Prepared Remarks of Senator Ron Wyden on a Bill to Extend the FISA Amendments Act of 2008

Today on the Senate floor we will be debating another extremely important matter: the extension of the FISA Amendments Act of 2008. This is a major surveillance law that was passed in 2008 as the successor to the warrantless wiretapping program that operated under the Bush Administration. This law gave the government new authorities to collect the communications of foreigners outside the United States, and the bill before the Senate today would extend this law for another five years. I expect today's debate to focus on whether the law contains adequate protections for the privacy of law-abiding Americans, and on the amendments that I and a number of other senators will offer to improve oversight of this authority and increase the public's understanding of its impact. This is likely to be the only floor debate that the Senate will have on this law during this nine-year period (*2008-2017*), which obviously makes today's discussion very important.

I've been a member of the Senate Intelligence Committee for twelve years, and I can tell you that the intelligence community is made up of a lot of hard-working, patriotic men and women. Their job is to follow whatever laws Congress lays down as they work to collect intelligence. Our job here in Congress is to make sure that the laws we pass adequately protect both national security and the rights of individual Americans. And we owe it to these hard-working men and women to conduct robust oversight of the work that they do, so that members of the public can have confidence that both their security and their rights are being protected.

I know there are going to be a number of senators coming to the floor to debate this bill and talk about whether the law should be reformed, but I'd like to kick things off if I can with an overview of what this law does, and how we got to this point.

This story 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, and they argued that if they weren't allowed to vote for their own government then they shouldn't have to pay taxes. Their well-known rallying cry was "No Taxation Without Representation," and early revolutionaries engaged in protests against these taxes all over the country. The most famous of these protests was of course the Boston Tea Party, in which colonists in Boston threw shiploads of tea into Boston Harbor to protest a tax on tea.

Because there were a lot of taxes on things like tea and sugar and paint and paper, and also because many colonists believed these taxes were unjust, there was a lot of smuggling going on in the American colonies. People would import things like sugar and simply avoid paying the tax on them. Naturally 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 authorities began issuing general warrants, which were called "writs of assistance," that authorized government officials to enter any house or building they wanted in order to search for smuggled goods. These officials weren't limited to only searching in certain houses, and they weren't required to show any evidence that the place they were searching had smuggled goods in it. Basically, government officials were allowed to say that they were looking for smuggled goods and then go searching through any house they wanted to see if they could find some.

If you are the English authorities and your goal is to find smuggled goods, then letting constables and customs officers search any house or building they want is actually a pretty effective way to do that. If you keep searching enough houses, eventually you'll find some smuggled goods in one of them, and then you can seize those goods and arrest whomever lives in that house for smuggling. The problem, of course, is that if you let government officials search any house they want, they're going to search through the houses of a lot of people who haven't broken any laws at all. And the American colonists had a huge problem with that. They said that it's not okay to just go around invading peoples' privacy unless you have specific evidence that they've done something wrong.

The law said that these writs of assistance were good until the king died. So when King George the Second 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, reminding the court that "A man's house is his castle." Mr. Otis described the writs of assistance as "a 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 that the American colonists had against the British government. So naturally America's Founding Fathers made certain to address this complaint when they wrote the Bill of Rights.

The Bill of Rights ensured that strong protections for individual liberties were included within our Constitution itself. And the Founding Fathers included strong protections for personal privacy in the Fourth Amendment, which 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 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."*

This was a direct rejection of the authority that the British had claimed to have when they ruled the American colonies. The Founding Fathers said that our government does not have the right to search any house that government officials want to search, even if it helps them do their job. Government officials may only search someone's house if they have evidence that someone is breaking the law and they show that evidence to a judge to get an individual warrant. For over two hundred years this fundamental principle has protected Americans' privacy while still allowing the government to enforce the law and protect public safety.

As time passed and the United States entered the 20th century, advances in technology gave government officials the power to invade individual privacy in ways that the Founding Fathers never dreamed of, and Congress and the courts sometimes struggled to keep up. Time and again Congress and the courts were most successful when they returned to the fundamental principles of the Fourth Amendment.

In 1928, the Supreme Court considered a famous case about whether the Fourth Amendment made it illegal for the government to listen to somebody's phone conversations without a warrant. Once again, this was a case about smuggling – specifically bootlegging. The government argued that as long as it did the wiretapping remotely, without entering anybody's house, then the Fourth Amendment did not apply. In a brilliant dissent, Justice Louis Brandeis argued that this was wrong, and that the Fourth Amendment was about preventing the government from invading Americans' privacy, regardless of how the government did it. I'm going to quote Justice Brandeis' words at length, because I think they are a brilliant and farsighted explanation of the principle that we are debating today.

"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 [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.

"Moreover, '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 lesser intrusions than these.

"… 'The principles [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 that right has never been forfeited by his conviction of some public offence.'

"… The evil incident to invasion of the privacy of the telephone is far greater than that involved in 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 [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 satisfactions of life are to be found in material things. They sought to protect Americans in 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 upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment."

Let me repeat those last two sentences: the right of the people to be left alone by their government is "the most comprehensive of rights," and "the right most valued by civilized men." And intrusions on individual privacy "whatever the means employed, must be deemed a violation of the Fourth Amendment."

Thankfully, while Justice Brandeis' view that the Fourth Amendment applies to modern, high-tech surveillance did not prevail in 1928, it was eventually adopted by the full Supreme Court.

When the Foreign Intelligence Surveillance Act, or FISA, was written in 1978, Congress applied this same principle to intelligence gathering. The original FISA statute states 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 a terrorist or a spy, and get an individual warrant. This upheld the same principle that the Founding Fathers fought for in the Revolution and enshrined in the Bill of Rights – government officials are not allowed to invade Americans' privacy unless they have specific evidence and individual warrants.

After 9/11, the Bush Administration decided that it needed additional surveillance authorities beyond what was in the FISA statute. Unfortunately, instead of asking Congress to change the law, the Bush Administration developed a warrantless wiretapping program that operated in secret for a number of years. When this finally became public, there was an incredible uproar. I remember how livid many of my constituents were when they learned about the warrantless wiretapping program, and I'll tell you I was pretty livid myself. I've been a member of the Intelligence Committee for twelve years, but the first time I heard about the warrantless wiretapping program was when I read about it in the *New York Times*. Finally, after over a year of heated debate, Congress passed the FISA Amendments Act of 2008, which replaced the warrantless wiretapping program with new authorities for the government to collect the phone calls and emails of people who are 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. Unlike traditional FISA authorities, and unlike law enforcement wiretapping authorities, section 702 does <u>not</u> involve

obtaining individual warrants. Instead, it allows the government to get programmatic warrants that last for an entire year and authorize the government to collect a potentially large number of phone calls and emails, with no requirement that the senders or recipients be connected to terrorism or espionage. If that sounds familiar, it should. General warrants that allowed government officials to decide whose privacy to invade were the exact sort of abuse that the American colonists protested, and that led the Founding Fathers to adopt the Fourth Amendment in the first place. For this reason, section 702 of FISA contains language that is specifically intended to limit the government's ability to use these new authorities to spy on American citizens.

Let me emphasize that because it's very important: It is never okay for government officials to use general warrants to deliberately invade the privacy of law-abiding Americans. It wasn't okay for constables and customs officials to do it in colonial days, and it's not okay for the NSA to do it today. So if the government is going to use general warrants to collect peoples' phone calls and emails, it is extremely important to ensure that this authority is only used against foreigners overseas, and not against Americans.

However, despite what you may have heard, this law doesn't actually prohibit the government from collecting Americans' phone calls and emails without a warrant. The FISA Amendments Act says 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 that still leaves room for a lot of circumstances under which Americans' phone calls and emails – including purely domestic phone calls and emails – could be swept up and reviewed without a warrant. This could happen if the government did not know that someone is an American, or if the government made a technical error, or if an American were talking to a foreigner – even if that conversation was entirely legitimate.

And to be clear, I am not talking only about hypothetical situations. The FISA Court 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 that the impact of this law on Americans' privacy has been real, not hypothetical.

When Congress passed the FISA Amendments Act four years ago it included an expiration date, which was intended to ensure that Congress would review this authority closely, and decide whether protections for Americans' privacy are adequate, or whether they need to be modified. Congress' role here is essentially to determine whether the constitutional teeter-totter, on which we balance the need of the government to collect information with the right of individual Americans to be left alone, is in balance. If it's unbalanced, then Congress has a responsibility to step up and figure out how to make appropriate changes in the law, to ensure that American security and American privacy are both being protected at the same time.

Unfortunately, Congress and the public do not currently have enough information to fully evaluate this law's impact on Americans' privacy. There are a number of key questions about the law's impact that intelligence officials have simply refused to answer publicly. Here are the big questions that I believe it is important to answer, if you want to understand what the impact of this law has been:

First, if you want to know what kind of impact this law has had on Americans' privacy, you probably want to know roughly how many phone calls and emails that are to and from Americans have been swept up by the government under this authority. 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 in this way. The intelligence community responded that it was "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.

Now, if you're someone who doesn't like the idea of government officials secretly reviewing your phone calls and emails, you probably don't find that answer reassuring. But it gets worse. In July of this year, I and a tripartisan group of twelve other senators, including Mark Udall, Mike Lee, Dick Durbin, Jeff Merkley, Rand Paul, Chris Coons, Mark Begich, Jeff Bingaman, Jon Tester, Bernie Sanders, Tom Udall and Maria Cantwell all wrote 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 of how many American communications had been swept up in this way. Is hundreds? Is it hundreds of thousands? Is it millions? The Director declined to publicly answer this question.

We also asked the Director if anyone else has already done such an estimate. If you can believe it, the Director declined to publicly answer this question as well. It seems to me that Congress and the public should be able to get a straightforward answer to that question – have any estimates been done already, and if so what did they say?

Second, if you want to understand this law's impact on Americans' privacy, then you probably want to know whether any wholly domestic communications have been collected under this authority. When I say wholly domestic, I'm 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 US communications, and I think people ought to know whether these safeguards are working or not.

So, when our tripartisan group of senators wrote to the Director back in July, we asked him if he knew whether any wholly domestic US communications have been collected under the FISA Amendments Act. I am disappointed to say that the Director declined to answer this question publicly as well. Think about that for a moment. We asked if he knew whether any wholly domestic communications have been collected under this law, and he declined to publicly provide a simple yes or no response.

So that means that the FISA Amendments Act involves the government going to a secret court on a yearly basis and getting programmatic warrants to collect peoples' phone calls and emails, with no requirement that these communications actually belong to people involved with terrorism or espionage. This authority isn't supposed to be used against Americans, but in fact intelligence officials say they don't even know how many American communications they are actually collecting. And once they have this pile of communications, which contains an unknown but potentially very large number of Americans' phone calls and emails, there are surprisingly few rules about what they can do 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 emails of a specific American, even if they don't have any actual evidence that the American is involved in nefarious activity. Again, if that sounds familiar, it should. General warrants allowing government officials to deliberately intrude on the privacy of individual Americans at their own discretion were one of the abuses that led America's Founding Fathers to rise up against the British, and they are exactly what the Fourth Amendment was written to prevent. If government officials want to search an American's house, or read their emails, 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 allows government officials to make an end-run around traditional warrant requirements and conduct "back door searches" for Americans' communications.

And let me be clear – if the government has clear evidence that an American is engaged in terrorism, espionage, or other serious crime, then I think the government should be able to read that person's emails and listen to that person's phone calls. In fact, I think that's an essential part of protecting public safety. But government officials should be required to get a warrant or an emergency authorization before they do this – that's an essential part of balancing public security with individual liberty.

So, the third thing that you want to know, if you're trying to decide whether the constitutional teeter-totter is in balance or out of whack, is whether the

government has ever taken advantage of this "back door searches" loophole and conducted a warrantless search for the phone calls or emails of specific Americans.

When we sent our tripartisan letter to the Director of National Intelligence back in July, we asked him to please say whether the intelligence community has ever deliberately conducted a warrantless search of this nature. Disappointingly, the Director declined to provide a public answer to this question as well.

If you're keeping score at home, you'll notice that the Director refused to publicly answer any of the questions that we asked in our letter. So if you're looking for reassurance that this law is being carried out in a way that respects the privacy of law-abiding American citizens, you won't find it in his response.

I should note that the Director did provide us with additional responses in a highly classified attachment to this letter. In fact, the attachment was so highly classified that I think eleven of the thirteen senators who signed the letter don't have any staff who are cleared to read it. Naturally this makes it hard for those senators, let alone the public, to gain any better understanding of the privacy impact of this law.

Several of us sent the Director a follow up letter last month, again urging him to provide public answers to these very straightforward questions. Again, the Director refused.

But while intelligence officials don't deny these facts, they still insist that are already protecting innocent Americans' privacy. They talk a lot about how this program is overseen by the secret FISA Court, and how this Court is charged with ensuring that all of the collection carried out under this program is constitutional.

To respond, I would just note again that under the FISA Amendments Act the government does not have to get the permission of the FISA Court to read particular emails 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 emails of an American citizen. And even when the Court reviews the government's collection and handling procedures, it's important to note that the FISA Court's rulings are made entirely in secret. It may seem hard to believe, but this court's rulings interpret major surveillance laws and even the US Constitution in significant ways, and the public has no idea what the Court is actually saying. What this means is that our country is developing a secret body of law, so that most Americans have no way of finding out how their laws and their Constitution are actually being interpreted. Needless to say, that's a big problem. Americans don't expect to know all the details of how government agencies collect information, but they do expect those agencies to operate within the boundaries of publicly understood law. And they have a need and a right to know how those laws and their Constitution are being interpreted, so that they can ratify or reject decisions that elected officials make on their behalf. To put it another way, Americans know that intelligence agencies will sometimes conduct secret operations, but they don't expect those agencies to rely on secret laws.

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 these warrants in open court. So when the courts upheld those writs of assistance, ordinary people could read about that decision, and people like 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, I and other senators have urged the Department of Justice and the intelligence community to establish a regular process for reviewing, redacting and releasing those opinions of the FISA Court that contain significant interpretations of law, so that members of the public have the opportunity to understand what their government thinks their laws and Constitution actually mean.

I obviously don't see a need to release every single routine decision that is made by this Court, and obviously most of the cases that come before the Court contain sensitive information about intelligence sources and methods that it is appropriate to keep secret. But the law itself should never be secret. And what federal courts think the law and the Fourth Amendment to the Constitution actually mean should never be a secret from the American public, the way it is today.

I was encouraged in 2009, when the Obama Administration wrote to Senator Rockefeller and me to inform us that they would be setting up a process for redacting and releasing those FISA Court opinions that contain significant interpretations of law. Unfortunately, over three years later, this process has produced literally zero results. Not a single redacted opinion or summary of FISA court rulings has been released. I can't even tell if the Administration still intends to fulfill this promise or not. I often get the feeling that they're hoping that people will just 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 me and other senators. For example, in response to a request that I made this past summer, the intelligence community acknowledged that on at least one occasion the FISA Court has ruled that collection carried out by the government under the FISA Amendments Act violated the Fourth Amendment to the Constitution. I think that's an important point to remember when you hear intelligence officials talk about what a great job they're doing at protecting Americans' privacy. And I would also note on this point that partially declassified internal reviews of FISA Amendments Act collection have noted that "Certain types of compliance issues continue to occur."

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 like to bring up is a term called "minimization procedures." This is an odd

term, but it simply refers to rules for dealing with information about Americans. Intelligence officials will tell you that their minimization procedures are the greatest thing since sliced bread and night baseball, and that even if there aren't enough privacy protections in the law itself, minimization procedures provide all the privacy protections that anyone could ever need.

Conveniently enough, these minimization procedures are classified, so most people will never know what they actually say. As someone who has access to these minimization procedures, I'll be the first to tell you that they're better than nothing, but they are absolutely not a substitute for having strong privacy protections written into the law itself.

Furthermore, senior intelligence officials have sometimes described these handling procedures in very misleading ways, and made protections for Americans' privacy sound a lot stronger than they actually are. I was particularly disappointed when the Director of the NSA, General Alexander, did this recently at a large technology conference. In response to a question about NSA surveillance of Americans, General Alexander referenced the FISA Amendments Act, and talked in particular about the minimization procedures that apply to collection of US communications. General Alexander said that when the NSA sweeps up communications from a "good guy," which I assume means a law-abiding American, the NSA has, quote, "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." Now most people who hear that would probably think that sounds pretty good, and I imagine it was what the people in the conference hall wanted to hear. The only problem is that it isn't true. It isn't true at all. The privacy protections provided by these minimization procedures simply are not as strong as General Alexander made them out to be.

In October, a few months after General Alexander made these comments, Senator Udall and I wrote him a letter asking him to please correct the record. I'll read the first few paragraphs of the letter we wrote:

"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 US persons. Specifically, you said: (And I'm quoting General Alexander here:)

> "'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 went to say:) "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's not exactly how minimization procedures work, and of course the privacy protections aren't as strong as that. If you'd like to read his letter, I've got it up on my website. I still don't know why General Alexander described the minimization procedures the way he did. It's possible that he misspoke, or that he was simply mistaken. But I think I'd be a lot more sympathetic if it hadn't taken the NSA nearly four months to correct the record. As inaccurate as the General's remarks were, if Senator Udall and I hadn't written our letter, I'm not sure that the NSA ever would have corrected them at all.

And again, I don't think that these minimization procedures are a bad idea. I just want to dispute the suggestion that because we have them we don't need privacy protections written into the law.

General Alexander also made another confusing remark in response to the same question. He said, and I quote, "…the story that we [the NSA] have millions or hundreds of millions of dossiers on people is absolutely false."

I've got to be honest: I've been on the Senate Intelligence Committee for twelve years, and I don't understand what the term "dossier" means in that context. So, in our letter in October, Senator Udall and I asked the Director to please clarify that statement. We asked, and I quote, "Does the NSA collect any type of data at all on 'millions or hundreds of millions of Americans'?" I think that's a pretty straightforward question. Really, if you're asking whether the NSA is doing a good job protecting Americans' privacy, I think it's one of the most basic questions of all. And if General Alexander saw fit, he could answer it with a simple yes or no.

Instead, the Director of the NSA replied that while he "appreciate[d] [our] desire to have responses to these questions on the public record," he would not provide a public answer. Let me go over that exchange again: The Director of the NSA said that "the story that we have millions or hundreds of millions of dossiers on people is absolutely false." Senator Udall and I then asked him "Does the NSA collect any type of data at all on 'millions or hundreds of millions of Americans'?" And the Director refused to answer the question.

At this point you are probably asking what I think should be done about all this. I recognize that the FISA Amendments Act has enabled the government to collect some useful intelligence information, so my goal in this debate is to reform the FISA Amendments Act, rather than force it to expire altogether. The two specific things I want to do are, first, to 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 where we can already see that they are needed.

I and other senators have prepared several amendments that are designed to increase oversight and improve the public's understanding of this law, and I'll describe them briefly.

First, I am sponsoring an amendment, which is cosponsored by Senators Mark Udall, Mike Lee, Dick Durbin, Jeff Merkley, Tom Udall, Mark Begich, Al Franken, Jim Webb, Jeanne Shaheen, Jon Tester, Jeff Bingaman, Frank Lautenberg, Chris Coons and Max Baucus that would require the Director of National Intelligence to submit a report to Congress on the privacy impact of the FISA Amendments Act. This amendment would require the report to state whether any estimate has been done of how many US communications have been collected under this authority, and to provide any estimates that exist. I would like to emphasize that this amendment would not require any entity to actually conduct such an estimate – the Director would only be required to provide any estimates that have already been done, and if no estimates exist he could simply 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 back-door searches. These are straightforward questions, and I think they're obviously relevant to understanding the scope of this law's impact on Americans' privacy.

Finally, this report would address General Alexander's confusing statements by requiring the DNI to simply state whether the NSA has collected any personally identifiable data on more than one million Americans. It is important that we get an answer to this question as well.

I want to emphasize that this amendment would 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 Congress why he did so. So to repeat – this amendment would not require the intelligence community to conduct any new estimates, and the President would have full discretion to decide whether or not any information should be public.

I'm offering this amendment because I think every member of Congress should understand the answers to these questions. If your constituents are anything like mine, they expect you to give government agencies the authority to protect our

country and gather intelligence on important topics, but they also expect you to conduct vigorous oversight of what those government agencies. There's often a temptation to say, "Well, I don't know what's going on, so I'll let somebody else worry about it." I think our constituents expect every one of us to know what's going on, or if we don't know, to ask the important questions. And this amendment is about asking those important questions.

There are two other proposed amendments that would increase public understanding of the impact of this law. Senator Leahy's amendment would direct the Intelligence Community Inspector General to conduct an audit of how the FISA Amendments Act authority has been used, which I certainly think would be helpful, and his amendment would also shorten the extension of this law from five years to three years. Given how little most members of Congress know about the actual impact of this law, I think that shorter extension period would be entirely appropriate.

I'm also pleased to see Senator Merkley's thoughtful amendment, which I and other senators have cosponsored. This amendment would address the very serious problem of secret law and require the executive branch to follow through on its promise to start telling the public about the secret interpretations of the law and the Constitution that have been made by the FISA Court.

I also proposed a second amendment, which had the support of a number of senators, that would have prohibited government officials from conducting the warrantless "back door" searches that I described earlier. Our amendment would have permitted officials to deliberately search for a specific American's communications pursuant to an individual warrant or emergency authorization, or in situations where the American was believed to be in danger. I am disappointed that we could not get an agreement to vote on this amendment, since I think it would go a long way toward restoring necessary privacy protections for the phone calls and emails of law-abiding Americans.

Finally, I am looking forward to the debate on Senator Paul's amendment, which goes well beyond the FISA Amendments Act itself to address some big-picture Fourth Amendment issues. Senator Paul brings an incredible amount of hard

work, passion, and intellectual engagement to these issues, and I'm looking forward to hearing what he has to say.

And I'm also looking forward to hearing from those colleagues who may have other views on this bill, and who perhaps think that we should simply extend this law for five years without any amendment at all. I'm confident that some of these members will be coming down here to make their case, and I'm hopeful that we can have a serious discussion about protecting security and protecting privacy. This is an important time for American security, but it is always an important time for Americans' rights and freedoms.