appropriate changes in the law to ensure that both security and privacy are being protected simultaneously.

Unfortunately, the Congress and the public—the American people—do not currently have enough information to adequately evaluate the impact of the law we are debating on Americans' privacy. There are a host of important issues about the law's impact that intelligence officials have simply refused to answer publicly.

I am going to now spend a few minutes outlining the big questions I believe Americans deserve answers to. Certainly, the Congress has to have answers to these questions in order to do our job—our job of doing robust oversight over this law and over intelligence, which, as I said a bit ago, is exactly what the hard-working men and women in the intelligence community need and deserve in order to do their job in a way that will generate confidence among the American people.

First, if we want to know what kind of impact this law has had on Americans' privacy, we probably want to know roughly how many phone calls and e-mails that are to and from Americans have been swept up by the government under this authority. Senator MARK UDALL, our distinguished colleague from Colorado and a great addition to the Intelligence Committee—he and I began the task of trying to ferret out this information some time ago. Over a year and a half ago, Senator MARK UDALL and I asked the Director of National Intelligence how many Americans have had their communications collected under this law; in effect, swept up by the government under these authorities.

The response was it is ''not reasonably possible to identify the number of people located in the United States whose communications may have been reviewed under the authority of the'' FISA Amendments Act. That is how the government responded to Senator UDALL and me.

If you are a person who does not like the idea of government officials secretly reviewing your phone calls and e-mails, you probably do not find that answer particularly reassuring. But suffice it to say, the situation got worse from there.

In July of this year, I and a tripartisan group of 12 other Senators, including Senator MARK UDALL, our colleague from Utah, Senator MIKE LEE, Senator DURBIN—I am pleased to be joined by Senator MERKLEY, who has been vital in this coalition, this

tripartisan coalition to get the best possible balance between security and liberty—he was a signer of the letter; Senator PAUL of Kentucky, who has also been an outspoken advocate of striking a better balance between privacy and liberty was a signer; Senator COONS, Senator BEGICH, Senator BINGAMAN, Senator TESTER, Senator SANDERS, Senator TOM UDALL, Senator CANTWELL—all of us joined in writing another letter to the Director of National Intelligence asking additional questions about the impact of this law on Americans' privacy.

We asked the Director if he could give us even a rough estimate—just a rough estimate—in other words, there has been discussion both in the press and in the intelligence community: This group of Senators is asking for something impossible. This group of Senators is asking for an exact count of how many Americans are being swept up under this FISA authority, their calls and e-mails reviewed. I wish to emphasize we just said, as a tripartisan group of Senators: We would just like a rough estimate—use any approach they want in terms of giving us an assessment of how many Americans' communications have been swept up in this way. Is it hundreds? Is it hundreds of thousands? Is it millions?

The tripartisan group of Senators basically was just asking for a report, the kind of information that is a prerequisite to doing good oversight. Frankly, I think when we talk about oversight and we cannot even get a rough estimate of how many law-abiding Americans have had their communications swept up under this law, if they do not have that kind of information, oversight—the idea of robust oversight—it ought to be called toothless oversight if they do not have that kind of information.

The Director declined to publicly answer this question. So our tripartisan group and others continued. We asked the Director if anyone else has already done such an estimate. We did not ask about doing anything new. The intelligence community said: Oh, my goodness. It will be so hard to give even a rough estimate. So we said: OK. Just tell us if anyone else has already done such an estimate. The Director declined to publicly answer this question as well.

Right at the heart of this discussion is, if we are serious about doing oversight, the Congress ought to be able to get a straightforward answer to the question: Have any estimates been done already as to whether law-abiding Americans have had their communications swept up under the FISA authority?

Second, if we want to understand this law's impact on Americans' privacy, we probably want to know whether any wholly domestic communications have been collected under the FISA authorities. When we are talking about wholly domestic communications, we are talking about one person in the United States talking to another person who is also in the United States. This law contains a number of safeguards that many people thought would prevent the warrantless collection of wholly domestic U.S. communications, and I think the Congress ought to know whether these safeguards are working.

So our tripartisan group of Senators dug into this issue as well, and we asked the Director back in July if he knew whether any wholly domestic U.S. communications had been collected under the FISA Amendments Act. So here we are talking about wholly domestic communications from one American, for example, in Rhode Island, to another American in the home State of Senator MERKLEY and myself. I am disappointed to say the Director declined to answer this question as well.

Let's contemplate that for a moment. A tripartisan group of Senators—Democrats, Republicans, Independents—asked if the government knew whether any wholly domestic communications had been collected under the FISA law, and the head of the intelligence community declined to publicly provide a simple yes or no response to that question.

That means the FISA Amendments Act involves the government going to a secret court on a yearly basis and getting programmatic warrants to collect people's phone calls and e-mails, with no requirement that these communications actually belong to people involved with terrorism or espionage. This authority is not supposed to be used against Americans, but, in fact, intelligence officials say they do not even know how many American communications they are actually collecting. The fact is, once the government has this pile of communications, which contains an unknown but potentially very large number of Americans' phone calls and e-mails, there are surprisingly few rules about what can be done with it.

For example, there is nothing in the law that prevents government officials from going to that pile of communications and deliberately searching for the phone calls or e-mails of a specific American, even if they do not have any actual evidence that the American is involved in some kind of wrongdoing, some kind of nefarious activity.

Again, if it sounds familiar, it ought to because that is how I began this discussion, talking about these sorts of general warrants that so upset the colonists. General warrants allowing government officials to deliberately intrude on the privacy of individual Americans at their discretion was, as I have outlined this morning, the abuse that led America's Founding Fathers to rise up against the British. They are exactly what the fourth amendment was written to prevent.

If government officials wanted to search an American's house or read their e-mails or listen to their phone calls, they are supposed to show evidence to a judge and get an individual warrant. But this loophole in the law allowed government officials to make an end run around traditional warrant requirements and conduct backdoor searches for American's communications.

Now, let me be clear. If the government has clear evidence that an American is engaged in terrorism, espionage—serious crimes—I think the government ought to be able to read that person's e-mails and listen to that person's phone calls. I believe and have long felt that is an essential part of protecting public safety. But government officials ought to be required to get a warrant. As the Presiding Officer knows, there are even emergency provisions—and I support these strongly as well—that allow for an emergency authorization before you get the warrant, in order to protect the well-being of the American people.

So what we want to know at this point, if you are trying to decide whether the constitutional teeter-totter is being properly balanced or is out of whack, you want to know whether the government has ever taken advantage of this backdoor search loophole and conducted a warrantless search for the phone calls or e-mails of specific Americans. So when the tripartisan group wrote to the Director of National Intelligence, we asked him to state whether the intelligence community has ever deliberately conducted a warrantless search of this nature. The Director declined to respond to this as well—declined to respond to a tripartisan group of Senators simply asking: Has the intelligence community ever deliberately conducted a warrantless search of this nature?

If anybody is kind of keeping score on this, you will notice that the Director refused to publicly answer any of the questions that were asked in our letter. So if you are looking for reassurance that the law is being carried out in a way that respects the privacy of law-abiding American citizens, you will not find it in his response.

I should note that the Director did provide additional responses in a highly classified attachment to his letter. This attachment was so highly classified that I think of the 13 Senators who signed the letter of the tripartisan group, 11 of those 13 Senators do not even have staff who have the requisite security clearance to read it. So naturally that makes it hard for those Senators, let alone the public, to gain a better understanding of the privacy impact of the law.

Several Senators sent the Director a followup letter last month again urging him to provide public answers to what we felt were straightforward questions—really sort of a minimum set of responses that the Congress needs to do oversight. The Director refused that as well.

Intelligence officials do not deny the facts I have outlined this morning.

They still insist they are already protecting innocent Americans' privacy. There is a lot of discussion about how this program is overseen by the secret FISA Court, how the court is charged with ensuring that all of the collections carried out under this program are constitutional.

To respond to those arguments, I would note that under the FISA Amendments Act, the government does not have to get the permission of the FISA Court to read particular e-mails or listen to particular phone calls. The law simply requires the court to review the government's collection and handling procedures on an annual basis. There is no requirement in the law for the court to approve the collection and review of individual communications even if government officials set out to deliberately read the e-mails of an American citizen.

Even when the court reviews the government's collection and handling procedures, it is important to note that the FISA Court's ruling are made entirely in secret. It may seem hard to believe, but the court's rulings that interpret major surveillance law and even the U.S. Constitution in significant ways—these are important judgments—the public has absolutely no idea what the court is actually saying. What that means is that our country is in effect developing a secret body of law so that most Americans have no way of finding out how their laws and their Constitution are being interpreted. That is a big problem. Americans do not expect to know the details of how government agencies collect information, but Americans do expect those agencies to operate within the boundaries of publicly understood law. Americans need and have a right to know how those laws and the Constitution are interpreted so they can ratify the decisions that elected officials make on their behalf. To put it another way, I think we understand that Americans know that intelligence agencies sometimes have to conduct secret operations, but the American people do not expect these agencies to rely on secret law.

I think we understand that the work of the intelligence community is so extraordinarily important. I see the distinguished chair of the committee here. Every member of our committee—every member—feels that it is absolutely critical to protect the sources and methods by which the work of the intelligence community is being done. But we do not expect the public to, in effect, just accept secret law.

When you go to your laptop and you look up a law, it is public. It is public. But what I have described is a growing pattern of secret law that makes it harder for the American people to make judgments about the decisions that are being made by those in the intelligence community. I think that can undermine the confidence the public has in the important work being done by the intelligence community.

If you think back to colonial times, when the British Government was issuing writs of assistance and general warrants, the colonists were at least able to challenge those warrants in open court. So when the courts upheld those writs of assistance, ordinary people could read about the decisions, and people such as James Otis and John Adams could publicly debate whether the law was adequately protecting the privacy of law-abiding individuals. But if the FISA Court were to uphold something like that today, in the age of digital communications and electronic surveillance, it could conceivably pass entirely unnoticed by the public, even by those people whose privacy was being invaded.

Since 2008 other Senators and I have urged the Department of Justice and the intelligence community to establish a regular process for reviewing, redacting, and releasing the opinions of the FISA Court that contain significant interpretation of the law so that members of the public have the opportunity to understand what their government thinks their law and their Constitution actually mean. I am not talking about a need to release every single routine decision made by the court. Obviously, most of the cases that come before the court contain sensitive information about intelligence sources and methods that are appropriate to keep secret.

I do not take a backseat to any Member of this body in terms of protecting the sources and methods of those in the intelligence community doing their important work, but the law itself should never be secret. What Federal courts think the law and the fourth amendment to the Constitution actually mean should never be a secret from the American people, the way it is today.

I am going to wrap up. I see Senator MERKLEY and Senator FEINSTEIN here. I have a couple of additional points.

I was encouraged in 2009 when the Obama administration wrote to Senator ROCKEFELLER and myself to inform us that they would be setting up a process for redacting and releasing those FISA Court opinions that contained significant interpretations of law. Unfortunately, over 3 years later, this process has produced literally zero results. Not a single redacted opinion or summary of FISA Court rulings has been released. I cannot even tell if the administration still intends to fulfill this promise. I often get the feeling they are hoping people will go away and forget that the promise was made in the first place.

I should note, in fairness, that while the administration has so far failed to fulfill this promise, the intelligence community has sometimes been willing to declassify specific information about the FISA Court's rulings in response to requests from myself and other Senators. For example, in response to a request I made this past summer, the intelligence community acknowledged that on at least one occasion—this was an acknowledgement from the intelligence community. The intelligence community acknowledged that at least on one occasion, the FISA Court had ruled that collection carried out by the government under the FISA Amendments Act violated the fourth amendment to the Constitution. I think that is an important point to remember when you hear people saying the law is adequately protecting Americans' privacy.

I would also note that on this point, partially declassified internal reviews of the FISA amendments collection act have noted that certain types of compliance issues continue to occur—continue to occur.

I have two last points. Beyond the fact that the programmatic warrants authorized by the FISA Amendments Act are approved by a secret court, the other thing that intelligence officials cite is that there are ''minimization'' procedures to deal with the issues that those of us who are concerned about privacy rights have raised. This is an odd term, but it simply refers to rules for dealing with information about Americans.

Intelligence officials will tell you that these are pretty much taking care of everything, and if there are not enough privacy protections in the law itself, minimization procedures provide all of the privacy protections any reasonable person could ever want or need. These minimization procedures are classified, so most people are never going to know what they say. As someone who has access to the minimization procedures, I will make it clear that I think they are certainly better than nothing, but there is no way, colleagues, these minimization procedures ought to be a substitute for having strong privacy protections written into the law.

I will close with the reason I feel so strongly about this, which is that senior intelligence officials have sometimes described these handling procedures in misleading ways and make protections for Americans' privacy sound stronger than they actually are. I was particularly disappointed when the Director of NSA did this recently at a large technology conference.

In response to a question about the National Security Agency's surveillance of Americans, General Alexander referenced the FISA Amendments Act and talked in particular about the minimization procedures that applied to the collection of U.S. communications. Understand that this was at a big, open technology conference. General Alexander said that when the NSA sweeps up communications from a ''good guy,'' which I think we all assume is a law-abiding American, the NSA has ''requirements from the FISA court and the Attorney General to minimize that, which means nobody else can see it unless there is a crime that is being committed.'' Now, anybody who hears that phrase says: That

is pretty good. I imagine that is what people in that technology meeting and the conference call wanted to hear. The only problem is that it is not true. It is not true at all. The privacy protections provided by these minimization procedures are simply not as strong as General Alexander made them out to be.

In October, a few months after General Alexander made the comments, Senator UDALL and I wrote him a letter asking him to please correct the record. The first paragraphs of the letter were:

Dear General Alexander:

You spoke recently at a technology convention in Nevada, at which you were asked a question about NSA collection of information about American citizens. In your response, you focused in particular on section 702 of the FISA Amendments Act of 2008, which the Senate will debate later this year. In describing the NSA's collection of communications under the FISA Amendments Act, you discussed rules for handling the communications of U.S. persons.

General Alexander said:

We may, incidentally, in targeting a bad guy hit on somebody [sic] from a good guy, because there's a discussion there. We have requirements from the FISA Court and the Attorney General to minimize that, which means nobody else can see it unless there's a crime that's been committed.

Senator UDALL and I wrote:

We believe that this statement incorrectly characterized the minimization requirements that apply to the NSA's FISA Amendments Act collection, and portrayed privacy protections for Americans' communications as being stronger than they actually are. We urge you to correct this statement, so that Congress and the public can have a debate over the renewal of this law that is informed by at least some accurate information about the impact it has had on Americans' privacy.

General Alexander wrote us back a few weeks later and said that, of course, that is not exactly how minimization procedures work and, of course, the privacy protections aren't as strong as that.

If anyone would like to read his letter, I put it up on my Web site. I don't know why General Alexander described the minimization procedures the way he did. It is possible he misspoke. It is possible he was mistaken. But I certainly would be more sympathetic to these arguments that all these privacy protections are being taken care of if it hadn't taken Senator UDALL and I making a push to get the NSA to correct the record with respect to these minimization procedures. Frankly, I am not sure, if there hadn't been a big push by Senators who had questions about what was said at that technology conference, I am not sure the NSA would have ever corrected what they originally said about minimization.

So minimization procedures are not a bad idea, but the suggestion that we don't need privacy protections written into the law because of them is a bad idea.

Finally, at that conference, General Alexander stated: ''The story that we [the NSA] have millions or hundreds of millions of dossiers on people is absolutely false.''

I have been on the Senate Intelligence Committee for 12 years, and I don't know what the term ''dossier'' means in that context.

So in October, Senator UDALL, a member of the committee, and I asked the Director to clarify that statement. We asked:

Does the NSA collect any type of data at all on 'millions or hundreds of millions of Americans'?

I think that is a pretty straightforward question. If we are asking whether the NSA is doing a good job protecting Americans' privacy, it is one of the most basic questions of all. If General Alexander saw fit, and he was the one who said they don't keep millions of dossiers, General Alexander could have answered our question about whether they were keeping these dossiers with a simple yes or no.

Instead, the Director of the NSA replied that while he appreciated our desire to have responses to the questions on the public record, he would not provide a public answer.

Again, the Director of the NSA said: ''The story that we [the NSA] have millions or hundreds of millions of dossiers on people is absolutely false.''

So two members of the committee asked: ''Does the NSA collect any type of data at all on 'millions or hundreds of millions of Americans,' '' and the Director refused to respond.

At this point, I close by way of saying I believe the FISA Amendments Act has enabled the government to collect useful intelligence information, and my goal is to reform the legislation. The two specific things I want to do are, first, require the intelligence community to provide more information about the impact of the FISA Amendments Act on Americans' privacy and, second, to make improvements to privacy protections so we can readily see where they are most needed.

So there will be several amendments that will be offered. The amendment I will be offering is sponsored by 15 Members of the Senate. It simply says the Director of the National Intelligence Agency should submit a report to the Congress on the privacy impact of the FISA Amendments Act.

This amendment would require the report to state whether any estimate has been done, how many U.S. communications have been collected under the authority, and to provide any estimates that exist. I wish to emphasize this amendment would not require any entity to actually conduct such an estimate. The Director would be required only to provide any estimates that have already been done and, if no estimates exist, the Director could say so.

Additionally, the amendment would require the report to state whether any wholly domestic communications have been collected under the FISA Amendments Act and whether any government agencies have ever conducted any warrantless, backdoor searches. These are straightforward questions, and they are obviously relevant to understanding the scope of the law's impact on privacy.

The report would address General Alexander's confusing statements by requiring the intelligence community to simply state whether the NSA has collected any personally identifiable data on more than 1 million Americans. The Congress and the country deserve an answer to this question as well.

The amendment does not force the declassification of any information. The amendment gives the President full discretion to redact as much information from the public version of the report as he deems appropriate, as long as he tells the Congress why.

To repeat, the amendment doesn't require the intelligence community to conduct a new estimate, and the President would have full discretion to decide whether any information should be made public.

I offer this amendment because I believe every Member of Congress ought to have the answers to these questions. If your constituents are similar to mine and Senator MERKLEY's, they expect us to give government agencies the authority to protect our country and to gather intelligence on important topics, but they also expect us to conduct vigorous oversight on what those agencies are doing.

It is, I guess, a temptation to say: I don't know what is going on, so I will let somebody else look at the privacy issues and go from there. I don't think that is good oversight.

To me, at a minimum, if we don't pass a requirement that we get a rough accounting of whether there has even been an estimate done with respect to how many law-abiding Americans have been swept up under these FISA authorities, my view is that oversight becomes toothless, and that is not what our obligation over these issues is all about.

There will be other important amendments as well. Senator MERKLEY has one that I think is particularly important because it goes to this question of secret laws. Senator LEAHY seeks to promote additional accountability as well with his important amendment. My colleague Senator PAUL will be offering an amendment, an important amendment as well, with respect to reasonable searches and seizures under the fourth amendment.

We obviously have crucial work to do with respect to the fiscal cliff issue in the next few days. We talked earlier when the majority leader was here about the impact of the budget and taxes, senior citizens not being able to see doctors. It is crucial work, and I continue to be part of that optimists caucus in the Senate, believing we can still find some common ground in these last few days on the fiscal cliff and avoid going over the fiscal cliff.

That is crucial work, but striking the right balance between protecting our country and protecting our individual liberties is also important work. For

that reason, I wanted to walk through the history of the FISA Amendments Act this morning, describe why it was so important, particularly for us to get even an accounting.

Remember, this doesn't disrupt any operations in the intelligence community. This is just an accounting of how many law-abiding Americans had their communications swept up under this law. That work is crucial too.

For that reason, I hope that on a bipartisan basis, the amendments will be viewed favorably by the Senate when we begin voting. Thank you for your indulgence for being part of this discussion, presiding in the chair, and with special thanks to the distinguished majority leader who gave me the opportunity to open this discussion about FISA this morning.

I yield the floor.

The ACTING PRESIDENT pro tempore. The Senator from California.

Mrs. FEINSTEIN. Mr. President, I would like to make an opening statement, as the committee chair, on the bill that is before the Senate.

This bill is a simple bill. This is a House bill that extends, reauthorizes the FISA Amendments Act. FISA is the Foreign Intelligence Surveillance Act. The House bill reauthorizes the FISA Amendments Act for 5 years, until December 31, 2017. That is all it does.

Without Senate action, these authorities to collect intelligence expire in 4 days. That is the reason it is the House bill before us, and that is the reason I urge this body to vote no on all amendments and send this reauthorization to the President where it will be signed. If it goes past the 31st, the program will be interrupted.

This is important. Reauthorization of the FISA Amendments Act has the support of the Director of National Security, Jim Clapper; the Attorney General, Eric Holder; and other national security officials who have made clear the importance of this legislation.

Following my remarks, I would like to enter letters into the RECORD from the Attorney General and the Director of National Intelligence, saying this reauthorization is the highest legislative priority of the Intelligence Community.

Let me explain what the expiring provisions of the FISA Amendments Act do. I assume that is agreeable with the President that these letters go into the RECORD following my remarks.

The ACTING PRESIDENT pro tempore. Without objection, it is so ordered.

(See exhibit 1.)

Mrs. FEINSTEIN. Let me describe what these provisions do and why they are necessary to reauthorize.

What will expire on December 31 is title VII of FISA, which is called the FAA, the FISA Amendments Act. This authorizes the executive branch of the government to go to the FISA Court, which is a special court—and most people don't know this—of 11 Federal District Court judges appointed by the Supreme Court who review government requests for surveillance activities and obtain annual approval for a program to conduct surveillance on non-U.S. persons, in other words, surveillance on individuals who are not U.S. citizens or lawful permanent residents and who are located outside the United States.

Under current law, the Attorney General and the Director of National Intelligence may submit an application to the FISA Court. I call this a program warrant. It identifies the category of foreign persons against whom the government seeks to conduct surveillance. This application is accompanied by targeting and minimization procedures that establish how the government will determine that someone targeted for surveillance is located outside the United States; and, secondly, how it is going to minimize the acquisition and retention of any information concerning U.S. persons who are accidentally caught up in this.

If the FISA Court finds the procedures to be consistent with both law and the fourth amendment, they enter an order authorizing this kind of surveillance for 1 year—and the judges on the FISA Court have found both—and they have authorized the program to continue.

The process that follows allows the intelligence community to collect the communications of international terrorists and other non-U.S. persons who are located outside the country by, for example, acquiring electronic communications such as phone calls and e-mails sent to or from a phone number or an e-mail address known to be used by the person under surveillance.

Without this authority, the intelligence community would need to return to the process of going to the FISA Court in every individual case involving collection directed at a non-U.S. person and to prove in each case there is probable cause to believe the individual is part of or working for a foreign power or a terrorist group.

Now, here is the question: Can the government use section 702 of FISA to target a U.S. person? The answer to that is no. The law specifically prohibits the use of section 702 authorities to direct collection against—that means target—U.S. persons. So no one should think the targets are U.S. persons.

This prohibition is codified in section 702(b), which states that surveillance authorities may not be used—and let me quote the law—''to intentionally target any person known at the time of acquisition to be located in the United States or to intentionally target a United States person reasonably believed to be located outside the United States.''

Now, if the government wants to engage in electronic surveillance targeting a U.S. person for foreign intelligence purposes, it must go back to the FISA Court and it must get a specific order from that court. In an emergency, the surveillance can commence before the court order is issued, but the government still must have probable cause to believe the U.S. person is an agent of a foreign power.

Let me take a few moments to address the principal concerns some of my colleagues have expressed about this legislation, which is the effect this one provision—Section 702—may have on the privacy and civil liberties of U.S. persons. And let me say that 13 members of the Intelligence Committee who have voted in favor of the extension of the FISA Amendments Act—and against previous amendments from Senator WYDEN—do not believe privacy is being eliminated under the law this bill would reauthorize.

As I have discussed, section 702 establishes a framework for the government to acquire foreign intelligence by conducting electronic surveillance on non-U.S. persons who are reasonably believed to be located outside of the United States under a program that is annually approved by the court. The privacy concerns stem from the potential for intelligence collection directed at non-U.S. persons located abroad to result in the incidental collection of or concerning communications of U.S. persons. I understand these concerns, and I would like to explain why I believe the existing provisions are adequate to address them.

First, this section is narrowly tailored to ensure that it may only be used to target non-U.S. persons located abroad. It includes specific prohibitions on targeting U.S. persons or persons inside the United States and prohibitions on engaging in so-called reverse-targeting, which means targeting a non-U.S. person abroad when the real purpose is to obtain their communications with a person inside the United States. That is prohibited.

Anytime the intelligence community is seeking to collect the communications of an American, it has to demonstrate that it has probable cause and get an individual FISA Court order.

Second, Congress recognized at the time this amendments act was enacted that it is simply not possible to collect intelligence on the communications of a person of interest without also collecting information about the people with whom and about whom that person communicates, including, in some cases, non-targeted U.S. persons. The concern was addressed when the FAA was originally drafted. Specifically, in order to protect the privacy and civil liberty of U.S. persons, Congress mandated that for collection conducted under 702, the Attorney General adopt and the FISA Court review and approve procedures that minimize the acquisition, retention, and dissemination of nonpublic information concerning unconsenting U.S. persons.

Third, numerous reports and assessments from the executive branch that I will describe in a moment provide the committee with extensive visibility

into how these minimization procedures work and enable both the Intelligence and the Judiciary Committees to see how these procedures are effective in protecting the privacy and civil liberties of U.S. persons.

Oversight by the legislative, judicial, and executive branch of the government over the past 4 years has been very thorough. There are procedures and requirements in place under current law that provide protection for the privacy and civil liberties of U.S. persons. Those entrusted with the responsibility to collect the oversight, the committees of jurisdiction, the FISA Court, and the executive branch agencies together remain vigilant and continue to review the operations of these agencies.

Let me give a quick summary of the 702 reporting requirements under current law.

They include a semiannual assessment by the Attorney General and the DNI. Every 6 months the AG and the DNI are required to assess compliance with the targeting and minimization procedures and the acquisition guidelines adopted under Section 702. They are both further required to submit each assessment to the FISA Court and the congressional Intelligence and Judiciary Committees.

The inspector general of the Department of Justice and the inspector general of each element of the intelligence community are also authorized review compliance with Section 702. The IGs are required to provide copies of such reviews to the Attorney General, to the Director of National Intelligence, and the congressional Intelligence and Judiciary Committees. So we have the AG reviewing, we have the IGs reviewing, and then we have separate reviews by the agency heads.

The head of each element of the intelligence community must conduct an annual review which includes the following:

First, an accounting of the number of disseminated intelligence reports containing a reference to the U.S. person's identity. As a matter of fact, Members can go into a classified room at the offices of the Senate Intelligence Committee and review these reports. Any Member has access to that review.

Second, an accounting of the number of U.S. 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. Members can review that.

Third, the number of targets who were later determined to be located in the United States and, to the extent possible, whether communications of such targets were reviewed. Members can go in the Intelligence Committee offices and review that.

Fourth, a description of any procedures developed by the head of such element of the intelligence community and approved by the Director of National Intelligence to assess the extent to which acquisitions under 702 acquire communications of U.S. persons, and the results of any such assessment.

So you see, the reporting requirements go on and on.

Then there is a semiannual report. Every 6 months, the AG is required to fully inform the congressional Intelligence and Judiciary Committees concerning the implementation of Title VII of FISA, and there is a whole list of things that must be reviewed and recounted. Then there is a semiannual Attorney General review on FISA. There is also the provision for documents from the FISA Court relating to significant construction or interpretation of FISA.

Mr. President, I ask unanimous consent to have printed in the RECORD this list.

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

SUMMARY OF SECTION 702 REPORTING REQUIREMENTS

Background: The surveillance authorities added to the Foreign Intelligence Surveillance Act (''FISA'') by FISA Amendments Act (''FAA'') enable the government to conduct intelligence collection targeting persons located outside the United States. The FAA provision that receives the most attention is known as ''Section 702,'' which authorizes the government to engage in certain forms of intelligence collection targeting non-U.S. persons located overseas for foreign intelligence purposes with the assistance of U.S.-based electronic communication service providers. This Section 702 collection is approved by the FISA Court on a programmatic basis, without the need for individualized court orders. Instead, the Director of National Intelligence (DNI) and Attorney General (AG) submit annual certifications to the Court for review and approval, which identify categories of non-U.S. person targets located overseas.

Reporting Requirements Relating to Section 702: FISA imposes a series reporting requirements on the AG, DNI, and agencies within the Intelligence Community (IC) that utilize Section 702 authorities. These include, with respect to section 702:

Semiannual AG/DNI Assessments of Section 702. Every six months, the AG and DNI are required to assess compliance with the targeting and minimization procedures and the acquisition guidelines adopted under Section 702. The AG and DNI are further required to submit each assessment to the FISA Court and the congressional intelligence and judiciary committees. Section 702(l)(1) [50 U.S.C. 1881a(l)(1)].

IG Assessments of Section 702. The Inspector General of the Department of Justice and the Inspector General of each element of the intelligence community ''authorized to acquire foreign intelligence information under [Section 702]'' (e.g., the NSA IG) are ''authorized'' to review compliance with the Section 702 targeting and minimization procedures and the acquisition guidelines. Section 702(l)(2)(A) [50 U.S.C. 1881a(l)(2)(A)] (emphasis added).

In addition, the IGs are required to 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'' and ''the number of targets that were later determined to be located in the United States and, to the extent possible, whether communications of such targets were reviewed.'' Section 702(l)(2)(B), (C) [50 U.S.C. 1881a(l)(2)(B), (C)].

Finally, the IGs are required to provide copies of such reviews to the AG, DNI, and the congressional intelligence and judiciary committees. Section 702(l)(2)(D) [50 U.S.C. 1881a(l)(2)(D)].

Annual Reviews by Agency Heads of Section 702. The head of each element of the intelligence community ''conducting an acquisition authorized under [Section 702]'' (e.g., the Director of NSA) are required to conduct annual reviews to ''determine whether there is reason to believe that foreign intelligence information has been or will be obtained from the acquisition.'' Among other things, the annual review must include:

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

(2) ''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;''

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

(4) ''a description of any procedures developed by the head of such element of the intelligence community and approved by the Director of National Intelligence to assess . . . the extent to which the acquisitions authorized under [Section 702] acquire the communications of United States persons, and the results of any such assessment.''

The head of each element of the intelligence community that conducts an annual review is also required to use the review to ''evaluate the adequacy of the minimization procedures utilized by such element.''

Finally, the head of each element of the intelligence community that conducts an annual review is required to provide a copy of each review to the FISA Court, AG, DNI, and the congressional intelligence and judiciary committees. Section 702(l)(3) [50 U.S.C. 1881a(l)(3)].

Semiannual AG Report on Title VII. Every 6 months, the AG is required to ''fully inform'' the congressional intelligence and judiciary committees ''concerning the implementation'' of Title VII. This reporting requirement is in addition the semiannual assessment performed under Section 702 and encompasses Section 703 and 704 of Title VII, as well as Section 702. Among other things, each report is required to include:

(1) certifications submitted in accordance with Section 702;

(2) justification for any exercise of the emergency authority contained in Section 702;

(3) directives issued under Section 702;

(4) ''a description of the judicial review during the reporting period . . . including a copy of an order or pleading in connection with such review that contains a significant legal interpretation of the provisions of [Section 702];''

(5) actions taken to challenge or enforce a directive under Section 702;

(6) compliance reviews of acquisitions authorized under Section 702;

(7) a description of any incidents of noncompliance with directives, procedures, or guidelines issued under Section 702; and

(8) the total number of applications made for orders under Sections 703 and 704, as well as the total number of such orders granted, modified; and denied; and the number of AG-

authorized emergency acquisitions under these sections. Section 707 [50 U.S.C. 1881f].

Semiannual AG Report on FISA. Every 6 months, the AG is required to submit a report to the congressional intelligence and judiciary committees concerning the implementation of FISA. This reporting requirement comes in addition to both the Section 702 semiannual assessment and the Title VII semiannual report and encompasses all the provisions of the Act. In addition to requirements that pertain to Titles I–V of FISA, the report must include a ''summary of significant legal interpretations'' involving matters before the FISA Court and copies of all decisions, orders, or opinions of the FISA Court that include ''significant construction or interpretation'' of any provision of FISA, including Section 702. Section 601(a) [50 U.S.C. 1871(a)].

Provision of Documents Relating to Significant Construction or Interpretation of FISA. Within 45 days of any decision, order, or opinion issued by the FISA Court that ''includes significant construction or interpretation of any provision of [FISA]'' (including Section 702), the AG is required to submit to the congressional intelligence and judiciary committees ''a copy of the decision, order, or opinion'' and any ''pleadings, applications, or memoranda of law associated with such decision, order, or opinion.'' Section 601(c) [50 U.S.C. 1871(c)].

Mrs. FEINSTEIN. So, Mr. President, it is not a question of this oversight not being done. I must respectfully disagree with the Senator from Oregon on that point. There is clearly rigorous oversight, and we have done hearing after hearing, we have looked at report after report, and any Member of this body who so wishes can go and review this material in the offices of the Intelligence Committee.

Now, let me talk about a protection that does exist for privacy, but will expire if this bill is not passed. That is section 704. Under this section, the intelligence community is required to get a specific judicial order before conducting surveillance on a U.S. person located outside the United States.

Before this provision was enacted in 2008 as the product of Senators who were concerned—and they were listened to, and this was enacted—the intelligence community could conduct intelligence collection on U.S. persons outside the country with only the approval of the Attorney General but without a requirement of independent judicial review. Section 704 provides that judicial review by the special Foreign Intelligence Surveillance Court. This will only be preserved if title VII of this act is reauthorized. If it isn't, the privacy provision goes down with it.

Now, let me talk a bit more about the oversight that we have done. If you listen to some, there has been little oversight, but that is not the case. We have held numerous hearings with Directors of National Intelligence Dennis Blair and Jim Clapper; with the head of the NSA, General Alexander; and with Bob Mueller at the FBI. We have had Eric Holder appear before the committee to discuss this, and we have heard from intelligence community professionals involved in carrying out surveillance operations, the lawyers who review these operations, and, importantly, the inspectors general who carry out oversight of the program and have written reports and letters to the Congress with the results of that report.

The intelligence committee's review of these FAA surveillance authorities has included the receipt and examination of dozens of reports concerning the implementation of these authorities over the past 4 years, which the executive branch is required to provide by law. We have received and scrutinized all the classified opinions of the court that interpret the law in a significant way.

Finally, our staff has held countless briefings with officials from the NSA, the DOJ, the Office of the DNI, and the FISA Court itself, including the FBI. Collectively, these assessments, reports, and other information obtained by the Intelligence Committee demonstrate that the government implements the FAA surveillance authorities in a responsible manner, with relatively few incidents of noncompliance.

Let me say this. Where such incidents of noncompliance have arisen, they have been inadvertent. They have not been intentional. They have been the result of human error or technical defect, and they have been promptly reported and remedied. That is important. Through 4 years of oversight, from all these reports, from all the meetings, from all the hearings, we have not identified a single case in which a government official engaged in a willful effort to circumvent or violate the law.

Keep in mind the oversight performed by Congress—that is, both Houses—and the FISA court comes in addition to the extensive internal oversight of the implementation that is performed by the Department of Justice, the Director of National Intelligence, and multiple IGs.

There is a view by some that this country no longer needs to fear attack. I don't share that view, and I have asked the intelligence committee staff to compile arrests that have been made in the last 4 years in America on terrorist plots that have been stopped. There are 100 arrests that have been made between 2009 and 2012. There have been 16 individuals arrested just this year alone. Let me quickly review some of these plots. Some of these may arrests come about as a result of this program. Again, if Members want to see the specific cases where FISA Amendments Act authorities were used, they can go and look at the classified background of these cases.

First, in November, 1 month ago, two arrests for conspiracy to provide material support to terrorists and use a weapon of mass destruction. That was Raees Alam Qazi and Sheheryar Alam Qazi. They were arrested by the FBI in Fort Lauderdale, FL. The next case is another conspiracy to provide material support. Arrested were Ralph Deleon, Miguel Alejandro Santana Vidriales and Arifeen David Gojali. These three men were planning to travel to Afghanistan to attend terrorist training and commit violent jihad; third, was a plot to bomb the New York Federal Reserve Bank; fourth, a plot to bomb a downtown Chicago bar; fifth, a conspiracy to provide material support to the Islamic Jihad Union; sixth, a plot to carry out a suicide bomb attack against the U.S. Capitol in February of 2012; seventh, a plot to bomb locations in Tampa, FL; eighth, a plot to bomb New York City targets and troops returning from combat overseas; ninth, a plot to assassinate the Saudi Ambassador to the United States; and it goes on and on and on.

So I believe the FISA Amendments Act is important and these cases show the program has worked. As the years go on, I believe good intelligence is the most important way to prevent these attacks.

Information gained through programs such as this one—and through other sources as well—is able to be used to prevent future attacks. So, in the past 4 years, there have been 100 arrests to prevent something from happening in the United States, some of these plots have been thwarted because of this program. I think it is a vital program. We are doing our level best to conduct good oversight and keep abreast of the details of the program and to see that these reports come in. I have tried to satisfy Senator WYDEN but apparently have been unable to do so.

I am hopeful the Senate Intelligence Committee's 13-to-2 vote to reauthorize this important legislation will be considered by all Members.

I ask unanimous consent to have printed in the RECORD the Statement of Administrative Policy on the House bill.

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

STATEMENT OF ADMINISTRATION POLICY

H.R. 5949—FISA AMENDMENTS ACT REAUTHORIZATION ACT OF 2012

(Rep. Smith, R–TX, and 5 cosponsors, Sept. 10, 2012)

The Administration strongly supports H.R. 5949. The bill would reauthorize Title VII of the Foreign Intelligence Surveillance Act (FISA), which expires at the end of this year. Title VII of FISA allows the Intelligence Community to collect vital foreign intelligence information about international terrorists and other important targets overseas, while providing protection for the civil liberties and privacy of Americans. Intelligence collection under Title VII has produced and continues to produce significant information that is vital to defend the Nation against international terrorism and other threats. The Administration looks forward to working with the Congress to ensure the continued availability of this critical intelligence capability.

Mrs. FEINSTEIN. It states that the administration strongly supports H.R. 5949, and it goes on to say what the bill

would do. It says it is vital and it produced and continues to produce significant information that is vital to defend the Nation against international terrorism and other threats.

I am very hopeful this bill will pass without amendment and thereupon can go directly to the President for signature.

I yield the floor.

EXHIBIT 1

INSPECTOR GENERAL OF THE INTELLIGENCE COMMUNITY,
Washington, DC, June 15, 2012.

Hon. RON WYDEN,
Senate Select Committee on Intelligence, U.S. Senate, Washington, DC.
Hon. MARK UDALL,
Senate Select Committee on Intelligence, U.S. Senate, Washington, DC.

DEAR SENATOR WYDEN AND SENATOR UDALL: Thank you for your 4 May 2012 letter requesting that my office and the National Security Agency (NSA) Inspector General (IG) determine the feasibility of estimating ''how many people inside the United States have had their communications collected or reviewed under the authorities granted by section 702'' of the FISA Amendment Act (FAA). On 21 May 2012, I informed you that the NSA Inspector General, George Ellard, would be taking the lead on the requested feasibility assessment, as his office could provide an expedited response to this important inquiry.

The NSA IG provided a classified response on 6 June 2012. I defer to his conclusion that obtaining such an estimate was beyond the capacity of his office and dedicating sufficient additional resources would likely impede the NSA's mission. He further stated that his office and NSA leadership agreed that an IG review of the sort suggested would itself violate the privacy of U.S. persons.

As I stated in my confirmation hearing and as we have specifically discussed, I firmly believe that oversight of intelligence collection is a proper function of an Inspector General. I will continue to work with you and the Committee to identify ways that we can enhance our ability to conduct effective oversight. If you have any questions concerning this response, please contact me.

Sincerely,

I. CHARLES MCCULLOUGH, III,
Inspector General of the Intelligence Community.

DIRECTOR OF NATIONAL INTELLIGENCE,
Washington, DC.

Hon. RON WYDEN,
U.S. Senate.
Hon. MIKE LEE
U.S. Senate.
Hon. RAND PAUL,
U.S. Senate.
Hon. MARK BEGICH,
U.S. Senate.
Hon. JON TESTER,
U.S. Senate.
Hon. TOM UDALL,
U.S. Senate.
Hon. MARIA CANTWELL,
U.S. Senate.
Hon. MARK UDALL,
U.S. Senate.
Hon. JEFF MERKLEY,
U.S. Senate.
Hon. CHRIS COONS,
U.S. Senate.
Hon. JEFF BINGAMAN,
U.S. Senate.
Hon. BERNARD SANDERS,
U.S. Senate.
Hon. DICK DURBIN,
U.S. Senate.

DEAR SENATORS: (U) Thank you for your July 26, 2012 letter on the FISA Amendments Act (FAA). As you noted, reauthorization of FAA is an extremely high priority for the Administration. The FAA authorities have proved to be an invaluable asset in our effort to detect and prevent threats to our nation and our allies.

The members of the Intelligence Community and I appreciate the need for Congress to be fully informed about this statute as it considers reauthorization. We have repeatedly reported to the Intelligence and Judiciary committees of both the House and Senate how we have implemented the statute, the operational value it has afforded, and the extensive measures we take to ensure that the Government's use of these authorities comports with the Constitution and the laws of the United States. Our record of transparency with the Congress includes many formal briefings and hearings, numerous written notifications and reports, and countless hours that our legal, operational, and compliance experts have spent in detailed discussions, briefings, and demonstrations with committee staff and counsel. In addition, we have provided classified and unclassified white papers, available to any Member of Congress, detailing how the law is implemented, the robust oversight involved, and the nature and value of the resulting collection.

(U) This extensive history of interaction with Congress has included discussions, within the past several months, of the issues raised in your letter of July 26. We have met at length with committee staff and counsel to discuss the legal and operational parameters associated with use of FAA 702. With the benefit of this information, the committees have reported FAA reauthorization legislation. We urge that it be brought to the floor of the Senate and House, and enacted without amendment as proposed by the Administration at the earliest possible date.

This degree of transparency with Congress has been possible because these hearings, briefings, reports, and discussion have generally been classified. The issues you have raised cannot be accurately and thoroughly addressed in an unclassified setting without revealing intelligence sources and methods, which would defeat the very purpose for which the laws were enacted. It remains vitally important to avoid public disclosure of sources and methods with respect to section 702 in order to protect the efficacy of this important provision for collecting foreign intelligence information.

(U) The ability to discuss these issues in a classified setting allows us to be completely transparent with Congress on behalf of the American people. We are committed to continuing that transparency. Although a meaningful and accurate unclassified response to the important questions you have asked is not possible. I am enclosing a classified response that addresses your questions in detail.

(U) That said, there is a point in your letter I would like to address directly. I strongly take exception to the suggestion that there is a ''loophole'' in the current law concerning access to communications collected under section 702 of the FAA. While our collection methods are classified, the basic standards for that collection are a matter of public law:

Section 702 only permits targeting of non-U.S. persons reasonably believed to be located outside of the United States. It does not permit targeting of U.S. persons anywhere in the world, or of any person inside the United States.

Section 702 prohibits so-called ''reverse targeting''—targeting a person located outside the United States as a pretext when the real goal is to target a person inside the United States.

Section 702 prohibits the intentional acquisition of any communication when all communicants are known at the time of acquisition to be within the United States.

(U) In enacting these standards for collection, Congress understood that some communications of U.S. persons would be incidentally acquired, and the statute therefore specifies minimization procedures that restrict that acquisition, retention, and dissemination of any information about U.S. persons. The Foreign Intelligence Surveillance Court is required by statute to ensure that those procedures are both reasonably designed to ensure compliance with the above limitations and consistent with the Fourth Amendment. In addition, components of the Executive Branch, including both my office and the Department of Justice, regularly assess compliance with the targeting and minimization procedures. Finally, the Intelligence Committees have been fully briefed on both the law and how the government collects and uses information under section 702. In short, there is no loophole in the law.

(U) As the legislation comes up for floor consideration, we would welcome the opportunity to meet with any Senator or appropriately cleared staff member to address these issues in a classified setting. I have asked Kathleen Turner, Director of my Office of Legislative Affairs, to contact your offices to try to schedule a briefing.

(U) I appreciate your taking the time to share your views with me, and I look forward to working with you to ensure that Congress has a full understanding of these and any other concerns you may have as the Senate considers legislation to reauthorize the FAA this fall.

Sincerely,

JAMES R. CLAPPER.

Enclosure.

UNCLASSIFIED upon removal of Enclosure.

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, AND UNITED STATES DEPARTMENT OF JUSTICE

Washington, DC, Feb. 8, 2012.

Hon. JOHN BOEHNER,
Speaker, United States House of Representatives, Washington, DC
Hon. HARRY REID,
Majority Leader, U.S. Senate, Washington, DC.
Hon. NANCY PELOSIm
Democratic Leader, United States House of Representatives, Washington, DC.
Hon. MITCH MCCONNELL,
Republican Leader, U.S. Senate, Washington, DC.

DEAR SPEAKER BOEHNER AND LEADERS REID, PELOSI, AND MCCONNELL: we are writing to urge that the Congress reauthorize Title VII of the Foreign Intelligence Surveillance Act (FISA) enacted by the FISA Amendments Act of 2008 (FAA), which is set to expire at the end of this year. Title VII of FISA allows the Intelligence Community to collect vital information about international terrorists and other important targets overseas. Reauthorizing this authority is the top legislative priority of the Intelligence Community.

One provision, section 702, authorizes surveillance directed at non-U.S. persons located overseas who are of foreign intelligence importance. At the same time, it provides a comprehensive regime of oversight by all three branches of Government to protect the privacy and civil liberties of U.S. persons. Under section 702, the Attorney General and the Director of National Intelligence may authorize annually, with the approval of the Foreign Intelligence Surveillance Court (FISC), intelligence collection targeting categories of non-U.S. persons abroad, without the need for a court order for each individual target. Within this framework, no acquisition may intentionally target a U.S. person, here or abroad, or any other person known to be in the United States. The law requires special procedures designed to ensure that all such acquisitions target only non-U.S. persons outside the United States, and to protect the privacy of U.S. persons whose nonpublic information may be incidentally acquired. The Department of Justice and the Office of the Director of National Intelligence conduct extensive oversight reviews of section 702 activities at least once every sixty days, and Title VII requires us to report to the Congress on implementation and compliance twice a year.

A separate provision of Title VII requires that surveillance directed at U.S. persons overseas be approved by the FISC in each individual case, based on a finding that there is probable cause to believe that the target is a foreign power or an agent, officer, or employee of a foreign power. Before the enactment of the FAA, the Attorney General could authorize such collection without court approval. This provision thus increases the protection given to U.S. persons.

The attached background paper provides additional unclassified information on the structure, operation and oversight of Title VII of FISA.

Intelligence collection under Title VII has produced and continues to produce significant intelligence that is vital to protect the nation against international terrorism and other threats. We welcome the opportunity to provide additional information to members concerning these authorities in a classified setting. We are always considering whether there are changes that could be made to improve the law in a manner consistent with the privacy and civil liberties interests of Americans. Our first priority, however, is reauthorization of these authorities in their current form. We look forward to working with you to ensure the speedy enactment of legislation reauthorizing Title VII, without amendment, to avoid any interruption in our use of these authorities to protect the American people.

Sincerely,

JAMES R. CLAPPER,
Director of National Intelligence.
ERIC H. HOLDER, JR.,
Attorney General.

BACKGROUND PAPER ON TITLE VII OF FISA PREPARED BY THE DEPARTMENT OF JUSTICE AND THE OFFICE OF DIRECTOR OF NATIONAL INTELLIGENCE (ODNI)

This paper describes the provisions of Title VII of the Foreign Intelligence Surveillance Act (FISA) that were added by the FISA Amendments Act of 2008 (FAA). Title VII has proven to be an extremely valuable authority in protecting our nation from terrorism and other national security threats. Title VII is set to expire at the end of this year, and its reauthorization is the top legislative priority of the Intelligence Community.

The FAA added a new section 702 to FISA, permitting the Foreign Intelligence Surveillance Court (FISC) to approve surveillance of terrorist suspects and other foreign intelligence targets who are non-U.S. persons outside the United States, without the need for individualized court orders. Section 702 includes a series of protections and oversight measures to safeguard the privacy and civil liberties interests of U.S. persons. FISA continues to include its original electronic surveillance provisions, meaning that, in most cases, an individualized court order, based on probable cause that the target is a foreign power or an agent of a foreign power, is still required to conduct electronic surveillance of targets inside the United States. Indeed, other provisions of Title VII extend these protections to U.S. persons overseas. The extensive oversight measures used to implement these authorities demonstrate that the Government has used this capability in the manner contemplated by Congress, taking great care to protect privacy and civil liberties interests.

This paper begins by describing how section 702 works, its importance to the Intelligence Community, and its extensive oversight provisions. Next, it turns briefly to the other changes made to FISA by the FAA, including section 704, which requires an order from the FISC before the Government may engage in surveillance targeted at U.S. persons overseas. Third, this paper describes the reporting to Congress that the Executive Branch has done under Title VII of FISA. Finally, this paper explains why the Administration believes it is essential that Congress reauthorize Title VII.

1. SECTION 702 PROVIDES VALUABLE FOREIGN INTELLIGENCE INFORMATION ABOUT TERRORISTS AND OTHER TARGETS OVERSEAS, WHILE PROTECTING THE PRIVACY AND CIVIL LIBERTIES OF AMERICANS

Section 702 permits the FISC to approve surveillance of terrorist suspects and other targets who are non-U.S. persons outside the United States, without the need for individualized court orders. The FISC may approve surveillance of these kinds of targets when the Government needs the assistance of an electronic communications service provider.

Before the enactment of the FAA and its predecessor legislation, in order to conduct the kind of surveillance authorized by section 702, FISA was interpreted to require that the Government show on an individualized basis, with respect to all non-U.S. person targets located overseas, that there was probable cause to believe that the target was a foreign power or an agent of a foreign power, and to obtain an order from the FISC approving the surveillance on this basis. In effect, the Intelligence Community treated non-U.S. persons located overseas like persons in the United States, even though foreigners outside the United States generally are not entitled to the protections of the Fourth Amendment. Although FISA's original procedures are proper for electronic surveillance of persons inside this country, such a process for surveillance of terrorist suspects overseas can slow, or even prevent, the Government's acquisition of vital information, without enhancing the privacy interests of Americans. Since its enactment in 2008, section 702 has significantly increased the Government's ability to act quickly.

Under section 702, instead of issuing individual court orders, the FISC approves annual certifications submitted by the Attorney General and the DNI that identify categories of foreign intelligence targets. The provision contains a number of important protections for U.S. persons and others in the United States. First, the Attorney General and the DNI must certify that a significant purpose of the acquisition is to obtain foreign intelligence information. Second, an acquisition may not intentionally target a U.S. person. Third, it may not intentionally target any person known at the time of acquisition to be in the United States. Fourth, it may not target someone outside the United States for the purpose of targeting a particular, known person in this country. Fifth, section 702 prohibits 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 in the United States. Finally, it requires that any acquisition be consistent with the Fourth Amendment.

To implement these provisions, section 702 requires targeting procedures, minimization procedures, and acquisition guidelines. The targeting procedures are designed to ensure that an acquisition only targets persons outside the United States, and that it complies with the restriction on acquiring wholly domestic communications. The minimization procedures protect the identities of U.S. persons, and any nonpublic information concerning them that may be incidentally acquired. The acquisition guidelines seek to ensure compliance with all of the limitations of section 702 described above, and to ensure that the Government files an application with the FISC when required by FISA.

The FISC reviews the targeting and minimization procedures for compliance with the requirements of both the statute and the Fourth Amendment. Although the FISC does not approve the acquisition guidelines, it receives them, as do the appropriate congressional committees. By approving the certifications submitted by the Attorney General and the DNI as well as by approving the targeting and minimization procedures, the FISC plays a major role in ensuring that acquisitions under section 702 are conducted in a lawful and appropriate manner.

Section 702 is vital in keeping the nation safe. It provides information about the plans and identities of terrorists, allowing us to glimpse inside terrorist organizations and obtain information about how those groups function and receive support. In addition, it lets us collect information about the intentions and capabilities of weapons proliferators and other foreign adversaries who threaten the United States. Failure to reauthorize section 702 would result in a loss of significant intelligence and impede the ability of the Intelligence Community to respond quickly to new threats and intelligence opportunities. Although this unclassified paper cannot discuss more specifically the nature of the information acquired under

section 702 or its significance, the Intelligence Community is prepared to provide Members of Congress with detailed classified briefings as appropriate.

The Executive Branch is committed to ensuring that its use of section 702 is consistent with the law, the FISC's orders, and the privacy and civil liberties interests of U.S. persons. The Intelligence Community, the Department of Justice, and the FISC all oversee the use of section 702. In addition, congressional committees conduct essential oversight, which is discussed in section 3 below.

Oversight of activities conducted under section 702 begins with components in the intelligence agencies themselves, including their Inspectors General. The targeting procedures, described above, seek to ensure that an acquisition targets only persons outside the United States and that it complies with section 702's restriction on acquiring wholly domestic communications. For example, the targeting procedures for the National Security Agency (NSA) require training of agency analysts, and audits of the databases they use. NSA's Signals Intelligence Directorate also conducts other oversight activities, including spot checks of targeting decisions. With the strong support of Congress, NSA has established a compliance office, which is responsible for developing, implementing, and monitoring a comprehensive mission compliance program.

Agencies using section 702 authority must report promptly to the Department of Justice and ODNI incidents of noncompliance with the targeting or minimization procedures or the acquisition guidelines. Attorneys in the National Security Division (NSD) of the Department routinely review the agencies' targeting decisions. At least once every 60 days, NSD and ODNI conduct oversight of the agencies' activities under section 702. These reviews are normally conducted on-site by a joint team from NSD and ODNI. The team evaluates and, where appropriate, investigates each potential incident of noncompliance, and conducts a detailed review of agencies' targeting and minimization decisions.

Using the reviews by Department of Justice and ODNI personnel, the Attorney General and the DNI conduct a semi-annual assessment, as required by section 702, of compliance with the targeting and minimization procedures and the acquisition guidelines. The assessments have found that agencies have ''continued to implement the procedures and follow the guidelines in a manner that reflects a focused and concerted effort by agency personnel to comply with the requirements of Section 702.'' The reviews have not found ''any intentional attempt to circumvent or violate'' legal requirements. Rather, agency personnel ''are appropriately focused on directing their efforts at non-United States persons reasonably believed to be located outside the United States.''

Section 702 thus enables the Government to collect information effectively and efficiently about foreign targets overseas and in a manner that protects the privacy and civil liberties of Americans. Through rigorous oversight, the Government is able to evaluate whether changes are needed to the procedures or guidelines, and what other steps may be appropriate to safeguard the privacy of personal information. In addition, the Department of Justice provides the joint assessments and other reports to the FISC. The FISC has been actively involved in the review of section 702 collection. Together, all of these mechanisms ensure thorough and continuous oversight of section 702 activities.

2. OTHER IMPORTANT PROVISIONS OF TITLE VII OF FISA ALSO SHOULD BE REAUTHORIZED

In contrast to section 702, which focuses on foreign targets, section 704 provides heightened protection for collection activities conducted overseas and directed against U.S. persons located outside the United States. Section 704 requires an order from the FISC in circumstances in which the target 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.'' It also requires a showing of probable cause that the targeted U.S. person is ''a foreign power, an agent of a foreign power, or an officer or employee of a foreign power.'' Previously, these activities were outside the scope of FISA and governed exclusively by section 2.5 of Executive Order 12333. By requiring the approval of the FISC, section 704 enhanced the civil liberties of U.S. persons.

The FAA also added several other provisions to FISA. Section 703 complements section 704 and permits the FISC to authorize an application targeting a U.S. person outside the United States to acquire foreign intelligence information, if the acquisition constitutes electronic surveillance or the acquisition of stored electronic communications or data, and is conducted in the United States. Because the target is a U.S. person, section 703 requires an individualized court order and a showing of probable cause that the target is a foreign power, an agent of a foreign power, or an officer or employee of a foreign power. Other sections of Title VII allow the Government to obtain various authorities simultaneously, govern the use of information in litigation, and provide for congressional oversight. Section 708 clarifies that nothing in Title VII is intended to limit the Government's ability to obtain authorizations under other parts of FISA.

3. CONGRESS HAS BEEN KEPT FULLY INFORMED, AND CONDUCTS VIGOROUS OVERSIGHT, OF TITLE VII'S IMPLEMENTATION

FISA imposes substantial reporting requirements on the Government to ensure effective congressional oversight of these authorities. Twice a year, the Attorney General must ''fully inform, in a manner consistent with national security,'' the Intelligence and Judiciary Committees about the implementation of Title VII. With respect to section 702, this semi-annual report must include copies of certifications and significant FISC pleadings and orders. It also must describe any compliance incidents, any use of emergency authorities, and the FISC's review of the Government's pleadings. With respect to sections 703 and 704, the report must include the number of applications made, and the number granted, modified, or denied by the FISC.

Section 702 requires the Government to provide to the Intelligence and Judiciary Committees its assessment of compliance with the targeting and minimization procedures and the acquisition guidelines. In addition, Title VI of FISA requires a summary of significant legal interpretations of FISA in matters before the FISC or the Foreign Intelligence Surveillance Court of Review. The requirement extends to interpretations presented in applications or pleadings filed with either court by the Department of Justice. In addition to the summary, the Department must provide copies of judicial decisions that include significant interpretations of FISA within 45 days.

The Government has complied with the substantial reporting requirements imposed by FISA to ensure effective congressional oversight of these authorities. The Government has informed the Intelligence and Judiciary Committees of acquisitions authorized under section 702; reported, in detail, on the results of the reviews and on compliance incidents and remedial efforts; made all written reports on these reviews available to the Committees; and provided summaries of significant interpretations of FISA, as well as copies of relevant judicial opinions and pleadings.

4. IT IS ESSENTIAL THAT TITLE VII OF FISA BE REAUTHORIZED WELL IN ADVANCE OF ITS EXPIRATION

The Administration strongly supports the reauthorization of Title VII of FISA. It was enacted after many months of bipartisan effort and extensive debate. Since its enactment, Executive Branch officials have provided extensive information to Congress on the Government's use of Title VII, including reports, testimony, and numerous briefings for Members and their staffs. This extensive record demonstrates the proven value of these authorities, and the commitment of the Government to their lawful and responsible use.

Reauthorization will ensure continued certainty with the rules used by Government employees and our private partners. The Intelligence Community has invested significant human and financial resources to enable its personnel and technological systems to acquire and review vital data quickly and lawfully. Our adversaries, of course, seek to hide the most important information from us. It is at best inefficient and at worst unworkable for agencies to develop new technologies and procedures and train employees, only to have a statutory framework subject to wholesale revision. This is particularly true at a time of limited resources. It is essential that these authorities remain in place without interruption—and without the threat of interruption—so that those who have been entrusted with their use can continue to protect our nation from its enemies.

Mr. GRASSLEY. Mr. President, the reauthorization of the Foreign Intelligence Surveillance Act Amendments Act, also known as the FISA Amendments Act, is a crucial authority for the U.S. Intelligence Community. Unless we act to pass this legislation, the law will expire in just a few days from now. It must be reauthorized immediately for a 5-year period.

I am familiar with the FISA Amendments Act, FAA, through my role as ranking member of the Judiciary Committee, which along with the Select Committee on Intelligence, has jurisdiction over this legislation and oversight of the intelligence operations conducted by the Department of Justice and Federal Bureau of Investigation. During the last year, my staff and I have engaged in extensive consultation with the intelligence community and the Department of Justice to understand how the FAA has been used. The committee held a closed hearing with witness testimony and questions from Senators as well.

We debated this legislation in committee where I opposed the version produced by the Judiciary Committee which is now the basis of the Leahy amendment. I opposed it because I have learned a great deal both about the value of the intelligence collected under the FAA and about the lengths that the intelligence community goes to protect the rights of U.S. citizens when collecting that intelligence.

Given the congressional oversight of this legislation, coupled with the built-in protections and oversight from the executive branch, the value of the intelligence gathered by this important legislation warrants reauthorization without the changes made by the Leahy amendment.

The most important portion of the FAA is Section 702. It authorizes, with approval of the Foreign Intelligence Surveillance Court, FISC, an 11-member panel of Article III judges appointed by the Supreme Court, electronic surveillance of non-U.S. persons located overseas, but without the need for individualized orders for every target of the surveillance, as is required for surveillance of anyone inside the United States. The law specifically prohibits targeting U.S. persons, acquiring wholly domestic communications, or targeting someone outside the U.S. with the intent to collect information on a target inside the U.S. known as ''reverse-targeting''.

It is possible that the communications of some U.S. citizens may be captured during the conduct of authorized surveillance. But that is only incidentally. The only way that a U.S. person's communication would be picked up would be if that person were in communication with a non-U.S. person overseas who had been targeted under the FAA.

Some people think that a U.S. person has a constitutional right not to have his communications with a foreign target eavesdropped by the U.S. government without a warrant. But that's not how the fourth amendment works. It protects the rights of the person who is being targeted, not anyone in contact with him. For example, if the government legally taps the phone of a mafia godfather in the United States, it can listen to his conversation with anyone who calls him. It doesn't need a court-issued warrant for the person calling, only for the godfather himself. He is the one who has a reasonable expectation of privacy in his telephone.

In the same way, when the government legally intercepts the communications of a terrorist living overseas, it can listen to his conversation with anyone who contacts him, even if the other party is in the United States. What matters is whether the government has the legal authority to intercept the communications of the terrorist in the first place. That's what the FAA provides. It is important to point out that no warrant is required because the target is not a U.S. citizen and is located overseas. So, the fourth amendment doesn't apply to him.

Instead, under Section 702, the FISC approves annual certifications from the attorney general and director of National Intelligence about collection of information on categories of foreign intelligence targets, what procedures the intelligence community will use to accomplish this surveillance, how they will target subjects for surveillance, and how the IC will use the information. The government must also demonstrate to the court that it has special procedures to weed out intentional collection of communications of anyone located inside the United States and to minimize the use of any incidentally collected information.

In addition, there is significant oversight of the program to protect U.S. citizens' rights. The law requires that the Attorney General and director of National Intelligence conduct semi-annual assessments of the surveillance activities. Furthermore, it authorizes the inspector general of the Department of Justice to review the program at any time. Both houses of Congress are provided the semi-annual reports and IG audits, as well as significant decisions of the FISC. These are on file with the Senate security office and any Senator and appropriately cleared staff can review them.

This process works. Our oversight of the implementation of the statute has found no evidence that it has been intentionally misused in order to eavesdrop on Americans. Senator FEINSTEIN, chair of the Senate Select Committee on Intelligence, and even Senator LEAHY, chairman of the Judiciary Committee, have stated that no such misconduct has been discovered.

For these reasons, we should reauthorize the statute without any changes, as the House has done. The only adjustment to the existing statute in the House bill is replacing the expiration date of December 31, 2012 with December 31, 2017, a 5-year period. That is also what the administration supports and what the intelligence committee passed this summer. A 5-year period would allow the intelligence community to continue utilizing these valuable tools against potential terrorists or other intelligence targets without interruption or delay. It will provide the intelligence community with much needed certainty and stability in a program that works to save American lives.

The combination of the statutory limitations on collection, targeting and minimization procedures, and acquisition guidelines, court review of those procedures and guidelines, and compliance oversight by the administration and Congress, ensure that the rights of U.S. persons are sufficiently protected when their communications are incidentally collected in the course of targeting non-U.S. persons located abroad.

I urge my colleagues to support the House passed version of the FAA reauthorization so we can ensure that there is no interruption in one of our most vital national security tools.

The ACTING PRESIDENT pro tempore. The Senator from Oregon.

AMENDMENT NO. 3435

Mr. MERKLEY. Mr. President, I call up my amendment which is at the desk.

The ACTING PRESIDENT pro tempore. The clerk will report.

The bill clerk read as follows:

The Senator from Oregon [Mr. MERKLEY] proposes an amendment numbered 3435.

Mr. MERKLEY. Mr. President, I ask unanimous consent that further reading be dispensed with.

The ACTING PRESIDENT pro tempore. Without objection, it is so ordered.

The amendment is as follows:

(Purpose: To require the Attorney General to disclose each decision, order, or opinion of a Foreign Intelligence Surveillance Court that includes significant legal interpretation of section 501 or 702 of the Foreign Intelligence Surveillance Act of 1978 unless such disclosure is not in the national security interest of the United States)

At the appropriate place, insert the following:

SEC. __. DISCLOSURE OF DECISIONS, ORDERS, AND OPINIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT.

(a) FINDINGS.—Congress finds the following:

(1) Secret law is inconsistent with democratic governance. In order for the rule of law to prevail, the requirements of the law must be publicly discoverable.

(2) The United States Court of Appeals for the Seventh Circuit stated in 1998 that the ''idea of secret laws is repugnant''.

(3) The open publication of laws and directives is a defining characteristic of government of the United States. The first Congress of the United States mandated that every ''law, order, resolution, and vote [shall] be published in at least three of the public newspapers printed within the United States''.

(4) The practice of withholding decisions of the Foreign Intelligence Surveillance Court is at odds with the United States tradition of open publication of law.

(5) The Foreign Intelligence Surveillance Court acknowledges that such Court has issued legally significant interpretations of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) that are not accessible to the public.

(6) The exercise of surveillance authorities under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), as interpreted by secret court opinions, potentially implicates the communications of United States persons who are necessarily unaware of such surveillance.

(7) Section 501 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861), as amended by section 215 of the USA PATRIOT Act (Public Law 107–56; 115 Stat. 287), authorizes the Federal Bureau of Investigation to require the production of ''any tangible things'' and the extent of such authority, as interpreted by secret court opinions, has been concealed from the knowledge and awareness of the people of the United States.

(8) In 2010, the Department of Justice and the Office of the Director of National Intelligence established a process to review and declassify opinions of the Foreign Intelligence Surveillance Court, but more than two years later no declassifications have been made.

(b) SENSE OF CONGRESS.—It is the sense of Congress that each 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 section 501 or section 702 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861 and 1881a) should be declassified in a manner consistent with the protection of national security, intelligence sources and methods, and other properly classified and sensitive information.

(c) REQUIREMENT FOR DISCLOSURES.—

(1) SECTION 501.—

(A) IN GENERAL.—Section 501 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861) is amended by adding at the end the following:

''(i) DISCLOSURE OF DECISIONS.—

''(1) DECISION DEFINED.—In this subsection, the term 'decision' means 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 this section.

''(2) REQUIREMENT FOR DISCLOSURE.—Subject to paragraphs (3) and (4), the Attorney General shall declassify and make available to the public—

''(A) each decision that is required to be submitted to committees of Congress under section 601(c), not later than 45 days after such opinion is issued; and

''(B) each decision issued prior to the date of the enactment of the _____ Act that was required to be submitted to committees of Congress under section 601(c), not later than 180 days after such date of enactment.

''(3) UNCLASSIFIED SUMMARIES.—Notwithstanding paragraph (2) and subject to paragraph (4), if the Attorney General makes a determination that a decision may not be declassified and made available in a manner that protects the national security of the United States, including methods or sources related to national security, the Attorney General shall release an unclassified summary of such decision.

''(4) UNCLASSIFIED REPORT.—Notwithstanding paragraphs (2) and (3), if the Attorney General makes a determination that any decision may not be declassified under paragraph (2) and an unclassified summary of such decision may not be made available under paragraph (3), the Attorney General shall make available to the public an unclassified report on the status of the internal deliberations and process regarding the declassification by personnel of Executive branch of such decisions. Such report shall include—

''(A) an estimate of the number of decisions that will be declassified at the end of such deliberations; and

''(B) an estimate of the number of decisions that, through a determination by the Attorney General, shall remain classified to protect the national security of the United States.''.

(2) SECTION 702.—Section 702(l) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1881a(l)) is amended by adding at the end the following:

''(4) DISCLOSURE OF DECISIONS.—

''(A) DECISION DEFINED.—In this paragraph, the term 'decision' means 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 this section.

''(B) REQUIREMENT FOR DISCLOSURE.—Subject to subparagraphs (C) and (D), the Attorney General shall declassify and make available to the public—

''(i) each decision that is required to be submitted to committees of Congress under section 601(c), not later than 45 days after such opinion is issued; and

''(ii) each decision issued prior to the date of the enactment of the _____ Act that was required to be submitted to committees of Congress under section 601(c), not later than 180 days after such date of enactment.

''(C) UNCLASSIFIED SUMMARIES.—Notwithstanding subparagraph (B) and subject to subparagraph (D), if the Attorney General makes a determination that a decision may not be declassified and made available in a manner that protects the national security of the United States, including methods or sources related to national security, the Attorney General shall release an unclassified summary of such decision.

''(D) UNCLASSIFIED REPORT.—Notwithstanding subparagraphs (B) and (C), if the Attorney General makes a determination that any decision may not be declassified under subparagraph (B) and an unclassified summary of such decision may not be made available under subparagraph (C), the Attorney General shall make available to the public an unclassified report on the status of the internal deliberations and process regarding the declassification by personnel of Executive branch of such decisions. Such report shall include—

''(i) an estimate of the number of decisions that will be declassified at the end of such deliberations; and

''(ii) an estimate of the number of decisions that, through a determination by the Attorney General, shall remain classified to protect the national security of the United States.''.

Mr. MERKLEY. Mr. President, I rise this morning to talk about the Foreign Intelligence Surveillance Act and the concerns I and many of my colleagues have.

Earlier this morning, Senator WYDEN, the senior Senator from Oregon, was discussing at length the importance of the fourth amendment, the importance of Americans knowing the boundaries and the rules under which our government collects intelligence and to know their rights to privacy are protected.

Under this Foreign Intelligence Surveillance Act, there are a variety of ways in which that assurance is compromised, and Senator WYDEN did a very good job of laying those out. I wish to emphasize that same message; that our country was founded on the principles of privacy and liberty, of protection from an overreaching central government.

During the founding, we set out and said we are going to be a new kind of nation; one that will not permit an overbearing, intrusive government spying on citizens or meddling in their private affairs. This belief was enshrined in our fourth amendment:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

I think that is an extraordinarily complete description saying that the government is bound—bound—by having to demonstrate before a court probable cause a case that is put forward and backed up by oath or affirmation, a case that is put forward with great detail about the places to be searched and the persons or things to be seized.

So the concept is laid out very clearly about what constitutes unreasonable searches and seizures. It is certainly not that the government can't collect information, just they have to show probable cause of a crime in order to create that boundary that says the information we have in our daily lives. I don't know how much broader it can be than houses, papers, and effects. It pretty much covers the entire parameter.

One of the problems we have is that sometimes lawyers start looking for loopholes, and we can address those loopholes if they are discussed in a public setting, if we can get our hands around them. But if they are loopholes created in secrecy, then indeed it is very hard to have a debate on the floor of the Senate about whether those loopholes or interpretations are right or whether we should change the law in order to address them.

Of course, our laws have had to be updated and changed over time to adapt to new technology and changing threats, and one of those developments was the creation of the Foreign Intelligence Surveillance Act in the 1970s.

In 1972, the Supreme Court held the fourth amendment does not permit warrantless surveillance for intelligence investigations within our country. One may wonder how this even took a Supreme Court decision since the fourth amendment is so absolutely clear on this point.

In 1978, Congress enacted FISA—Foreign Intelligence Surveillance Act—to regulate government surveillance within our country that is conducted for foreign intelligence purposes. Under FISA, the government had to obtain an order from a special court called the FISA Court in order to spy on Americans. This is certainly an appropriate boundary to implement. The order required the government to obtain a warrant and show probable cause. These are the same basic, commonsense protections we have had in place for other types of searches. This development required individualized and particular orders from the FISA Court to collect communications.

But now let's fast forward to 2001. President Bush decided in secret to authorize the National Security Agency to start a new program of warrantless surveillance inside the United States. This is in complete contravention of the fourth amendment and in complete contravention of the law at that time. As I am sure many of my colleagues will certainly recall, this was revealed to the American people 4 years later when it was reported in the New York Times in 2005. In response, after years of back and forth contentious debate, Congress passed the FISA Amendments Act—the bill we are considering on this floor today. We are considering a reauthorization. This law gave the government new surveillance authority but also included a sunset provision to ensure that Congress examines where the law is working and the way it was intended.

The debate we are having right now on this floor is that reexamination. I will note that I think it is unfortunate that we are doing this at the last second. We have known that this intelligence law is going to expire for years. It was laid out for a multiyear span.

Certainly, it is irresponsible for this Chamber to be debating this bill under a falsely created pressure that it needs to be done without any amendments in order to match the bill from the House. That is a way of suppressing debate on critical issues here in America.

If you care about the fourth amendment, if you care about privacy, you should be arguing that we should either create a very short-term extension in order to have this debate fully or that we should have had this debate months ago so it could have been done in a full and responsible manner, with no pressure to vote against amendments in order to falsely address the issue of partnering with the House bill.

This law included that sunset provision. Now here we are looking at the extension. It is a single-day debate, crowded here into the holidays when few Americans will be paying attention. But I think it is important, nonetheless, for those of us who are concerned about the boundaries of privacy and believe the law could be strengthened to make our case here in hopes that at some point we will be able to have the real consideration these issues merit.

In my opinion, there are serious reforms that need to be made before we consider renewing this law. This law is supposed to be about giving our government the tools it needs to collect the communications of foreigners, outside of our country. If it is possible that our intelligence agencies are using the law to collect and use the communications of Americans without a warrant, that is a problem. Of course, we cannot reach conclusions about that in this forum because this is an unclassified discussion.

My colleagues Senator WYDEN and Senator UDALL, who serve on Intelligence, have discussed the loophole in the current law that allows the potential of backdoor searches. This could allow the government to effectively use warrantless searches for law-abiding Americans. Senator WYDEN has an amendment that relates to closing that loophole.

Congress never intended the intelligence community to have a huge database to sift through without first getting a regular probable cause warrant, but because we do not have the details of exactly how this proceeds and we cannot debate in a public forum those details, then we are stuck with wrestling with the fact that we need to have the sorts of protections and efforts to close loopholes that Senator WYDEN has put forward.

What we do know is that this past summer, the Director of National Intelligence said in a public forum that on at least one occasion the FISA Court has ruled that a data collection carried out by the government did violate the fourth amendment. We also know that the FISA Court has ruled that the Federal Government has circumvented the spirit of the law as well as the letter of the law. But too much else of what we should know about this law remains secret. In fact, we have extremely few details about how the courts have interpreted the statutes that have been declassified and released to the public. This goes to the issue of secret law my colleague from Oregon was discussing earlier. If you have a phrase in the law and it has been interpreted by a secret court and the interpretation is secret, then you really do not know what the law means.

The FISA Court is a judicial body established by Congress to consider requests for surveillance made under the FISA Amendments Act, but, almost without exception, its decisions, including significant legal interpretations of the statute, remain highly classified. They remain secret.

I am going to put up this chart just to emphasize that this is a big deal. Here in America, if the law makes a reference to what the boundary is, we should understand how the court interprets that boundary so it can be debated. If the court reaches an interpretation with which Congress is uncomfortable, we should be able to change that, but of course we cannot change it, not knowing what the interpretation is because the interpretation is secret. So we are certainly constrained from having the type of debate that our Nation was founded on—an open discussion of issues.

These are issues that can be addressed without in any way compromising the national security of the United States. Understanding how certain words are interpreted tells us where the line is drawn. But that line, wherever it is drawn, is, in fact, relevant to whether the intent of Congress is being fulfilled and whether the protection of citizens under the fourth amendment is indeed standing strong.

An open and democratic society such as ours should not be governed by secret laws, and judicial interpretations are as much a part of the law as the words that make up our statute. The opinions of the FISA Court are controlling. They do matter. When a law is kept secret, public debate, legislative intent, and finding the right balance between security and privacy all suffer.

In 2010, due to concerns that were raised by a number of Senators about the problem of classified FISA Court opinions, the Department of Justice and the Office of the Director of National Intelligence said they would establish a process to declassify opinions of the FISA Court that contained important rulings of law. In 2011, prior to her confirmation hearing, Lisa Monaco, who is our Assistant Attorney General for National Security, expressed support for declassifying FISA opinions that include ''significant instructions or interpretations of FISA.''

So here we have the situation where the Department of Justice and the Office of the Director of National Intelligence said they would establish a process of declassifying opinions. They understood that Americans in a democracy deserve to know what the words are being interpreted to mean. We have the Assistant Attorney General for National Security during her hearings express that she supports significant instructions or interpretations being made available to the public. But here we are 2 years later since the 2010 expressions and a year from the confirmation hearings for Lisa, and nothing has been declassified—nothing.

The amendment I am offering today sets out a three-step process for sending the message it is important Americans know the interpretations of these laws. It does so in a fashion that is carefully crafted to make sure there is no conflict with national security.

First you call upon the Attorney General to declassify the FISA report in court of review opinions that include significant legal interpretations. If the Attorney General makes a decision, however, that it cannot be declassified—those decisions—in a way that does not jeopardize national security, then the amendment requires the administration to declassify summaries of their opinions.

So at the first point, you have the official written court opinions. But possibly woven into those court opinions are a variety of contexts about ways and manner of gathering intelligence that pose national security problems. This amendment says: OK, if that is the case, we certainly do not want to disclose sensitive information about ways and means of collecting intelligence, so declassify summaries. That way, we can understand the legal interpretation without adjoining information that might represent a national security problem.

This amendment goes further. If the Attorney General decides that not even a summary can be declassified without compromising national security, then the amendment requires the administration to report to Congress regarding the status of its process for declassifying these opinions—a process the administration has already said it is undertaking. It just says: Tell us where you are.

It is probably very clear from my discussion that I would prefer that the opinions, the actual court opinions, be declassified and that perhaps, if they are sensitive, the national security information would be redacted. That is the normal process in which documents are declassified—you black out or remove sections that are sensitive. But the amendment I am presenting goes further on the side of protecting national security, saying: You don't have to just redact court opinions, you can do a summary that addresses significant legal implications without addressing the ways and means that might be embedded in a further court decision. Furthermore, Mr. Attorney General, if you make a decision that not even that is possible, then update us on the process.

But the key point is that it requires the Attorney General to make a decision, a clear decision over the national security balance and provide what can be done within the context, within the framework of not compromising our national security.

This is so straightforward that anyone bringing the argument to this floor that we should not do it because it compromises national security really has no case to make—absolutely no case to make.

The ACTING PRESIDENT pro tempore. The time of the Senator, under the order, has expired.

Mr. MERKLEY. My understanding is that 30 minutes was allocated?

The ACTING PRESIDENT pro tempore. Thirty minutes equally divided.

Mr. WYDEN. Mr. President, parliamentary inquiry: Can I yield to Senator MERKLEY time from general debate in order to let him complete his remarks?

The ACTING PRESIDENT pro tempore. With the unanimous consent of the Senate.

Mr. WYDEN. I ask unanimous consent.

The ACTING PRESIDENT pro tempore. Without objection, it is so ordered.

Mrs. FEINSTEIN. Well, wait a minute.

The ACTING PRESIDENT pro tempore. Is there objection?

Mrs. FEINSTEIN. I object, if it is time on our side that will be used.

Mr. MERKLEY. Mr. President, if there is no one else waiting to speak, I ask unanimous consent to speak as in morning business and will yield when someone is ready, prepared to speak to the bill.

The ACTING PRESIDENT pro tempore. Is there objection?

The Senator from California.

Mrs. FEINSTEIN. Mr. President, let me do something I do sometimes—correct myself. If the Senator is offering to use the time on his side, that is fine with me. As long as it is not using the time for the bill on our side.

Mr. WYDEN. Mr. President, I think this is acceptable, yes.

Mrs. FEINSTEIN. I thank the Senator.

Mr. MERKLEY. Mr. President, I thank my colleagues for setting out the parameters. I am going to wrap this up in fairly short order.

I again wish to emphasize that if any of my colleagues would like to come down and argue that this in any way compromises national security, I will be happy to have that debate because this has been laid out very clearly so the Attorney General has complete control over any possible compromise of information related to national security. Indeed, although I think it is important for this body to continue to express that the spirit of what we do in this Nation should be about citizens to the maximum extent possible having full and clear understanding of how the letter of the law is being interpreted.

Let me show an example of a passage. Here is a passage about what information can be collected: '' . . . reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation (other than a threat assessment) conducted in accordance with subsection (a)(2),'' and so on.

Let me stress these words: ''relevant to an authorized investigation.''

There are ongoing investigations, multitude investigations about the conduct of individuals and groups around this planet, and one could make the argument that any information in the world helps frame an understanding of what these foreign groups are doing. So certainly there has been some FISA Court decision about what ''relevant to an authorized investigation'' means or what ''tangible things'' means. Is this a gateway that is thrown wide open to any level of spying on Americans or is it not? Is it tightly constrained in understanding what this balance of the fourth amendment is? We do not know the answer to that. We should be able to know.

If we believe that an administration and the secret court have gone in a direction incompatible with our understanding of what we were seeking to defend, then that would enable us to have that debate here about whether we tighten the language of the law in accordance with such an interpretation. Again, is this an open gateway to any information anywhere in the world, anytime, on anyone or is it a very narrow gate? We do not know. American citizens should have the ability to know, and certainly a Senator working to protect the fourth amendment should know that as well. We have always struck a balance in this country between an overbearing government and the important pathway to obtaining information relevant to our national security.

The amendment I am laying forth strikes that balance appropriately. It urges the process to continue by providing an understanding of what the secret court interpretations are, which is very important to democracy. It provides the appropriate balance with national security, gives clear decision-making authority to the Attorney General of this process, and in that sense it gives the best possible path that honors national security concerns while demanding transparency and accountability for this issue of privacy and protection of the fourth amendment.

The ACTING PRESIDENT pro tempore. The Senator from Oregon.

Mr. WYDEN. For purpose of general debate, how much time remains on our side and how much time remains under the control of the distinguished chair of the committee?

The ACTING PRESIDENT pro tempore. The opponents have 140 minutes remaining; the proponents have 183 minutes remaining.

Mr. WYDEN. I thank the Chair. I will speak out of our time in order to respond to a couple points. I also wish to commend my colleague Senator MERKLEY from Oregon for his excellent statement. He has been doing yeoman's work in terms of trying to promote accountability and transparency on this issue and the work he has done in the Senate. I am going to correct a couple of misconceptions about what has been said and also talk on behalf of the good work Senator MERKLEY is doing.

With respect to this amendment I will be offering, I believe the Senate cannot say we passed the smell test with respect to doing vigorous oversight if we don't have some sense of how many Americans in our country who are communicating with each other are being swept up under this legislation. For purposes of the FISA Amendments Act, I think we ought to know, generally, how many Americans are being swept up under the legislation. Oversight essentially would be toothless without this kind of information.

I wish to correct one misconception with respect to where we are on the language in the reporting amendment. The distinguished chair of the committee urged Senators to visit the offices of the Senate Select Committee on Intelligence to see the documents the chair has stated relate to intelligence officials who say it is impossible for them to estimate the number of law-abiding Americans who have had their communications swept up under the legislation. However, the fact is that when colleagues read the amendment I will be offering, they will see I am not requiring anyone to take on a new task of preparing an estimate of how many law-abiding Americans have been swept up in it. This is simply a request to the intelligence community, which states that if any estimate has already been done, that estimate ought to be provided.

When the distinguished chair of the committee says Senators should go over to the committee's offices and look at the documents which state that the intelligence community cannot do a new estimate, I want Senators to know the language of my amendment does not ask for a new estimate. In no way does it ask for a new estimate. It simply says: If an estimate has been done, that estimate ought to be furnished. If no estimate has been done, the answer to that is simply no. We will be very clear about it, and the matter will have been clarified. If no estimate has been done, then fine; the answer is no.

As I indicated earlier, the amendment also requires the intelligence community to state whether any wholly domestic communications have been collected. That again can be answered with a yes or no. Finally, it requires a response as to whether the National Security Agency has collected personal information on millions of Americans, and that too is a very straightforward answer.

I think when we talk about this kind of information, we ought to come back

to the fact that no sources and methods in the intelligence community would be compromised. In no way would the operations or the important work of the intelligence community be interrupted. What it would simply do is provide us with what I think are the basics that this Senate needs to be able to say it is doing real oversight over a very broad area of surveillance law.

I hope Senators will ask themselves as we look at this: Do we in the Senate know whether anyone has ever estimated how many U.S. phone calls and e-mails have been warrantless collected under the statute? Does the Senate know whether any wholly domestic phone calls or e-mails have been collected under this statute? Does the Senate know whether the government has ever conducted any warrantless, backdoor searches for Americans' communication? If not, this is the Senate's chance to answer that question.

When our constituents come forward and ask us whether the government is protecting our privacy rights as we protect our security, the question is: How does the Senator look their constituents in the eye and tell them they don't know and are not in a position to get information that is essential to pass the smell test when it comes to this body doing basic oversight over what is certainly a broad and, for many Americans, rather controversial surveillance law.

I assume—because we have already heard some characterizations of my amendment, which are simply and factually incorrect—that we will have other responses to the reporting amendment in terms of objections. I have already stated my first concern: The intelligence community stating that they cannot estimate how many Americans' communications are collected under key section 702 of FISA. Again, my response is that when Senators look at the text of the amendment, it does not require anybody to do an estimate. It simply says that if estimates do exist, they ought to be provided to the Congress. When it comes to our oversight responsibilities, I do not think that request is excessive or unreasonable.

Second, I think we will hear the House and Senate Intelligence Committees already do oversight of FISA. Every Member of the Congress has to vote on whether to renew the FISA Amendments Act. Frankly, I think every Member of this body ought to be able to get a basic understanding of how the law actually works, and that is not available today.

Next, we will hear that the intelligence community has already provided the Congress with lots of information about the FISA Amendments Act. As the Presiding Officer knows from his service on the committee, much of that information is in highly classified documents that are difficult for most Members to review. The reality is most Members literally have no staff who have the requisite security clearance in order to read them.

The amendment I am talking about with respect to basic information on the number of Americans who have had their communications swept up under FISA—whether Americans with respect to wholly domestic communications have been swept up under this law—in my view that information ought to be available to this body in documents Members can actually access. Frankly, it ought to be available in a single document which Members can access.

In connection with the discussion about these issues, we will also hear the answers to these questions should not be made public. The amendment I am going to be offering with respect to getting a rough set of estimates as to how many Americans are being swept up under these authorities—and whether an estimate actually even exists—gives the President full authority to redact whatever information he wishes from the public version of the report. Under the amendment I am pursuing, the executive branch would have full discretion to decide whether it is appropriate to make any of this information public.

As we ensure more transparency and more accountability with respect to this information and access to it, no sources or methods which have to be protected—including important work the intelligence committee is doing—will be compromised in any way. The last word on this subject is the call of the President of the United States, who has the full discretion to decide whether it is appropriate to make any of this information public.

Finally, we are undoubtedly going to hear that the law is about to expire and amendments will slow it down. First of all, I think many of us would rather have had this debate earlier in this session of the Senate, and had there been more dialog on many of these issues, that would have been possible. We are where we are, and I think all of us understand that. We understand this is a huge challenge. The fiscal cliff is vital in terms of our work this week, but I continue to believe the other body is perfectly capable of passing this legislation before the end of the year.

The amendments that are being offered all go to the issue of transparency and accountability. Not one of those amendments would jeopardize the ongoing issues and operations which relate to the sources and methods of the intelligence community. The Congress can make amendments to improve oversight and still keep this law from expiring.

With respect to the reporting amendment, I hope the argument made by the distinguished chair of the committee that the intelligence community has said they cannot estimate how many Americans' communications have been collected under section 702—that Senators go to the offices of the Intelligence Committee. When colleagues look at the text of the amendment, the amendment does something different than the issue which has been raised by the distinguished chair of the committee. The amendment does not require anyone to do an estimate. It simply says that if an estimate already exists, that estimate ought to be provided to the Congress.

Let me also make some brief remarks on this issue of secret law that touches on the point raised by my colleague from Oregon Senator MERKLEY, who I think has given a very good presentation on the floor and has a very good amendment. When the laws are interpreted in secret, the results frequently fail to stand up to public scrutiny. We have talked about this on the floor and in the committee and it isn't that surprising when we think about it. The law-making process in our country is often cumbersome, it is often frustrating, and it is often contentious. But over the long run I think we know this process is the envy of the world because it gives us a chance to have a real debate, generate support of most Americans because then people see, when they have had a chance to be a part of a discussion, that they are empowered in our system of government. On the other hand, when laws are secretly interpreted behind closed doors by a small number of government officials without public scrutiny or debate, we are much more likely to end up with interpretations of the law that go well beyond the boundaries of what the public accepts or supports. So let's be clear that when we are talking about public scrutiny and having debates, that is what allows the American people to see that those of us who are honored to serve them are following their will.

Sometimes it is entirely legitimate for government agencies to keep certain information secret. In a democratic society, of course, citizens rightly expect their government will not arbitrarily keep information from them, and throughout our history our people have guarded their right to know. But I think we also know our constituents acknowledge certain limited exceptions exist in this principle of openness. For example, most Americans acknowledge that tax collectors need to have access to some financial information, but the government does not have the right to share this information openly. So we strike the appropriate balance on a whole host of these issues on a regular basis.

Another limited exception exists for the protection of national security. The U.S. Government has the inherent responsibility to protect its citizens from threats, and it can do this most effectively if it is sometimes allowed to operate in secrecy. I don't expect our generals to publicly discuss the details of every troop movement in Afghanistan any more than Americans expected George Washington to publish his strategy for the Battle of Yorktown. By the same token, American citizens recognize their government may sometimes rely on secret intelligence collection methods in order to

ensure national security, ensure public safety, and they recognize these methods often are more effective when the details—what are the operations and methods as we characterize them under intelligence principles—remain secret. But while Americans recognize government agencies will sometimes rely on secret sources and methods to collect intelligence information, Americans expect these agencies will at all times operate within the boundaries of publicly understood law.

I have had the honor to serve on the Intelligence Committee now for over a decade. I don't take a backseat to anyone when it comes to the importance of protecting genuine, sensitive details about the work being done in the intelligence community, particularly their sources and methods. However, the law itself should never be secret. The law itself should never be secret because voters have a right to know what the law says and what their government thinks the text of the law means so they can make a judgment about whether the law has been appropriately written, and they can then ratify or reject the decisions elected officials make on their behalf.

When it comes to most government functions, the public can directly observe the functions of government and the typical citizen can decide for himself or herself whether they support or agree with the things their government is doing. American citizens can visit our national forests—we take particular pride in them in our part of the country—and decide for themselves whether the forests are being appropriately managed. When our citizens drive on the interstate, they can decide for themselves whether those highways have been properly laid out and adequately maintained. If they see an individual is being punished, they can make judgments for themselves whether that sentence is too harsh or too lenient, but they generally can't decide for themselves whether intelligence agencies are operating within the law. That is why, as the U.S. intelligence community evolved over the past several decades, the Congress has set up a number of watchdog and oversight mechanisms to ensure intelligence agencies follow the law rather than violate it. That is why both the House and the Senate have Select Intelligence Committees. It is also why the Congress created the Foreign Intelligence Surveillance Court, and it is why the Congress created a number of statutory inspectors general to act as independent watchdogs inside the intelligence agencies themselves. All these oversight entities—one of which I am proud to serve on, the Senate Select Committee on Intelligence—all of them were created, at least in part, to ensure intelligence agencies carry out all their activities within the boundaries of publicly understood law.

But I come back to my reason for bringing up this issue this afternoon. The law itself always ought to be public and government officials must not be allowed to fall into the trap of secretly reinterpreting the law in a way that creates a gap between what the public thinks the law says and what the government is secretly claiming the law says. Any time that is being done, it first violates the public trust, and, second, I have long felt that allowing this kind of gap—a gap between the government's secret interpretation of the law and what the public thinks the law is—undermines the confidence our people are going to have in government. Also, by the way, it is pretty shortsighted because history shows the secret interpretations of the law are not likely to stay secret forever, and when the public eventually finds out government agencies are rewriting these surveillance laws in secret, the result is invariably a backlash and an erosion of confidence in these important government intelligence agencies and the important work, as I noted this morning, our intelligence officials are doing.

So this is a big problem. Our intelligence and national security agencies are staffed by exceptionally hard-working and talented men and women, and the work they do is extraordinarily important. If the public loses confidence in these agencies, it doesn't just undercut morale, it makes it harder for these agencies to do their jobs. If we ask the head of any intelligence agency, particularly an agency that is involved in domestic surveillance in any way, he or she will tell us that public trust is a vital commodity and voluntary cooperation from law-abiding Americans is critical to the effectiveness of their agencies. If members of the public lose confidence in these government agencies because they think government officials are rewriting surveillance laws in secret, those agencies are going to be less effective. I don't want to see that happen. On my watch, I don't want to be a part of anything that makes our intelligence agencies less effective.

Officials at these government agencies do not get up in the morning to do their work with malicious intent. They work very hard to protect intelligence sources and methods for good reasons. Sometimes what happens is people lose sight of the difference between protecting sources and methods, which ought to be kept secret, and the law itself, which should not be kept secret. Sometimes they even go so far as to argue that keeping the interpretation of the law secret is actually necessary because it prevents our Nation's adversaries from figuring out what our intelligence agencies are allowed to do. My own view is this is ''Alice in Wonderland'' logic, but if the U.S. Government were to actually adopt it, then all our surveillance laws would be kept secret because that would, I guess one could argue, be even more useful. When Congress passed the Foreign Intelligence Surveillance Act in 1978, it would have been useful to keep the law secret from the KGB so Soviet agents wouldn't know whether the FBI was allowed to track them down. But American laws and the American Constitution shouldn't be public only when government officials think it is convenient. They ought to be public all the time. Americans ought to be able to find out what their government thinks those laws mean, and I think it is possible to do that while still ensuring that sensitive information—information about sources and methods and the operations of the intelligence community—is appropriately kept secret.

My own view is the executive branch in the United States has so far failed to live up to their promises of greater transparency in this area, greater commitment to ensuring the public sees how our laws are being interpreted. As long as there is a gap between the way the government interprets these laws and what the public sees when people are sitting at home and looking it up on their laptops, I am going to do everything I can to reduce that gap and to ensure our citizens, consistent with our national security, have additional information with respect to how our laws are interpreted. We can do that while at the same time protecting the critical work being done by officials in the intelligence community.

With that, I am happy to yield to the distinguished chairwoman.

The ACTING PRESIDENT pro tempore. The Senator from California.

Mrs. FEINSTEIN. Mr. President, I wish to take a moment to clarify this question of secret law. This code book I am holding is the law. It is not secret. This is all of the code provisions which guarantees the legality of what the intelligence community does. There is a whole section on congressional oversight. There is a whole section on additional procedures regarding persons inside the United States and persons outside the United States. This, in fact, is the law. We can change the law, and Senator WYDEN had something to do with adding section 704. He did, in fact, change the law to put additional privacy protections in and those privacy protections are up for reauthorization in this bill before us.

I wish to address, if I could, what Senator MERKLEY said in his comments. I listened carefully. What he is saying is opinions of the Foreign Intelligence Surveillance Court should, in some way, shape or form, be made public, just as opinions of the Supreme Court or any court are made available to the public. To a great extent, I find myself in agreement with that. They should be. Why can't they be? Because the law and the particular factual circumstances are mixed together in the opinion, so the particular facts and circumstances are possibly classified. Hopefully the opinion can either be written in a certain way for public release or the Attorney General can be required to prepare a summary of what that opinion said for release to the public.

There is one part of Senator MERKLEY's amendment which I think we can work together on regarding the FISA Court opinions, and that is on page 5, lines 3 to 11, where the amendment says:

. . . if the Attorney General makes a determination that a decision may not be declassified and made available in a manner that protects the national security of the United States, including methods or sources related to national security, the Attorney General shall release an unclassified summary of such decision.

I have talked to Senator MERKLEY about this, and I have offered my help in working to establish this. The problem is, we have 4 days, and this particular part of the law expires, the FISA Amendments Act. I have offered to Senator MERKLEY to write a letter requesting declassification of more FISA Court opinions. If the letter does not work, we will do another intelligence authorization bill next year, and we can discuss what can be added to that bill on this issue.

I am concerned that what is happening is the term ''secret law'' is being confused with what the Foreign Intelligence Surveillance Court issues in the form of classified opinions based on classified intelligence programs. As I have made clear, the law is public and when possible, the opinions of the Foreign Intelligence Surveillance Court should be made available to the public in declassified form. It can be done, and I think it should be done more often.

If the opinion cannot be made public, hopefully a summary of the opinion can. And I have agreed with Senator MERKLEY to work together on this issue.

I ask unanimous consent that all quorum calls during debate on the FISA bill be equally divided between the proponents and opponents.

The ACTING PRESIDENT pro tempore. Without objection, it is so ordered.

The Senator from Oregon.

Mr. WYDEN. Mr. President, just to respond to the points made by the distinguished chair of the committee—and, by the way, I think the chair's reference to being willing in the next intelligence authorization bill to work with those of us—and Senator MERKLEY has made good points this afternoon to try to include language in the next intelligence authorization bill to deal with secret law—I think that would be very constructive. I appreciate the chair making that suggestion.

Colleagues may know that under the leadership of the chair of the committee and the distinguished Senator from Georgia, the vice chair of the committee, Mr. CHAMBLISS, we were able, late last week, to work out the disagreements with respect to the intelligence authorization bill this year. I wish to thank the chair for those efforts. I think we have a good bill. I think all of us are against leaks. That is what was at issue. I think we have now dealt with the issue in a fashion so as to protect the first amendment and the public's right to know, and I appreciate the chair working with this Senator on it.

I think we have a good intelligence authorization bill now for this year. I think the chair's suggestion that we look at dealing with this issue of secret law—in addition, I hope, to adopting the Merkley amendment—that we deal with it in the next intelligence authorization bill is constructive. I do want to respond to one point on the merits with respect to comments made by the distinguished chair on this issue.

The distinguished chair of the committee essentially said the law is public because the text of the statute is public. That is true. That is not in dispute. It is true that the text of the law is public. But the secret interpretations of that law and the fourth amendment from the FISA Court are not public. The administration pledged 3 years ago to do something about that. They pledged it in writing in various kinds of communications, and that still has not been done. That is why this is an important issue with respect to transparency and accountability.

The distinguished chair of the committee is absolutely correct that the law is public. The text of the law is public. Nobody disputes that. But the secret interpretations of the law and the fourth amendment—the interpretations of the FISA Court are not public, and we have received pledges now for years that this would change.

I remember—perhaps before the distinguished chair of the committee was in the Chamber—talking about how Senator ROCKEFELLER and I got a letter indicating that this was going to be changed and that we were very hopeful we were going to again get more information with respect to legal interpretations, matters that ought to be public that do not threaten sources and methods and operations. We still have not gotten that. That is the reason why Senator MERKLEY's work is so important.

I see my friend and colleague. I say to Senator MERKLEY, the distinguished chair of the committee has made the point—I think while the Senator had to be out of the Chamber—that the law is public because the text of it is public. But what the Senator has so eloquently described as being our concern is that the opinions of the FISA Court—their opinions and views about the fourth amendment—are what has been secret, and the administration has said for years now they would do something about it.

So the Senator's amendment seeks to give this the strongest possible push. I think that is why the Senator's amendment is so important. The Senator is obviously making a lot of headway because the distinguished chair of the committee has also said this issue of secret law is something that can be addressed as well in the intelligence authorization bill.

If we can adopt the Senator's amendment and then move on to the intelligence authorization bill, that will be a very constructive way to proceed, very much in the public interest. The Senator is obviously making headway.

Mr. MERKLEY. Mr. President, if I could interject for a moment.

Mr. WYDEN. Yes, of course.

The ACTING PRESIDENT pro tempore. The Senator from Oregon.

Mr. MERKLEY. I thank my colleague from Oregon for spearheading this whole conversation about privacy and national security and how the two are not at war with each other. We are simply looking for appropriate warrant processes, an assurance to the public that the boundaries of privacy are being respected. Certainly, a piece of that is the secret law. I appreciate the comments of the chair of the Intelligence Committee on this issue. I do feel that in a democracy, understanding how a statute is interpreted is essential to the conduct of our responsibility in forging laws and ensuring that the constitutional vision is protected.

Mr. WYDEN. I thank my colleague. He is making an important point. I have sat next to Senator FEINSTEIN in the Intelligence Committee now for 12 years, and I think all of us—and we have had chairs on both sides of the aisle—understand how important the work of the intelligence community is. This is what prevents so many threats to our country from actually becoming realities—tragic realities.

What my friend and colleague from Oregon has hammered home this afternoon is that if a law is secret and there is a big gap between the secret interpretation of a law and what the public thinks the law means—my friend and I represent people who, for example, could be using their laptop at home in Coos Bay. If they look up a law and they see what the public interpretation is and they later find out that the public interpretation is real different than what the government secretly says it is, when people learn that, they are going to be very unhappy.

I see my colleague would like some additional time to address this issue. I am happy to yield to him.

Mr. MERKLEY. I thank Senator WYDEN.

The Senator mentioned an Oregonian sitting in Coos Bay working on his or her laptop and calling the Senator's office and saying: Hey, the law says the government can collect tangible material related to an investigation. Does that mean they can collect all of my Web conversations—knowing that the Web circuits travel around the world multiple times and at some point they travel through a foreign space. They ask this question in all sincerity because they care about the fourth amendment and their privacy.

How much ability do we have to give them a definitive answer on that?

Mr. WYDEN. Absent the information we are seeking to get under the amendment I am going to offer, I do not

think it is possible for a Senator to respond to the question.

The issue for an individual Senator would be: Do you know whether anyone has ever estimated how many U.S. phone calls and e-mails have been warrantlessly collected under the statute? Do you know whether any wholly domestic phone calls and e-mails have been collected under this statute, which I believe is the exact question my colleague from Oregon has asked.

I do not believe a Member of the Senate can answer that question. Being unable to answer that question means that oversight, which is so often trumpeted on both sides of the aisle, is toothless when it comes to the specifics.

I hope that responds to my colleague's question.

Mr. MERKLEY. Absolutely. I think about other questions our constituents might ask. They might ask if our spy agencies are collecting vast data from around the world and they become interested in an American citizen, can they search all that data without getting a warrant—a warrant that is very specific to probable cause and an affirmation.

Again, I suspect the answer we could give to the citizen would be that we cannot give a very precise evaluation of that, not knowing how the concept of information related to an investigation has been interpreted and laid out.

Mr. WYDEN. My colleague is asking a particularly important question because the Director of the National Security Agency, General Alexander, recently spoke at a large technology conference, and he said that with respect to communications from a good guy, which we obviously interpret as a law-abiding American, and someone overseas, the NSA has ''requirements from the FISA Court and the Attorney General to minimize that''—to find procedures to protect the individual, the law-abiding American's rights, essentially meaning, in the words of General Alexander, ''nobody else can see it unless there's a crime that's been committed.''

If people hear that answer to my colleague's question—which, frankly, General Alexander responded to directly—they pretty much say that is what they were hoping to hear; that nobody is going to get access to their communications unless a crime has been committed.

The only problem, I would say to my friend, is Senator UDALL and I have found out that is not true. It is simply not true. The privacy protections provided by this minimization approach are not as strong as General Alexander made them out to be. Senator UDALL and I wrote to General Alexander, and he said—and I put this up on my Web site so all Americans can see the response—the general said: That is not really how the minimization procedures work—these minimization procedures that have been described in such a glowing way—and that the privacy protections are not as strong as we have been led to believe. He may have misspoken and may have just been mistaken, but I am not sure the record would be correct even now had not Senator UDALL and I tried to make an effort to follow it up.

I can tell the Senator that at this very large technology conference—this was not something that was classified—at a very large technology conference recently in Nevada, what the head of the National Security Agency said was taking place with respect to protecting people, in response to my colleague's questions: Were their e-mails and phone calls protected, the general said to a big group: They are, unless a crime has been committed. The real answer is that is not correct.

Mr. MERKLEY. I thank my colleague from Oregon for being so deeply invested in the details of this over many years, utilizing a fierce advocacy in support of the fourth amendment and privacy to bring to these debates. I also thank the chair of the Intelligence Committee for her comments earlier today about secret laws and her own concerns about that and her willingness to help to work to have the administration provide the type of information that clarifies how these secret opinions interpret statutes. My thanks go to the Senator from California, Mrs. FEINSTEIN.

The PRESIDING OFFICER (Mrs. MCCASKILL.) The Senator from Oregon.

Mr. WYDEN. I thank my friend. Just one last point with respect to this technology conference where so many people walked away and thought their privacy was being protected by strong legal protections. General Alexander made additional confusing remarks that were in response to that same question with respect to the protections of law-abiding people.

General Alexander said, '' . . . the story that we [the NSA] have millions or hundreds of millions of dossiers on people is absolutely false.''

Now, I have indicated this morning as well, having served on the Intelligence Committee for a long time, I do not have the faintest idea of what anybody is talking about with respect to a dossier. So Senator UDALL and I followed that up as well. We asked the Director to clarify that statement. We asked, ''Does the NSA collect any type of data at all on millions or hundreds of millions of Americans?'' So that, too, is a pretty straightforward question.

The question Senators have been asking about this are not very complicated. If you are asking whether the National Security Agency is addressing these privacy issues, I think it is one of the most basic questions you can ask. Does the National Security Agency collect any type of data at all on millions or hundreds of millions of Americans? If the Agency saw fit, they could simply answer that with a yes or no. Instead, the Director of the Agency replied that while he appreciated our desire to have responses to those questions on the public record, there would not be a public response forthcoming.

So to go over the exchange again, the Director of National Security Agency states that '' . . . the story that we have millions or hundreds of millions of dossiers on people is absolutely false.'' Senator UDALL and I then asked: Does the NSA collect any type of data at all on millions or hundreds of millions of Americans? The Agency is unwilling to answer the question.

So that is what this debate is all about, is reforming the FISA Amendments Act and, in particular, getting enough information so that it is possible for the Senate to say to our constituents: We are doing oversight over this program.

I think right now, based on what we have outlined over the last 3 or more hours, it is clear that on so many of the central questions—the gap, for example, between the secret interpretation of the law and the public interpretation of the law, our inability to find out whether Americans in their wholly domestic communications have had their rights violated, how many law-abiding Americans have had their e-mails and phone calls swept up under FISA authorities, responses to these questions that stem from public remarks made by intelligence officials at public conferences—the inability to get answers to these questions means that this Senate cannot conduct the vigorous oversight that is our charge.

I expect we will have colleagues coming in. With the weather, it is a special challenge to get here from our part of the country.

I have a parliamentary inquiry. The distinguished chair of the committee already, I believe, got unanimous consent that the time in quorum calls be allocated to both sides. That was my understanding. Is that correct?

The PRESIDING OFFICER. That is correct.

Mrs. FEINSTEIN. I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The assistant legislative clerk proceeded to call the roll.

Mr. COONS. 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. COONS. Madam President, I ask unanimous consent to speak in general debate as to H.R. 5949 and that my time in so speaking be charged against Senator WYDEN.

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

Mr. COONS. Madam President, in this dangerous world, we have an obligation to give our intelligence community the tools and the resources they need to keep us safe. But we also have a fundamental obligation—just as great, I believe—to protect the civil liberties of law-abiding American citizens. A right to private communications free from the prying eyes and

ears of the government should be the rule, not the exception, for American citizens on American soil whom law enforcement has no reason to suspect of wrongdoing. Yet the legislation that we debate on this Senate floor today, the FISA Amendments Act, or the Foreign Intelligence Surveillance Act Amendments Act, would reauthorize surveillance authority that most Americans, most of the Delawareans whom I represent, would be shocked to learn the government has in the first place.

Under section 702, FISA permits the government to wiretap communications in the United States without a warrant if it reasonably believes the target of the wiretap to be outside of the country and has a significant purpose of acquiring foreign intelligence information.

Of course, communications are by definition between two or more people, so even if one participant is outside our country, the person they are talking to may be here in the United States and they may well be an American citizen.

Under this legislation, the government is permitted to collect and store their communications but without clear legal limits on what can be done with this information. They can keep it for an indefinite period of time. They can search within these communications and use them in civilian criminal investigations. Perhaps most concerning of all to me, they can search information obtained under this act for the communications of a specific individual U.S. citizen without judicial oversight and for any reason. If these are all true and this is the case, then I am gravely concerned.

What is at issue today is the scope of the government's power to conduct surveillance without getting a warrant. The warrant requirement is enshrined in our legal system from the very founding of our Nation because we believe in judicial checks and balances. If the government suspects wrongdoing by a U.S. citizen, it must convince a judge to approve a warrant. Warrants are issued each and every day in courts across the United States for investigation of potential offenses across the whole spectrum of criminal activity, including crimes affecting national security. In contrast, surveillance under this act is not required to meet this standard, leaving American citizens vulnerable to potentially very real violations of their privacy.

The balance between privacy and security is an essential test for any government, but it is a vital test for our government and for this country.

This law, in my view, does not contain some essential checks that are supposed to protect our privacy.

This law in its current form does contain some checks that I want to review that are supposed to protect our privacy. It requires that the government surveillance program must be reasonably designed to target foreigners abroad and not intentionally acquire wholly domestic communications. The law requires that a wiretap be turned off when the government knows it is listening in on a conversation between two U.S. individuals, and it forbids the government from targeting a foreigner as a pretext for obtaining the communications of a U.S. national. All three of these are important privacy protections currently in the law.

The problem is that we here in the Senate—and so the citizens we represent—don't know how well any of these safeguards actually work. We don't know how courts construe the law's requirements that surveillance be, as I mentioned, reasonably designed not to obtain any purely domestic information. The law doesn't forbid purely domestic information from being collected.

We know that at least one FISA Court has ruled that a surveillance program violated the law. Why? Those who know can't say, and average Americans can't know. We can suspect that U.S. communications occasionally do get swept up in this kind of surveillance, but the intelligence community has not—in fact, they say they cannot offer us any reasonable estimate of the number or frequency with which this has happened.

The government also won't state publicly whether any wholly domestic communications have been obtained under this authority, and the government won't state publicly whether it has ever searched this surveillance, this body of communications, for the communications of a specific American without a warrant.

For me, this lack of information, this lack of understanding, this lack of detail about exactly how the protections in this act have worked is of, as I said, grave concern. Too often, this body finds itself in the position of having to give rushed consideration to the extension of expiring surveillance authorities.

The intelligence communities tell us these surveillance tools are indispensable to the fight against terrorism and foreign spies, just as they did during the PATRIOT Act reauthorization debate last year. Also as in the case of the PATRIOT reauthorization, the expiration of these authorities, we were told, would throw ongoing surveillance operations into a legal limbo, that it could cause investigations to collapse or harm our ability to track terrorists and prevent crimes. All of these are profound and legitimate concerns. It is precisely because this legislation is so important that it is all the more deserving of the Senate's careful, timely, and deliberate attention.

This kind of serious consideration requires more declassified information on the public record than we have available now. That is why I am supporting the amendments reported by the Judiciary Committee, on which I serve, which would help to shine a light on exactly how this surveillance authority is used. It would direct the intelligence community inspector general to issue a public report explaining whether and how the FISA Amendments Act respects the privacy interests of Americans.

This amendment would also give us another chance to amend this FAA after we receive this report by adjusting the sunset not to 2017 but to 2015. The new expiration date would align the sunset of the FISA Amendments Act with those in the PATRIOT Act, allowing for more comprehensive review of both surveillance authorizations.

Concerns about privacy rights of law-abiding American citizens, as well as the striking lack of current public information, are also why I support the amendment of Senator MERKLEY to direct the administration to establish a framework for declassifying FISA Court opinions about the FAA. Secure sources and methods vital to the success of our intelligence community must be protected. I agree with that, and this amendment would do that. But the default position here ought to be that the legal analysis about the government's use of warrantless surveillance in this country is public rather than hidden from view.

I also strongly support the amendment of Senator WYDEN to force the intelligence community to provide Congress and the public, as appropriate, with specifics on just how much domestic communication has been captured under the FAA and what the intelligence community does with that information. This amendment simply asks for the most basic information about the practical consequences of the use of the powerful surveillance authorities in this act. To what extent are these authorities being used to discover the content of private conversations by U.S. citizens? What is the order of magnitude? We don't know.

This amendment is simply common sense. The Delawareans for whom I work and the Nation for whom we work expect that the government cannot listen in on their phone calls or read their e-mails unless a judge has signed a warrant. If there is a reason why this requirement is not consistent with national security, then I say let the intelligence community make that case and allow us to debate that and consider it in public. It is simply not acceptable for the intelligence community to ask us to surrender our civil liberties and then refuse to tell us with any specificity why we must do so, the context, and the scale of the exercise of this surveillance authority. In my view, America's first principles demand better.

I thank Senator WYDEN for his leadership on this issue, and I thank Majority Leader REID for ensuring that we have the opportunity to debate and consider these amendments and the very important issues they reflect here today.

I urge all of my colleagues to consider carefully and then support these

amendments to the FAA. We cannot let the impending deadline distract us from the important opportunity to conduct oversight and implement responsible reforms. To simply be rushed to passage when we have known the deadline was approaching for years strikes me as an abrogation of our fundamental oversight responsibility. This Chamber deserves a full and informed debate about our intelligence-gathering procedures and their potentially very real impact on Americans' privacy rights, and we need it sooner rather than later. These amendments would allow us to have that conversation and to work together on a path that strikes the essential balance between privacy and security for the citizens of these United States.

Madam President, I yield the floor, and I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The assistant legislative clerk proceeded to call the roll.

Mr. PAUL. 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. PAUL. Madam President, I rise today in support of the Fourth Amendment Protection Act. The fourth amendment guarantees the right of the people to be secure in their persons, their houses, their papers, and their effects against unreasonable searches and seizures.

John Adams considered the fight against general warrants—or what they called in those days writs of assistance—to be when ''the child Independence was born.'' Our independence and the fourth amendment go hand in hand. They emerge together. To discount or to dilute the fourth amendment would be to deny really what constitutes our very Republic.

But somehow, along the way, we have become lazy and haphazard in our vigilance. We have allowed Congress and the courts to diminish our fourth amendment protections, particularly when we give our papers to a third party—once information is given to an Internet provider or to a bank. Once we allowed our papers to be held by third parties, such as telephone companies or Internet providers, the courts determined we no longer had a legally recognized expectation of privacy.

There have been some dissents over time. Justice Marshall dissented in the California Bankers Association v. Schulz case, and he wrote these words:

> The fact that one has disclosed private papers to a bank for a limited purpose within the context of a confidential customer-bank relationship does not mean that one has waived all right to the privacy of the papers.

But privacy and the fourth amendment have steadily lost ground over the past century. From the California Bankers Association case, to Smith v. Maryland, to U.S. v. Miller, the majority has ruled that records, once they are held by a third party, don't deserve the same fourth amendment protections.

Ironically, though, digital records seem to get less protection than paper records. As the National Association of Defense Attorneys has pointed out, ''since the 1870s, a warrant has been required to read mail, and since the Supreme Court's decision in Katz v. the United States, a warrant has generally been required to wiretap telephone conversations. However, under current law, e-mail, text messages, and other communication content do not receive this same level of protection.'' Why is a phone call deserving of more protection than our e-mail or texts?

In U.S. v. Jones, the recent Supreme Court case that says the government can't put a GPS tracking device on a car without a warrant, Justice Sotomayor said this:

> I for one doubt that people would accept without complaint the warrantless disclosure to the government of a list of every Web site they have visited in the last week, or month, or year. . . . I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to the Fourth Amendment protection.

Justices Marshall and Brennan, dissenting in Smith v. Maryland, emphasized the danger of giving up fourth amendment protections. They wrote:

> The prospect of government monitoring will undoubtedly prove disturbing even to those with nothing illicit to hide. Many individuals, including members of unpopular political organizations or journalists with confidential sources, may legitimately wish to avoid disclosure of their personal contacts.

In Miller and in Smith, the Supreme Court held that the fourth amendment did not protect records held by third parties. Sotomayor wrote in the Jones case that it may be time to reconsider these cases, reconsider how they were decided; that their approach is, in her words, ''ill-suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.''

Today, this amendment that I will present, the Fourth Amendment Protection Act, does precisely that. This amendment would restore the fourth amendment protection to third-party records. This amendment would simply apply the fourth amendment to modern means of communications. E-mailing and text messaging would be given the same protections we currently give to telephone conversations.

Some may ask, well, why go to such great lengths to protect records? Isn't the government just interested in the records of bad people?

To answer this question, one must imagine their Visa statement and what information is on that Visa statement. From our Visa statement, the government may be able to ascertain what magazines we read; whether we drink and how much; whether we gamble and how much; whether we are a conservative, a liberal, a libertarian; whom we contribute to; what our preferred political party is; whether we attend a church, a synagogue, or a mosque; whether we are seeing a psychiatrist; and what type of medications we take. By poring over a Visa statement, the government can pry into every aspect of one's personal life. Do we really want to allow our government unfettered access to sift through millions of records without first obtaining a judicial warrant?

If we have people who are accused of committing a crime, we go before a judge and get a warrant. It is not that hard. I am not saying the government wouldn't be allowed to look through records. I am saying that the mass of ordinary, innocent citizens should not have their records rifled through by a government that does not first have to ask a judge for a warrant before they look at personal records.

We have examples in the past of abuses by our own country. During the civil rights era, the government snooped on activists. During the Vietnam era, the government snooped on antiwar protesters. In a digital age, where computers can process billions of bits of information, do we want the government to have unfettered access to every detail of our lives? From a Visa statement, the government can determine what diseases one may or may not have; whether one is impotent, manic, depressed; whether someone is a gun owner and whether he or she buys ammunition; whether one is an animal rights activist, an environmental activist; what books we order, what blogs we read, and what stores or Internet sites we look at. Do we really want our government to have free and unlimited access to everything we do on our computers?

The fourth amendment was written in a different time and a different age, but its necessity and its truth are timeless. The right to privacy and, for that matter, the right to private property are not explicitly mentioned in the Constitution, but the ninth amendment says that the rights not stated are not to be disparaged or denied.

James Otis—arguably the father of the fourth amendment—put it best when he said:

> One of the most essential branches of English liberty is the freedom of one's house. A man's house is his castle; and whilst he is quiet, he is as well guarded as a prince in his castle.

Today's castle may be an apartment, and who knows where the information is coming from. It may be paper in one's apartment or it may be bits of data stored who knows where, but the concept that government should be restrained from invading a sphere of privacy is a timeless concept.

Over the past few decades, our right to privacy has been eroded. The Fourth Amendment Protection Act would go a long way toward restoring this cherished and necessary right. I hope my colleagues will consider supporting, defending, and enhancing the fourth amendment, bringing it into a modern

age where modern electronic and computer information and communications are once again protected by the fourth amendment.

Madam President, I reserve the remainder of my time.

Mrs. FEINSTEIN. Madam President, is the Senator going to call up his amendment?

AMENDMENT NO. 3436

Mr. PAUL. Madam President, I ask unanimous consent to call up my amendment, which is at the desk.

The PRESIDING OFFICER. Without objection, the clerk will report.

The assistant legislative clerk read as follows:

The Senator from Kentucky [Mr. PAUL], for himself and Mr. LEE, proposes an amendment numbered 3436.

Mr. PAUL. Madam President, I ask unanimous consent that the reading of the amendment be dispensed with.

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

The amendment is as follows:

(Purpose: To ensure adequate protection of the rights under the Fourth Amendment to the Constitution of the United States)

At the appropriate place, insert the following:

SEC. _____. FOURTH AMENDMENT PRESERVATION AND PROTECTION ACT OF 2012.

(a) SHORT TITLE.—This section may be cited as the ''Fourth Amendment Preservation and Protection Act of 2012''.

(b) FINDINGS.—Congress finds that the right under the Fourth Amendment to the Constitution of the United States of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures is violated when the Federal Government or a State or local government acquires information voluntarily relinquished by a person to another party for a limited business purpose without the express informed consent of the person to the specific request by the Federal Government or a State or local government or a warrant, upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

''(c) DEFINITION.—In this section, the term ''system of records'' means any group of records from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular associated with the individual.

(d) PROHIBITION.—

(1) IN GENERAL.—Except as provided in paragraph (2), the Federal Government and a State or local government is prohibited from obtaining or seeking to obtain information relating to an individual or group of individuals held by a third-party in a system of records, and no such information shall be admissible in a criminal prosecution in a court of law.

(2) EXCEPTION.—The Federal Government or a State or local government may obtain, and a court may admit, information relating to an individual held by a third-party in a system of records if—

(A) the individual whose name or identification information the Federal Government or State or local government is using to access the information provides express and informed consent to the search; or

(B) the Federal Government or State or local government obtains a warrant, upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

The PRESIDING OFFICER. The Senator from California.

Mrs. FEINSTEIN. Madam President, I rise in opposition to this amendment. This amendment is extraordinarily broad. It is much broader than FISA, and in the course of my remarks, I would hope to address how broad it is. It essentially bars Federal, State, and local governments from obtaining any information relating to an individual that is held by a third party unless the government first obtains either a warrant or consent from the individual. This is also not germane to FISA. It has not been reviewed by the Judiciary Committee, which would have jurisdiction over this matter. For that reason alone, I would vote against it. Also, it impedes the timely reauthorization of the FISA Amendments Act.

I also oppose the substance of the amendment. The amendment is titled the ''Fourth Amendment Preservation and Protection Act.'' In reality, it seeks to reverse over 30 years of Supreme Court precedent interpreting the fourth amendment.

In 1967 the Supreme Court established its reasonable expectation of privacy test under the fourth amendment, in the case of Katz v. United States. Nine years later, in a case known as U.S. v. Miller, the Supreme Court held:

[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities.

So already you have a Supreme Court case saying that the fourth amendment does not prohibit the use of this kind of information by the government.

The Miller case involved the government obtaining account records from a bank. But in 1979, just 3 years after Miller, the Supreme Court took up the issue of third-party collection in a case involving the installation and use of pen registers, which are electronic devices that enable law enforcement to collect telephone numbers dialed from a particular phone line without listening to the content of those calls. The 1973 case is known as Smith v. Maryland, and in it the Court held:

[W]e doubt that people in general entertain any actual expectation of privacy in the numbers they dial. All telephone users realize that they must ''convey'' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed. All subscribers realize, moreover, that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills. . . . Telephone users . . . typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes. Although subjective expectations cannot be scientifically gauged, it is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret. . . . This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.

More recently, in the Court's 2012 decision in U.S. v. Jones, some Justices have questioned whether the time has come to revisit Miller and Smith in some form. Now, perhaps they are right, but this amendment isn't the form they had in mind. And this isn't the time to do so.

This amendment is so broad that the police could not use cell phone data to find a missing or kidnapped child without a warrant or the consent of the missing child—impossible to get. Similarly, they could not ask the phone company to provide the home address of a terrorist, drug dealer, or other criminal without consent or warrant. They could not ask a bank if such criminals had recently deposited large sums of money. In fact, as written, this amendment would prohibit law enforcement from looking up the name, address, and phone number of a criminal suspect, witness, or any other person online unless they obtained a warrant or the consent of the criminal suspect. As you can see, the amendment is too broad.

As I have already stated, the FAA authorities expire in 4 days. If those authorities are allowed to lapse, our intelligence agencies will be deprived of a critical tool that enables those agencies to acquire vital information about international terrorists and other important targets overseas, plus what they may be plotting in the United States. It is imperative that we pass a clean reauthorization of these authorities without amendments that will hamper passage in the House.

I urge my colleagues to oppose this amendment.

The PRESIDING OFFICER. The Senator from Vermont.

AMENDMENT NO. 3437

Mr. LEAHY. Madam President, I ask unanimous consent to set aside the pending amendments and call up my amendment, which is at the desk.

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

The clerk will report.

The assistant legislative clerk read as follows:

The Senator from Vermont [Mr. LEAHY] for himself, Mr. DURBIN, Mr. FRANKEN, Mrs. SHAHEEN, Mr. AKAKA, and Mr. COONS, proposes an amendment numbered 3437.

Mr. LEAHY. I ask unanimous consent that reading of the amendment be dispensed with.

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

The amendment is as follows:

(Purpose: In the nature of a substitute)

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the ''FAA Sunsets Extension Act of 2012''.

SEC. 2. EXTENSION OF FISA AMENDMENTS ACT OF 2008 SUNSET.

(a) EXTENSION.—Section 403(b)(1) of the FISA Amendments Act of 2008 (Public Law

110-261; 50 U.S.C. 1881 note) is amended by striking ''December 31, 2012'' and inserting ''June 1, 2015''.

(b) TECHNICAL AND CONFORMING AMENDMENTS.—Section 403(b)(2) of such Act (Public Law 110-261; 122 Stat. 2474) is amended by striking ''December 31, 2012'' and inserting ''June 1, 2015''.

(c) ORDERS IN EFFECT.—Section 404(b)(1) of such Act (Public Law 110-261; 50 U.S.C. 1801 note) is amended in the heading by striking ''DECEMBER 31, 2012'' and inserting ''JUNE 1, 2015''.

SEC. 3. INSPECTOR GENERAL REVIEWS.

(a) AGENCY ASSESSMENTS.—Section 702(l)(2) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1881a(l)(2)) is amended—

(1) in the matter preceding subparagraph (A), by striking ''authorized to acquire foreign intelligence information under subsection (a)'' and inserting ''with targeting or minimization procedures approved under this section'';

(2) in subparagraph (C), by inserting ''United States persons or'' after ''later determined to be''; and

(3) in subparagraph (D)—

(A) in the matter preceding clause (i), by striking ''such review'' and inserting ''review conducted under this paragraph'';

(B) in clause (ii), by striking ''and'' at the end;

(C) by redesignating clause (iii) as clause (iv); and

(D) by inserting after clause (ii), the following:

''(iii) the Inspector General of the Intelligence Community; and''.

(b) INSPECTOR GENERAL OF THE INTELLIGENCE COMMUNITY REVIEW.—Section 702(l) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1881a(l)) is amended—

(1) by redesignating paragraph (3) as paragraph (4); and

(2) by inserting after paragraph (2) the following:

''(3) INSPECTOR GENERAL OF THE INTELLIGENCE COMMUNITY REVIEW.—

''(A) IN GENERAL.—The Inspector General of the Intelligence Community is authorized to review the acquisition, use, and dissemination of information acquired under subsection (a) in order to review compliance with the targeting and minimization procedures adopted in accordance with subsections (d) and (e) and the guidelines adopted in accordance with subsection (f), and in order to conduct the review required under subparagraph (B).

''(B) MANDATORY REVIEW.—The Inspector General of the Intelligence Community shall review the procedures and guidelines developed by the intelligence community to implement this section, with respect to the protection of the privacy rights of United States persons, including—

''(i) an evaluation of the limitations outlined in subsection (b), the procedures approved in accordance with subsections (d) and (e), and the guidelines adopted in accordance with subsection (f), with respect to the protection of the privacy rights of United States persons; and

''(ii) an evaluation of the circumstances under which the contents of communications acquired under subsection (a) may be searched in order to review the communications of particular United States persons.

''(C) CONSIDERATION OF OTHER REVIEWS AND ASSESSMENTS.—In conducting a review under subparagraph (B), the Inspector General of the Intelligence Community should take into consideration, to the extent relevant and appropriate, any reviews or assessments that have been completed or are being undertaken under this section.

''(D) REPORT.—Not later than December 31, 2014, the Inspector General of the Intelligence Community shall submit a report regarding the reviews conducted under this paragraph to—

''(i) the Attorney General;

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

''(iii) consistent with the Rules of the House of Representatives, the Standing Rules of the Senate, and Senate Resolution 400 of the 94th Congress or any successor Senate resolution—

''(I) the congressional intelligence committees; and

''(II) the Committees on the Judiciary of the House of Representatives and the Senate.

''(E) PUBLIC REPORTING OF FINDINGS AND CONCLUSIONS.—In a manner consistent with the protection of the national security of the United States, and in unclassified form, the Inspector General of the Intelligence Community shall make publicly available a summary of the findings and conclusions of the review conducted under subparagraph (B).''.

SEC. 4. ANNUAL REVIEWS.

Section 702(l)(4)(A) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1881a(l)(4)(A)), as redesignated by section 3(b)(1), is amended—

(1) in the matter preceding clause (i)—

(A) in the first sentence—

(i) by striking ''conducting an acquisition authorized under subsection (a)'' and inserting ''with targeting or minimization procedures approved under this section''; and

(ii) by striking ''the acquisition'' and inserting ''acquisitions under subsection (a)''; and

(B) in the second sentence, by striking ''The annual review'' and inserting ''As applicable, the annual review''; and

(2) in clause (iii), by inserting ''United States persons or'' after ''later determined to be''.

Mr. LEAHY. Madam President, when Congress passed the FISA Amendments Act of 2008, it granted the Government sweeping new electronic surveillance powers which, if abused or misused, could impinge on the privacy rights of Americans. Congress enacted these controversial authorities with the understanding that it would re-examine these provisions within four years, and determine whether to allow these authorities to continue.

While there is no question that the surveillance powers established in the FISA Amendments Act have proven to be extraordinarily important for our national security, it is equally clear to me that those broad powers must continue to come with rigorous oversight and strong privacy protections.

That is why the Senate should adopt the Senate substitute amendment that would allow the government to continue using these authorities, but for a period of time that ensures strong and independent oversight. This amendment was considered and reported favorably by the Senate Judiciary Committee last July. I urge Senators to support this reasonable and commonsense measure. I call on all Senators who talk about accountability and oversight to join with us to adopt this better approach to ensuring our security and our privacy.

Many of us will remember that the FISA Amendments Act was originally passed to clean up what one Bush administration lawyer called the ''legal mess'' of the warrantless wiretapping program, which undermined the privacy rights and civil liberties of countless Americans. More than that, the warrantless wiretapping program undermined the public's trust in our Government, and in the intelligence community's ability to police itself.

During the debate on the FISA Amendments Act in 2007 and 2008, I worked with others on the Judiciary Committee to ensure that important oversight, accountability, and privacy protections were put into place, including express prohibitions on the warrantless wiretapping of U.S. persons or any individual located here in the United States, as well as a prohibition against the practice of so-called ''reverse targeting.''

I am convinced that the oversight and accountability provisions that we included in the original legislation have helped to prevent the abuse of these surveillance tools. Based on my review of information provided by the Government, and after a series of classified briefings, I have not seen evidence that the law has been abused, or that the communications of U.S. persons are being intentionally targeted. But let's be absolutely clear, my conclusion is based on the information I have seen to date, and current compliance does not guarantee future compliance. We must not relax our oversight efforts, and I believe that there is more that can be done to protect against future abuse and misuse.

In June, after the Senate Intelligence Committee originated the Senate bill to reauthorize and extend FISA, Senator GRASSLEY and I asked for a sequential referral, just as I did in 2008, to allow the Judiciary Committee to consider and improve this important legislation. The bill that was approved by the Intelligence Committee provided for a general and unfettered extension of the expiring provisions until June 2017.

I hoped that the Senate Judiciary Committee would improve on that, and we did. I worked with Senator FEINSTEIN, Chair of the Senate Intelligence Committee, to craft a compromise to shorten the sunset to 2015 and to add some accountability and oversight provisions. I appreciated the Senator from California's commitment to helping to improve this sensitive and important legislation and her strong words of support for the Senate Judiciary Committee bill. The Senate Judiciary Committee adopted the substitute and reported the Senate bill to the Senate promptly last July. That is the bill that I am offering, the Senate bill. There is no reason for us to merely rubberstamp the House bill. We have a better bill with better provisions and more accountability and oversight. I am pleased that Senators DURBIN, FRANKEN, SHAHEEN, AKAKA, and COONS have joined me as cosponsors of this amendment.

The Senate bill that the Judiciary Committee adopted, and that I am offering to improve on the House bill

that has been brought before us, provides for a shorter sunset of the expiring surveillance authorities. The House bill's sunset is longer than that adopted by the Senate Select Committee on Intelligence and unnecessarily extended. The Senate bill I offer provides for extending FISA authorities, but would sunset them in June 2015. This will allow the existing programs to continue but ensures that we revisit them in a timely fashion as more information becomes available. It would also align with the June 2015 sunset of certain provisions of the USA PATRIOT Act, thereby enabling Congress to evaluate all of the expiring surveillance provisions of FISA together. This is an approach that Chairman FEINSTEIN and I both supported during the PATRIOT Act reauthorization debate in 2011, along with many members of the Judiciary and Intelligence Committees. This is the position the intelligence community and the administration supported then and as recently as last year. It is the right position and the right sunset, and that is why the Senate bill should include it and will if my amendment is adopted.

As we have seen through our experience with the USA PATRIOT Act, sunsets are important oversight tools. Sunsets force Congress to re-examine carefully the surveillance powers that have been authorized. If we know we have to actually look at it because it is going to run out, what happens is amazing—Senators in both parties actually look at it. More importantly, sunsets force the administration to provide full and accurate information to justify to Congress the reauthorization of significant authorities. Any administration is going to be willing to kick the ball down the road if they don't have to do it; if they have a sunset, they do. The last thing we want is for the NSA and the FBI to take for granted that they will have these powers, especially when the misuse or abuse of these powers could significantly impact the constitutional liberties of Americans. Likewise, we must never take for granted our constitutional liberties, and we should not shy away from our duty as Senators to protect against any such misuse or abuse.

I acknowledge and appreciate those in the intelligence community who work very hard to ensure compliance with our laws and Constitution. But it is also important to note that there has never been a comprehensive review of these authorities by an independent Inspector General that would provide a complete perspective on how these authorities are being used, and whether they are being used properly.

The DOJ Inspector General recently completed a review of the FBI's implementation of the FISA Amendments Act, but this was limited in scope—not only because it was just limited to the FBI, and not any other part of the intelligence community, but also because it was limited in scope to the period ending in early 2010. Notably, this was the first report ever issued by the DOJ Inspector General regarding the FBI's use of Section 702 authorities, and it was issued in September 2012—after the Senate Intelligence and Judiciary Committees reported their bills, and after the House voted to pass its clean extension.

Even more troubling is the fact that we still have not received a report from the NSA Inspector General that fully assesses the NSA's compliance with its targeting and minimization procedures, or the limitations we put in place to protect the privacy of Americans. I am told that a preliminary report on the adequacy of the management controls at the NSA is being finalized—but it is just that: a preliminary report, and not an actual, final, comprehensive, or definitive assessment of whether NSA analysts are complying with the procedures and rules that they have put into place. Indeed, the NSA Inspector General's office has acknowledged that there is more work to be done, and that this review—once completed—will just be a first step. Moreover, as with the DOJ Inspector General's report, this review is limited just to a single agency, and does not incorporate any review or assessment of any information-sharing that might be taking place.

To address the limitations faced by the IGs for individual agencies, our Senate bill as embodied in my substitute amendment adds some commonsense improvements to the oversight provisions in the FISA Amendments Act, including a comprehensive independent review by the Inspector General of the Intelligence Community. The Office of the Inspector General of the Intelligence Community was established in 2010 and has the unique ability to provide a comprehensive assessment of the surveillance activities across the intelligence community, rather than just a limited view of a single agency. An independent review by the Inspector General for the Intelligence Community could answer some remaining questions about the implementation of the FISA Amendments Act, particularly with respect to the protection of the privacy rights of U.S. persons. I also believe that an unclassified summary of such an audit should be made public in order to provide increased accountability directly to the American people.

These are reasonable improvements to the law that I urge all Senators to support. We often hear Senators speak about the need for vigorous and independent oversight of the Executive Branch, the need to support independent inspectors general who are not beholden to a particular agency, and the need for Congress to conduct its own independent reviews as a check on the power of the Executive. So I ask those same Senators this question: When Congress has authorized the use of expansive and powerful surveillance tools that have the potential to impact so significantly the constitutional rights of law-abiding Americans, isn't this exactly the type of situation that calls for that sort of vigorous and independent oversight? Put simply, someone needs to be watching the watchers—and watching them like a hawk. I call upon all Senators, on both sides of the aisle, who talk about accountability and oversight to join with us to adopt this better approach to ensuring our security and our privacy by adopting the Senate bill as embodied in the substitute amendment.

No one can argue that shortening the sunset or adding oversight provisions somehow hampers the Government's ability to fight terrorism or somehow harms national security. That is not true. All Senators should know that neither the 2015 sunset date nor the added oversight provisions have any operational impact on the work of the intelligence community. No one—I repeat, no one from the administration has ever said to me that these provisions cause any operational problems for the intelligence community, and to suggest otherwise now is simply not accurate.

In fact, when the Senate Select Committee on Intelligence reported its bill last year that bill had exactly the same sunset date of June 2015 that is in the substitute amendment. I was encouraged that Senator FEINSTEIN supported this 2015 sunset date when the Judiciary Committee approved this substitute amendment, and noted then that this substitute amendment does not cause any operational problems for the intelligence community.

So where does that leave us? It leaves us with a simple choice. We can enable the intelligence community to continue using these authorities until 2015, while adding commonsense improvements that will help us to conduct vigorous oversight. Or the Senate can abdicate its responsibilities and rubberstamp the House bill that extends these powerful authorities for another five years, without a single improvement in oversight or accountability—even though we may not have all the information we need to make an informed determination.

As an American, and as a Vermonter, the choice is simple for me. We have an obligation to ensure that these expansive surveillance authorities are accompanied by safeguards. We can fulfill our duty to protect the privacy and civil liberties of the American public, while continuing to provide the intelligence community with tools to help keep America safe. That is what the Senate bill as embodied in the substitute amendment accomplishes. I urge Senators to choose this balanced, commonsense approach, and to support adopt the Senate substitute to the over-expansive House bill.

The PRESIDING OFFICER. The Senator from California.

Mrs. FEINSTEIN. Madam President, in listening to the distinguished chairman of the Judiciary Committee and also reading the amendment, I want to

make clear that there are parts of this amendment to which I would agree. However, the House bill is now before us, which would extend the sunset of the FISA Amendments Act 5 years versus 2½ years in the Leahy Amendment. So, before us is the 5-year authorization period which the House has already passed. We have 4 days before the FISA Amendments Act essentially end. I cannot support that shorter time but I support the 5-year extension.

The part of the amendment of the chairman of the Judiciary Committee that I do agree with is the expanded mission of the inspector general of the Intelligence Community. Since the chairman is now becoming the President in rapid promotion, I will be happy to address my remarks to him.

(The PRESIDENT pro tempore assumed the Chair.)

Mr. President, Mr. Chairman, I want you to know we have spent large amounts of time on the particular issue of Section 702 reporting. For example, the law requires semiannual Attorney General and DNI assessments of section 702. Every 6 months they assess compliance with the targeting and minimization procedures. The law also requires the inspector general of Justice and the IG of every element of the intelligence community authorized to acquire foreign intelligence information to review compliance within Section 702. In addition, the IGs are required to review the number of disseminated intelligence reports containing a reference to a U.S.-person identity and the number of U.S. person identities subsequently disseminated. The law also already requires annual reviews by agency heads of Section 702. It also requires a semiannual Attorney General report on Title VII every 6 months to fully inform the congressional Intelligence and Judiciary Committees. And there is another semiannual report on FISA required for the Attorney General to submit a report to the committees. Finally, there are requirements for the provision of documents relating to significant construction or interpretation of FISA by the FISA Court.

So it is clear that there are many reporting requirements on FISA and specifically section 702. I would also add that the Intelligence Committee has had hearings with the DNI, with Attorney General Holder, with Director of FBI Mueller on how Section 702 is carried out. I will also tell you the Intelligence Committee staff spends countless hours going over the reports in meetings with representatives of the departments. However, I would say to Chairman LEAHY that what I would like to do is look at your amendment and see how it compares to what is currently being done and possibly add some parts of your amendment to our authorization bill next year.

I would urge that we have your staff and the Intelligence Committee staff work together to see what we can do. The real reason to oppose all of this at this time is that these authorities expire in 4 days. I remember the vote in the Judiciary Committee on this amendment very well. Had the bill come to the floor over the summer, after it passed out of Committee, then we might have had time to convince the House to consider these changes to current law. But here we are where we have a 5-year House bill in front of us and only 4 days to extend the sunset. As I am opposing all amendments, I would respectfully and, not quite sorrowfully but almost, have to oppose your amendment with the caveat I added, Mr. Chairman.

In deference to you and your chairmanship of the Judiciary Committee, the Intelligence Committee staff will work closely with yours to see if there is anything that needs to be added to a future intelligence authorization bill.

I thank you for that and I yield the floor.

The PRESIDENT pro tempore. The Senator from Oregon.

Mr. WYDEN. Mr. President, first, I strongly support your amendment, given how little most Members of Congress know about the actual impact of the law. The shorter extension period as envisioned by the distinguished chairman of the Judiciary Committee makes a lot of sense. I also think it makes sense to have the intelligence community inspector general conduct an audit on how FISA Amendment Act authority has been used.

Once again, we have had this discussion about how much everybody already knows about how the FISA Amendments Act affects the operations of this program on law-abiding Americans. I would have to respectfully disagree. I asked Senators, as we touched on this in the course of the afternoon, whether they know if anyone has ever estimated how many U.S. phone calls and e-mails have been warrantlessly collected under this statute?

Senator UDALL and I have asked this very simple question: Has there been an estimate—not whether there is going to be new work, whether they are going to be difficult assignments. We have asked whether there has ever been an estimate of how many U.S. phone calls have been warrantlessly collected under the statute. We were told in writing we were not going to be able to get that information.

I think Senators ought to also ask themselves whether they know if any domestic phone calls and e-mails, what are wholly domestic communications, have been conducted under this statute. I think they will also find they do not know the answer to this question. I think Senators also would want to know whether the Government has ever conducted any warrantless backdoor searches for Americans' communications.

So when we have the argument that has now been advanced several times in the course of the day that we already know so much, we do not need all these amendments, it is just going to delay passage of the legislation, I urge people—go to my Web site, in particular—to look at what we have learned from the intelligence community, which is the response to request after request, particularly requests of a tripartisan group of Senators asking yes or no questions: Has there been an estimate? For example, how many law abiding Americans have had their communications swept up into these FISA authorities? Our inability to get that answer makes it clear that when one talks about robust oversight under this legislation, the reality is that there is enormous lack of specifics with respect to how this legislation actually works.

I would only say in response to the amendment offered by the Presiding Officer, Senator LEAHY, the chairman of the Judiciary Committee, I think his amendment is very appropriate. Given how little is known, to me it is one of the fundamental pillars of good oversight that we do not grant open-ended kind of authorizations when we lack so much fundamental information about how this program works, particularly how it would affect law-abiding Americans.

With that, I yield back.

Mrs. FEINSTEIN. Mr. President, I suggest the absence of a quorum.

The PRESIDENT pro tempore. The clerk will call the roll.

The bill clerk proceeded to call the roll.

The PRESIDENT pro tempore. The majority leader.

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

The PRESIDENT pro tempore. Without objection, it is so ordered.

LETTER OF RESIGNATION

Mr. REID. Mr. President, I have in my hands a letter from Brian Schatz, the Lieutenant Governor of the State of Hawaii, and that letter is a resignation letter.

I ask unanimous consent the resignation letter be printed in the RECORD.

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

DECEMBER 26, 2012.

Re Resignation as Lieutenant Governor.

Hon. NEIL ABERCROMBIE,
Governor, State of Hawai'i, State Capitol, Honolulu, Hawaii.

DEAR GOVERNOR ABERCROMBIE: Thank you for the confidence you have placed in me today by appointing me to represent Hawaii in the United States Senate by filling the vacancy in the Senate caused by the death of Senator Inouye.

Because of the critical issues facing our nation, I will need to go to Washington, D.C. immediately to assume the duties of the office of United States Senator. In order to ensure that the duties and responsibilities of the Lieutenant Governor are performed for the State of Hawai'i with as little interruption as possible, I hereby tender my resignation as Lieutenant Governor, effective immediately.

Very truly yours,

BRIAN SCHATZ.